Università
Ca'Foscari
Venezia

Master's Degree

In

Global Development and Entrepreneurship

Final Thesis

The Digital Services Act as a new tool to deal with the spreading of Illegal content online

Supervisor
Ch. Prof. Giuliano Zanchi

Graduand
Sara Salvador
Matriculation number
849666

Academic Year
2020 / 2021

Index:

Chapter 5. Different types of illegal content online

5.1 Intellectual Property Infringements and Counterfeit Goods

5.1.1 Online Service providers offering or facilitating access to copyright-protected material

- Cyberlockers
- Stream-Ripping Services
- Linking or Referring Websites
- Peer-to-peer and BitTorrent indexing websites
- Unlicensed download sites
- Piracy Apps' Websites
- Hosting providers
- Unlicensed IPTV Services
- Social Media

5.1.2 E-commerce Platforms

5.1.3 Online Pharmacies and Counterfeit Pharmaceuticals

5.2 Child Sexual abuse

5.3 Terrorism

5.4 Illegal Hate Speech

Chapter 6. Not illegal but harmful content online

6.1 Non-consensual pornography

6.2 Disinformation

Part III Conclusions

Introduction

More than ever before, our lives have become dependent on technology and online platforms. Any time we want to communicate with friends, to look for the features of the new cutting-edge technological device we are planning to buy, to find the recipe of a new cake we want to try or even just to listen to our favourite playlist, we rely on electronic devices and on the wide array of online platforms we can have access to.

According to the data of the *Global Digital Report of 2019*[1], the average time spent online daily at global level is of 6 hours and 42 minutes. This means that every day people spend more than one quarter of the day staring at their screen and being connected to the Internet. The huge amount of time spent online has made the Web a fertile environment for enterprises that wanted to expand their business beyond their borders or just to reach their customers more easily.

The Covid-19 pandemic of the last year fostered this digitalisation process even further. In fact, the global pandemic and the consequent lockdowns imposed by governments drastically changed the lifestyle and purchasing behaviours worldwide. Companies had necessarily to rely on online platforms in order to stay competitive in the new global scenario and most of them, mainly SME, had to build their web presence from scratch. To achieve this, businesses had to rely totally on the main online platforms who are able to reach a wide array of potential customers and, as a consequence, online big platforms gained power as never before. To prevent these big players from ruling the not well-defined areas of the new economic scenario as they please, governments have to set new rules in order to keep the legal framework of digital laws and regulations updated with the new needs of the digital market.

At the same time, the increasing amount of time spent on the Internet brought to a rise of the online spread of illegal content. Illicit online content can be of various

[1] Digital 2019 Essential Insight into how people around the word use the internet, mobile devices, social media and e-commerce. Hootsuite publication. Data are related to 2019 so the report does not consider the massive increase of time spent online that followed the Covid-19 pandemic.
https://p.widencdn.net/kqy7ii/Digital2019-Report-en

kinds: online scams, sale of counterfeit products, the sharing of copyrighted multimedia content without the legitimate owner consent, pedo-pornography, pharmaceutical products sold without any control by the authorities, etc. Ever since businesses began to expand online, providers of illegal content have always been present as a parallel economic world that has continued to expand quickly due to the difficulty to detect them as well as a not defined action plan to act against this abuse. The 2020's pandemic and the sudden increase in online users have made the Web a further breeding ground especially for suppliers of counterfeit products. Certain illegal suppliers have been able to take full advantage of people's fear in addition to the weaknesses of the economic situation and the shortcomings in the health sector, for example by selling non-compliant facemasks[2] or vaccines of dubious origin.

Furthermore, it is extremely easy for online users to come across illegal content because it or links that redirect to its website are often located in the most used online platforms. However, reporting and removing such content can be difficult due to multiple factors such as a lack of timely response by the platform after the content has been notified, the lack of transparency of certain platforms and the endless strategies that can be implemented by illegal providers to hide their identity and location.

In past years, the European Union, as well as Member States singularly, has enacted several laws and regulations in order to give major responsibility to online service providers on the need to identify and remove illegal or harmful content. However, given the lack of satisfying results and the speed at which the virtual world has evolved recently, governments have realised the imminent need to provide a clearer and more uniform legislative framework about how to deal with online platforms and illegal content online. Since the online world doesn't have physical boundaries, it is very important to give the Community a unique direction and to avoid fragmented legislations at national level that have two main negative consequences. The first problem is the concrete risk that the same harmful or illegal content could be treated

[2] mascherine non conformi

differently according to the national laws and this is a great obstacle for the achievement of an homogeneous market. The second consequence is that a fragmented legal framework is a discouraging factor for SME that want to expand their online presence since they have to face many costs in order to deal with a patchy regulation. In addition, the proposal aims to limit the power of big online platforms and ensure greater transparency in order to help SME that have to rely on these web giants as their only choice to have visibility on the market.

Structure of the paper

This paper is going to describe how the European Commission with its new proposal, together with the current laws, aims to deal with the new online challenges and especially with the spread of illegal online content. In fact, in the first part, we want to illustrate the draft law published by the Commission on 15 December 2020, the Digital Services Act. In particular, the purpose is to highlight how this proposal intends to give a single direction to the contrast of illegal content online, and how it intends to enhance responsibility for big online platforms that have the power to make the web a safer place. In the second part, we identified and listed the main types of illegal content that can be encountered online, as well as the risks that this content may arise for the EU community and economy and the main difficulties that authorities can encounter in detecting and removing it. In this context we will also consider the not illegal but harmful content that can be defined as anything in the Web which causes a person distress or harm, such as cyberbullying and revenge porn. Finally, in the third and last part, we highlight the positive and negative aspects of the new legislation, the difficulties that might arise and the areas that will probably need a further development in the future.

Part I

THE DIGITAL SERVICES ACT

Chapter 1

Context of the proposal

Well before the pandemic of the last year, the Commission President von der Leyen stressed the need for the European Union to lead the transition to a digital world. It would be naive for Europe to underestimate the huge changes that the digitalization process brought to the economy in the last decade, as well as the uncertainties that have followed. In a paper published in February 2020[3], the European Commission states that digital solutions can enrich our lives in many ways, but the *benefits arising from digital technologies do not come without risks and costs*. Despite these difficulties, the digital world is certainly the future. The European Union needs not only to invest in innovation, but also to make citizens feel as safe in the online world as they are offline, by providing a secure online environment. However, the one sure thing is that the more interconnected citizens are, the more they are vulnerable to malicious activities of cybercriminals. In order to tackle these threats, the EU in the past years settled new rules and gave recommendations, but the dynamic development of the digital environment has been much faster than the relative laws. As mentioned earlier, the Covid-19 pandemic and the consequent lockdowns have changed the way in which companies and users approached the Web, making this process of digitalization indispensable and quick. The excessive speed of this online expansion has highlighted even further the problems and **legislative gaps** that for years have been affecting the regulations for digital service users and providers.

Since the adoption of the e-Commerce Directive in 2000 many changes have concerned the Information Society and **new digitals services have emerged**. At the very beginning, it was not easy to identify which new value some platforms were bringing to the society and this has led to a lack of data on many aspects of platforms' economic role and behaviour. It was, and still is, very hard to assess and predict the impact of these

[3] Communication: Shaping Europe's digital future, first publication 19 February 2020, Luxembourg: Publications Office of the European Union, 2020. (https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_it)

new service providers on the economy, since companies, such as Facebook and Google, based they business model mainly on the sale and exploitation of data they got from users. In a recent report of the European Commission, data are defined as a *"nebulous concept* difficult to both define and measure*"*[4]*.* In fact, platforms, by nature, connect multiple parties to each other, facilitate flows of information from one party to another and, also, keep data for themselves. This huge data base has enabled few very big platforms, the most used by users, to become the *gatekeeper* of the Internet. The fact that all the data are in the hands of a few very large companies has given them an enormous power that must necessarily be managed by governments to avoid abuses or unfair practices that could undermine the free competition on the market. In fact, in the present pandemic situation, all the SMEs have necessarily to rely on these big platforms if they want to gain visibility and reach a wide array of potential customers.

In addition to the huge power these *gatekeepers* have over the future of the businesses' economy, it must be considered that the **management of illegal content online** also depends largely on the measures taken by them. With the rise of online users the presence of illegal content on the Web has increased as well, but the existing laws have failed in contrasting it successfully. The European Commission stated that "*what is illegal offline must also be illegal online",* yet in the digital world there is a wider spread of illegal content that is often too easily accessible by users. According to the Commission, Member States and stakeholders it is essential to strengthen and modernise rules, clarifying the responsibilities and roles of online platforms. The spread of copyright protected material and the sale of counterfeit or dangerous goods must be tackled as effectively online as it is in any other physical market. For this purpose, it is extremely necessary to define and set clearer rules on the transparency, behaviour and accountability of online platforms who act as gatekeepers of information.

[4] The Commission in 2020 published a study on the actual traffic of user data that is creating a huge value in the economic world. The report is "Work stream on Measurement & Economic Indicators, Progress Report" published by Expert Group for the Observatory on the Online Platform Economy. (https://platformobservatory.eu/app/uploads/2020/07/ProgressReport_Workstream_on_Measurement_and_Economic_Indicators_2020.pdf)

Although immediate changes are needed, it is essential to maintain the core principles of the e-Commerce Directive of 2000 and to protect the fundamental rights in the digital world, as well as the anonymity where it is technically possible. According to the Directive 2000/31/EC it is prohibited to impose a general monitoring clause to online platforms, and this principle must remain untouched. However, it is fundamental to define and clarify the active role that online platforms should adopt when some illegal content is notified and when they, instead, become responsible due to a lack of immediate reaction. Another relevant point is to encourage online big platforms to undertake internal searches in order to find and tackle illegal content and, at the same time, don't make them lose the benefit of exemption from liability. Fundamental in this subject is the good faith of the provider of intermediary services, that we will analyse deeper in the next chapters.

Regarding the **consistency with other existing policy**, the Digital Services Act is built on the provisions of the e-Commerce Directive, particularly on the internal market principle set out in Article 3. What is added is a cooperation and coordination mechanism for the supervision of the fulfilment of its obligations. This proposal also deletes the articles 12-15 of the e-Commerce Directive and reproduces them clarifying the horizontal framework of the liability exemption for providers of intermediary services. Furthermore, depending on the legal system of each Member State, the competent authorities can order providers to act and remove a specific illegal content, as well as prevent it from reappearing on their platforms. Especially in this last case, it is essential that the ordinance is issued in compliance with the Union law, keeping the prohibition of imposing general monitoring obligations.

The proposed Regulation introduces a **horizontal legal framework** for all the categories of products, contents, services and activities on intermediary services and doesn't define what is illegal or not. In fact, the illegal nature of such content results from the Union law or from the national law. At the same time, some specific categories of illegal content have already a sector-specific legislation, such as copyright infringements, child sexual abuse material, terrorist content, illegal hate speech and

some illegal products. For this reason, it is very important to clarify the relationship between the Digital Services Act and these sector-specific laws. The new proposal aims to integrate the current sector-specific legislation and "does not affect the application of existing EU laws regulating certain aspects of the provision of information society services, which apply as *lex specialis*"[5].

As has been said before, the proposed Regulation is mainly built on the evaluation of the e-Commerce Directive of 2000. This directive aimed to guarantee especially three aspects: the well-functioning of digital services in the internal market, the effective removal of illegal content online and an adequate level of information and transparency for consumers. Despite the important incentive that it brought for the growth of digital services in the European market, the initial objectives have not been fully achieved. The digital landscape has evolved very fast and new digital service providers have emerged bringing with them new challenges. In order to deal with these new challenges, Member States have legislated independently, but this law fragmentation urge to be clarified given the need to unify the internal market of digital services.

Moreover, the increasing importance of the online environment for the global economy and the inevitable emergence of new digital services in the future will lead to a further fragmentation because, with a view to facing the new arising problems, Member States will continue to legislate independently. The legal fragmentation among

[5] Digital Services Act, Explanatory Memorandum, Context of the Proposal. The Regulation define itself as a lex specialis since its application will be horizontal to the current laws, particularly as defined in Article 1 the Regulation is without prejudice to rules established in:
Directive 2000/31/EC;
Directive 2010/13/EC;
Union law on copyright and related rights;
Regulation (EU) …/…. on preventing the dissemination of terrorist content online [TCO once adopted];
Regulation (EU) …./….on European Production and Preservation Orders for electronic evidence in criminal matters and Directive (EU) …./….laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [e-evidence once adopted]
Regulation (EU) 2019/1148;
Regulation (EU) 2019/1150;
Union law on consumer protection and product safety, including Regulation (EU) 2017/2394;
Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.

States will create a fertile environment for the spread of illegal content since it will be more difficult to contrast it efficiently. Furthermore, the patchwork of national measures will hinder new and innovative services from entering and scaling up in the European market, fostering and consolidating the strong position of the few big businesses who can afford to incur high costs. From this perspective, the power of very big online players will increase even further at the expense of other smaller businesses, of national and supranational authorities and of users. To avoid this scenario is fundamental to act immediately, in order to better distribute powers and responsibilities between public authorities and big online platforms. The key points of such intervention in the digital environment would be 1) the introduction of new procedural obligations for digital service providers to tackle illegal content on their platform; 2) remove eventual obstacles and disincentives that providers may have to take voluntary measures against illegal content and, in addition, enhance transparency; and 3) impose heavier obligations to very big online platforms since they have many resources that can support States in the fight against any potential risks that may arise while browsing on their platform. All these measures have been approved by the EU governance, the Member States and the stakeholder taken into account.

In fact, before submitting the Digital Services Act proposal, The Commission, to have a better understanding of the main issues relating the digital environment, **consulted a wide range of different stakeholders**. Such stakeholders are digital service providers such as online platforms and intermediary service providers, users of digital services, brand owners and businesses of various size, media publishers, social partners, business trading online, national authorities, civil society organizations, international organizations, academia, the technical community and the general public. All these different stakeholders have highlighted the same relevant issues and they all agree on the need to improve the fight against illegal content online and enhance online security, as well as on the need to further the internal market for digital services. Furthermore, they agree on the need to enhance responsibilities for the digital service providers by establishing clear obligations harmonized across the EU. Most of the respondents said

that they have encountered harmful and illegal content, products or services while browsing online and that during the Covid-19 pandemic the dangerous content has even increased. They also claimed they notified such harmful or illegal content to the online service providers and that they have been dissatisfied with the slow or lacking reaction by the platform. Another common issue that came up was the urgent need to provide a better identification of online sellers. Too often, also in well-known large online platforms, it is easy to find and buy counterfeit or illegal products without being able to identify the seller's identity. This issue often concerns platforms whose headquarters are established outside the EU and, for this reason, the stakeholders, as well as the Commission, generally agree that the obligation to provide clear information about the seller identity should concern all the platforms selling products, services or offering content in the Union, regardless of their place of establishment. A major transparency by big online platforms is needed not only about the sellers' identity, but also in many other aspects that have emerged during the consultation of the interested parties. One concrete risk is that during the removal of illegal content some not illegal material may be removed by mistake or, also, that the removal of a considered harmful content would result in an unjustified restriction of freedom of expression. In some circumstances the line between illegal or just harsh content can be very thin. For example, in the case of illegal hate speech or defamation, platforms on one hand have to act in a timely manner to limit the spread of the dangerous content, on the other, in order to be certain that a content is actually illegal or defamatory, it is necessary to wait for a court sentence or a double check. A relevant recent case who has captured the attention of the entire world has been the one of the Facebook account of Donald Trump, temporary blocked by the platform because according to the inner policies the content of the last posts was exhorting to violence and inciting hatred. The public opinion was divided between those who approved the decision of the platform and those who denounced this measure as excessive, because taken on the basis of different political opinions and on a subjective view. Transparency is needed also to avoid not illegal content from being removed by mistake. For instance, an unfair takedown of an advertising of a company that use that

specific online platform as its only mean to attract customers could create a serious damage to the company's economy. For this reason, it is very important that online platforms inform their users about the removal rules and internal policies of the platforms. A clear and transparent guidance of the way the platform deal with some kind of contents must be provided in order to ensure a deep understanding of how the algorithm works and to allow unfairly damaged businesses to act to have their content restored as soon as possible. The Regulation proposal, in fact, establishes that platforms must have a clear and easy mechanism to notify illegal content as well as a clear redress possibility to contest the decision of removal.

Another significant case that fostered the proposal of the Digital Services Act is the legal case between Facebook and Eva Glawischnig-Piesczek[6]. A member of an Austrian party, Ms Eva Glawischnig-Piesczek, asked Facebook to delete a harmful defamatory comment about her. As the platform didin't comply with her request, she proceeded against it and obtained from the Austrian court an order prohibiting the platform from publishing or disseminating such content or any similar content. As mentioned earlier, the e-Commerce Directive provided that a hosting platform should not be liable for content generated by users if it is not aware of the illegal nature of such content and that Member States cannot "*impose a general obligation on providers … to monitor the information they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*"[7]. The case reached the Austrian Supreme Court which asked to the Court of Justice of the European Union to decide whether the Directive precluded national courts from requiring platforms to remove also content that is identical or equivalent to content that has been previously declared illegal. The CJEU clarified that the prohibition of the directive was about *general*

[6] Case C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Limited, Judgment of the Court (Third Chamber) of 3 October 2019. The case gained not just European, but global attention from media. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=1309)

[7] The prohibition to impose a general monitoring obligation is maintained in the Digital Services. The reference is of the Directive on electronic commerce that can be read at the Act. Official Journal L 178 , 17/07/2000 P. 0001 – 0016.
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

*monitorin*g and that the court could ask to find and remove a *specific identical content* and that host providers should be able to identify and remove equivalent content using automated searching tools. However, this sentence had been deeply criticized because it seems to be detrimental to the freedom of expression, because of the lack of a clear definition of *equivalent content* and because technologically speaking there is not such an *automated tool* who can help detecting equivalent content as the CJEU claims.

The case was a very relevant starting basis to highlight the need of clarifying the extent to which online companies should be liable for user-generated content as well as to point out the different law approach of Member States. In addition, the Commission took inspiration from this judgement while preparing the Digital Services Act proposal, whose aim is to find a solid solution to these big issues, in fact it wants to give a unique guideline at the EU level, to define better online platforms' responsibilities according to their size and to outline rules about transparency and intervention mechanisms.

Chapter 2

General overview of Digital Services Act and how it is structured

2.1 General Overview

The Digital Service Act (or DSA) is part of the package of reforms with which the EU is willing to create a new digital single market. On 15 December 2020, the proposal has been submitted by the EU Commission with the aim of amending parts of Directive 2000/31/EC (the e-Commerce Directive) while maintaining its core principles and now it is following the legislative process that could last for years. After the General Data Protection Regulation[8] approved in 2016, in addition to being a leader in privacy legislation, the EU was ready to come up with the new proposal to lead all Member States and online platforms on a single direction: the creation of a safer online environment and a fair and competitive online world also for small and medium enterprises. The Regulation has been presented to regulate *ex ante* the activities of online platforms who act as gatekeepers of information that now are following their own rules and therefore setting rules for their users and competitors. With the approval of this Regulation the power of online platforms would be channelled to guarantee a competitive environment for all companies that need to use such platforms to reach their customers and to guarantee a secure online environment where illegal and harmful content is tackled and removed.

The same day the Commission also presented the Digital Markets Act, a Regulation who is willing to integrate the DSA and will introduce prohibitions and restrictions as well as new obligations for online platforms. Rather than the Digital Services Act, this proposal focuses more on the need to avoid discriminations by platforms in favour of their own services and to avoid behaviours that could damage their competitors in addition to the obligation to share users' data they store.

[8] 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.

2.2 What is new

The main novelties that the Digital Services Act will introduce are:

(1) The review of the of the e-Commerce Directive, as mentioned earlier, and a modernised liability regime for online services providers. The key principles of the Directive 2000/31/EC will remain generally unchanged but there are some additional caveats about the management of illegal content. Particularly, this Regulation lays down the obligation for intermediaries to put in place a user-friendly *notice-and-action* mechanism to allow the notification of illegal content.

(2) New obligations for providers about the information they need to gather about the sellers they host on their platforms. Furthermore, better traceability of providers that are established outside the EU and that are providing services to users inside the European Market through the need to designate a legal representative inside the EU.

(3) More transparency is required to online platforms about many issues:

   i. If some content is removed, the need to give an explanation to the user who uploaded the content and provide him with the information on the redress possibilities.

   ii. The obligation for platforms to publish detailed reports on their activities regarding the tackling and removal of illegal content.

   iii. Transparency on the advertisements that are displayed to users. They have to provide information about why the user is seeing that advertisement, on whose behalf the ad is displayed and also share information about the parameters they use to address the ad.

(4) Additional and more burdensome obligations for very big online platforms, who need to consider and prevent the *systemic risks* they may cause.

(5) Proportioned fines for platforms that don't respect the obligations.

2.3 Structure

The Digital Services Act is divided in Chapters and Sections.

Chapter I defines the general provisions and gives a definition of the specific terms present in the document. These terms are often difficult to understand for someone who doesn't have experience with the online world and it is fundamental to give a clear definition of them for legal purposes.

Chapter II gives provisions on the exemption of liability of providers of intermediary services and specifically defines, in the articles 3,4 and 5, when providers are not responsible for the information that they just transmit and store for a third-party. Important in this chapter is the specification that if a platform carry out voluntary investigations by its own, it does not lose the liability exemption and that the imposition of a general monitoring obligation is always prohibited. Finally, the articles 8 and 9 impose an obligation to respect authorities' orders related to the tackling of illegal content or to provide and disclose information.

Chapter III defines "due diligence obligations for a transparent and safe online environment" and it is divided into five sections.

Section 1 defines the "obligations applicable to all providers of intermediary services". Thus, these obligations apply to *all providers of intermediary services* regardless of their size or the specific service they provide. In the first articles of this Section it is recognised the need for *all providers* to establish a "single point of contact" (Article 10) that allows a direct and quick communication with the authorities of the Member States, the Commission and the Board as well as the obligation for providers offering services inside the EU but established outside the EU to nominate a legal representative. The last two articles of this sections define

which information the providers must include in the general terms of their services and the transparency reporting obligations that they must fulfil.

Section 2 defines further obligations that are applied to providers of hosting services. Very important in this section is the mandatory introduction of a *notice and action mechanism* that providers shall make available to allow their users and third parties to notify illegal or harmful content. If after the notification the provider decides to remove the illegal content, he must communicate to the content owner the reason why the content has been deleted or suspended.

Section 3 gives many important additional provisions applicable to all online platforms with the exception of micro or small enterprises. In the first article it is considered the obligation for providers to create an internal complaint-handling system to allow users whose content has been removed or whose account has been suspended to take action to have it restored if they think the removal has been unfair. Damaged users as well as platforms have also the right to involve certified out-of-court dispute settlement bodies with the purpose to resolve any disagreement. The Section provides information about trusted flaggers and obliges providers to give priority to notifications submitted by them; it also defines protective measures against the misuse of the notification tool. In this context is also treated the requirement for platforms to inform authorities in the moment they become aware of “criminal offences involving a threat to the life or safety of persons” (Article 21). With the purpose to provide a safer online environment, this Section also requires platforms to acquire, store and verify information about traders and sellers using their service. Additionally, the Section establishes for platforms the obligation to publish reports on their disputes and removal activity of illegal content along with transparency obligations with respect to the advertising on their online interface.

Section 4 introduces additional provision for very large online platforms and it considers the systemic risks that may arise given the wide network and the

dominant position of such platforms. The focus of this Section is on the efforts and the measures that such platforms need to take in order to reduce the systemic risk they may cause, including the obligation to submit themselves to independent audits and the requirement to provide information about their recommender systems and the online advertising they display on their interface. Furthermore, very big online platforms shall provide access to data to the Digital Services Coordinator of establishment or the Commission whenever required in order to allow to check the compliance with the Digital Services Act. For the same purpose, they have to appoint one or more compliance officers to ensure the observance of the provisions and to comply with additional transparency reporting obligations.

Section 5 contains other provisions about due diligence obligations, about the development of codes of conduct and codes of conduct for online advertising and about crisis protocols in case of "extraordinary circumstances affecting public security or public health" (Article 37).

Chapter IV contains the provisions about the implementation, sanctions and enforcements of this Regulation and it is divided into sections.

Section 1 defines provisions concerning the competent authorities nominated by Member States including the Digital Services Coordinators, independent and impartial figures who perform their task "transparently and in a timely manner" as defined in the Article 39, while their specific powers are explained in the article 41. The Article 40 defines the areas of jurisdiction of Member States. Furthermore, this Section settles the penalties that shall be applied against providers that do not observe the provisions of the Regulation and that "shall be effective, proportionate and dissuasive", as well as the right of recipients of the service to lodge a complaint against providers with the Digital Services Coordinators.

Section 2 just lays down provisions about the nature, the structure and the tasks of the European Board for Digital Services, “an independent advisory group of Digital Services Coordinators”, called *the Board*, that should cooperate with the European Commission and the Digital Services Coordinators designated at national level.

Section 3 establishes additional provisions about the supervision, investigation, enforcement and monitoring of very large online platforms. The Article 50 lays down an enhanced supervision in case the very big platform infringes the provisions who apply only to such platforms (more specifically the provisions settled in the Section 4 of Chapter III). This section also considers the potential intervention of the Commission in the event that the Digital Services Coordinator of establishment didn’t take any action against a violation or if the intervention has been required by the Coordinator. The Commission with the aim to conduct investigations may require from the platform specific information, it can take interviews and it has the power to carry out on-site inspections. Furthermore, it can adopt interim measures and settle binding commitments added to necessary monitoring actions. Finally, this Section defines provisions in case of non-compliance with the Regulation as well as fines and periodic penalty payments that platforms shall pay until they provide required information, submit to an ordered on-site inspection, comply with interim measures or binding commitments.

Section 4 defines common provision on enforcements, such as the need to establish a reliable information sharing system to support communication between the Board, the European Commission and the national Digital Services Coordinators.

Section 5 considers the power of the Commission to adopt delegates and establishes that the Commission shall be assisted by the Digital Services Committee, defined by within the meaning of Regulation (EU) No 182/2011.

Chapter V, finally, gives the final provisions of this Regulation. These last articles are very important since they state the deletion of Articles 12 to 15 of the Directive 200/31/EC that are replaced by the Articles 3,4,5, and 7 of the Digital Services Act. In this Chapter are also considered the terms to evaluate the implementation and results of this Regulation as well as its entry into force and application.

Chapter 3

How the Digital Services Act is willing to contrast illegal content online

3.1 Some definitions and liability of providers of intermediary services

3.1.1 Illegal content definition

In the explanatory memorandum of the Digital Services Act the Commission has explicitly stated that such paper does not purport to define the illegal nature of specific contents or services since it has been defined already both in Union and national law. Despite this premise, the Regulation includes a definition of illegal content. The **Recital 12** states that "the concept of *illegal content* should be defined broadly", in fact it regards not only contents but also "products, services and activities". Furthermore, they give even a wider interpretation of such content defining it as any information, independently of its form, that under the applicable law is either itself illegal or that relates to illegal activities. According to the Commission explanation, information that is "illegal in itself" is, for example, illegal hate speech, terrorist content and unlawful discriminatory content, while the related "activities that are illegal" are the sharing of pedo-pornographic images, online stalking, unlawful non-consensual sharing of private images, the sale of nonconforming or counterfeit products, the use or share of material protected by copyright without the owner consent or activities who infringe the consumer protection law. The concept of illegal content is repeated in the Article 2 letter *g* where it is defined as any information which is not in compliance with the Union law or Member States' law, "irrespective of the precise subject matter or nature of the law".

Nevertheless, the lack of a well-defined definition of illegal content into the text of the DSA has raised debates during the approval process of such Regulation. In fact Member States have expressed concern about the fact that in order to evaluate the illegal nature of a specific content a *hosting provider* shall take into account a very wide body of legislation at both European and National level. This can be very complex,

considering the cross-border nature of the business of most digital intermediaries and how the typology of some illegal content may vary across the domestic law of Member States. To clarify this risk, let's take the Italian law as an example. In the Italian legal system there are some inner specific laws that are not present in the other Member States of the European Union. For example, *the apology of fascism* [9] that is the propaganda of fascist organizations or movements, or the public exaltation of exponents, principles, methods, facts or antidemocratic aims typical of fascism; or the so-called crime of *negationism*[10], introduced in 2016, which includes incitement to discrimination or racial hatred, ethnic or religious, that is based in whole or in part on the denial of the Shoah or crimes of genocide, crimes against humanity and war crimes. The provider, therefore, should know the legislation in force in the different Member States in which it operates and adopt more or less restrictive policies depending on the national context of reference. It is clear that this can complicate the activity of digital intermediaries a lot, in addition to the fact that unequal treatment of the same content, justified on the basis of the diversity of the applicable national legislation, could lead to disputes between digital operators on the one hand, and users or national authorities on the other hand.

3.1.2 Intermediary services and liability

In general, the Regulation states that providers are not responsible for the information processed and carried out by the user of their services, provided that they (the intermediary services providers) do not create or intervene in any way on the content of such information. The Chapter II of the DSA gives an explanation of the different liability of intermediary services' providers according to the nature of the service they provide. Particularly it distinguishes between a service of *mere conduit*, *caching* and *hosting*.

[9] Apologia del fascismo, legge Scelba n. 645/1952, legge Reale n. 152/1975, legge Mancino n. 205/1993
[10] L'aggravante di negazionismo. Legge, 16/06/2016 n° 115, G.U. 28/06/2016 https://www.gazzettaufficiale.it/eli/id/2016/06/28/16G00124/sg

- *Mere conduit* is a simple service of "transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network" as defined in the article 3. Given the nature of simple transmission of the information, the *mere conduit* service provider shall not be liable for the possible infringing nature of the information under the condition that the provider does not start the transmission, does not choose the recipient and does not select or change the content of the transmission[11]. To give an example, this can be the case of the email provider which is not responsible and absolutely not aware of the e-mail content, or again the internet access provider that merely provides simple network access for users. It is clear that the exemption of liability exists as long as the provider is in a position of absolute neutrality with respect to the information conveyed.

- *Caching* is a service consisting of the "transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request"(Article 2) [12]. According to the article 4, the service provider shall not be liable for the information, provided that the provider does not modify the information, conforms with the conditions on access to the information and with the provisions about the updating of such information, does not intervene with the legal utilization of technology to gain data on the use of the information and acts expeditiously to remove the access to the information he stored after knowing about the removal of such information from the network or after knowing that a court or another competent authority has ordered the disablement or removal of such

[11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Article 3.
[12] Digital Services Act proposal, Article 2, letter f.

content. Thus, the purpose of the caching system is to increase the efficiency of the network by keeping for a limited period of time at the server of the provider the information to which users have access, so as to facilitate the access to the same information for other recipients. Obviously, in this case too, the reference to the obligation not to modify information, in order to be free from liability, must be understood in a substantive and non-technical sense.

- Finally, as defined in Article 14, a *hosting* service "consists of the storage of information provided by a recipient of the service". The hosting provider shall not be legally responsible for the content stored by request of the receiver of the service, provided that the provider is not aware and does not have actual knowledge of the infringing nature of such content or activity and, at the moment he becomes aware of the illegality of such content, acts expeditiously to remove or disable the access to it. Such exemption from liability does not apply when the recipient of the content is acting under the control or the authority of the hosting provider and when the provider, that allows consumers to conclude distance contracts with external sellers, "would lead an average and reasonably well-informed consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control"(Article 5).

So, through articles 3 to 5, the DSA, maintains the safe harbour from liability already considered by the e-Commerce Directive for intermediary services providers that are mere conduits, caching or hosting providers. However, in addition to the Directive 2000/31/EC, the current Regulation wants to propose:

a) to include illegal content in addition to illegal activities,

b) to exclude the liability exemption for the safeguard of the consumer protection law – the article 5 in fact states that the exemption does not apply for online platforms that facilitate consumers to conclude distance contracts with traders when the platform present information in a way that would lead a consumer to believe that the product/service is provided by the platform itself – as mentioned above,

Another novelty that the DSA wants to introduce in order to refresh the e-Commerce Directive content is the liability exemption for intermediary service providers who conduct "voluntary own-initiative investigations" led by the purpose to detect, identify and remove, or disable the access to infringing content. In this way the new Regulation does not want to penalize but instead it wants to provide providers with the confidence to engage in such voluntary investigations and to encourage them to take an active role in countering illegal content. However, Article 7 of the new regulation reiterate one of the core principle of the e-Commerce Directive: the prohibition to impose on these providers a general obligation to monitor the information they transmit or store. This because a general monitoring obligation could burden providers excessively and interfere with their freedom to lead a business, at the same time it could "disproportionately limit users' freedom of expression and freedom to receive information"[13]. Despite the prohibition to impose a general monitoring obligation, after obtaining actual awareness of the illegal nature of the content, providers should act expeditiously to remove it in order to benefit from the exemption from liability. If the order to act against a specific content is coming from a national or administrative authority, the providers shall inform such authority about the action taken against the content and when it was taken. Furthermore, another obligation of providers is to provide without undue delay specific information on individual users that they can be required by a competent authority, presumably to allow the authorities to assess the

[13] Digital Services Act, Explanatory Memorandum, 3. Results of Ex-Post Evaluations, Stakeholder Consultations and Impact Assessments, Fundamental Rights paragraph.

identity and liability of anyone who have uploaded illegal or harmful content[14]. About this provision, the recitals of the DSA, that are non-binding and aiming to fill gaps in the current legislation, state that orders to provide information about users should be issued in compliance with the GDPR. The fact that the DSA is without prejudice to the GDPR is also confirmed in the first article of such regulation proposal.

3.2 Detecting and Notifying Illegal content online

The area of application of the Digital Services Act is broader than the e-Commerce Directive. The new Regulation wants to impose different obligations for different categories of online intermediary service providers in accordance with the size, the role and the impact that they have on the safety of the online world and of the society in general. Accordingly, the Regulation proposal introduced distinct rules for:

- **all providers of intermediary services** including mere conduit and caching service providers;
- **hosting service providers**, for example a cloud service or a webhosting service, who store and spread information to the public;
- **online platform services** who base their business on bringing together vendors and buyers, for example online stores, online marketplaces, app stores, social media and peer-to-peer economy platforms;
- **very large online platforms**, defined in the DSA also "VLOP", that are platforms whose user base reach more than 10% of the European Union total population (about 45 million users). These providers have more burdening rules since they have a heavy impact on the economy and on the society, they also are supposed to effective support authorities in the countering of illegal content dissemination in the online world.

[14] The EU's Proposed Digital Services Act. New Obligations and Sanctions for Online Platforms. Latham & Watkins LLP, March 2021.

3.2.1 Provisions applicable to all providers of intermediary services

Chapter III of the draft gives basic obligations that will apply to all providers of intermediary services. According to the article 10, all providers will have **to establish a single point of contact** with competent authorities and particularly with the Member States' authorities, the Commission and the Board[15] in order to allow direct communication by electronic means. If the provider does not have his legal basis or establishment in the European Union but he offers services to users inside the EU, he shall **designate a legal representative** inside one of the Member States where he is providing its services. Such representative should be provided with the powers and resources needed to cooperate with competent authorities, as well as the Commission and the Board and he can be held liable for the infringements of the rules established by this Regulation. Article 12 requires all providers to include in their general **"terms and conditions"** all the information about the restrictions they may impose on the use of their services. They need to specify, using a clear and understandable language, the inner policies, measures and tools they use with the purpose to moderate content, including the "algorithmic decision-making and human review"(Article 12). When applying and implementing the restrictions providers are required to act diligently with regards to the respect of fundamentals rights and the interests of all parties involved. Then, all providers need to ensure **transparency**. For this reason, once a year they are obliged to **publish reports** about their moderation actions, particularly about the removal of content disabling of the access to such content. In these reports they need to share information about the number of orders they receive from authorities, the number of notifications they received and the action they took about it, the voluntary own-initiative measures they took and the complaints they received about the removed contents. The mandatory yearly report is not required for providers that are qualified as micro or small enterprises since it would be too burdening for them and the DSA aims

[15] Board is the *European Board for Digital Services* defined in Article 47 of the Digital Services Act and that is described in this paper at Chapter 3, paragraph 3.6 "The Board and Enhanced supervision over VLOPs".

to act proportionally and to balance the need for a safer online environment with the need to protect enterprises to stay competitive in the market.

3.2.2 Additional provisions applicable to providers of *hosting* services, including online platforms

For hosting services providers the Commission gives further provisions that add to what already said in the previous paragraph. Hosting services providers will have to put in place on their site or platform ***notice and action mechanisms***. This mechanism shall allow everyone – every user, third person or entity – to notify the existence of any content they consider to be illegal. Such mechanisms should be easy to find, to access, user-friendly and the notification have to be submitted only by electronic means. At the same time, the mechanism shall allow submitters to give detailed and adequately substantiated explanations particularly about the reason why the person think the specific content is illegal, where the content is located in detail, the name and e-mail address of the submitter as well as a statement that he is in good faith. If the submitter provided his personal contacts, the hosting services provider shall promptly send a confirmation of reception of the notice and inform him about his decision in respect of the content object of the notification. In the 6th paragraph of the Article 14 is highlighted again the necessity for the provider to act "in a timely, diligent and objective manner" (Article 14). When the provider decides to remove a specific content, he has to give the information owner a statement of reasons" (Article 15). The provider shall provide a clear and precise explanation of why the content has been removed or the access has been disabled, he also shall inform the recipient on the redress possibilities available[16] and "in particular through internal complaint-handling mechanisms[17], out-of-court dispute settlement and judicial redress"[18](Article 15). Furthermore, to enhance transparency and communication with authorities, the hosting provider shall publish

[16] Mezzi di ricorso a disposizione.
[17] Internal complaint-handling system is clearly explained in Chapter 3, paragraph 3.2.3.
[18] Digital Services Act, Article 15, paragraph 2, letter f.

information about the decisions and statements of reasons in a database managed by the European Commission that is open to the public.

3.2.3 Additional provisions applicable to online platforms

Section 3 of Chapter III of the DSA draft gives additional provisions applicable to online platforms, that are, as explained above, hosting services providers who stores and disseminates information to the public – and thus far the definition is the same of another hosting services provider– and bring together sellers and consumers. As defined by a report of OECD[19], examples of online platforms may be marketplaces, social media and searching engines, app stores, payments systems, creative content outlets and much more.

To recap the previous section, both hosting services providers and online platform have the obligation to put in place a notice and action mechanism along with the duty to provide the reasons of their action against a specific infringing content. In addition, online platforms need to ensure the safety and reliability of the products and services they offer and for this reason they have to comply with supplementary requirements.

- **Internal complaint-handling system**. Online platforms are required to establish an internal procedure that will allow the owner whose content has been removed or the access has been disabled to complain about the removal. Such inner complaint-handling system shall be easily accessible and user-friendly and the complaints have to be handled in a timely and diligent manner. In this Article, it is clear the desire to protect the content owner from unfair removals that may occur by mistake for instance by

[19] An Introduction to online platforms and their role in the digital transformation, OECD 2019, chapter 2: What is an "online platform"? https://read.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_19e6a0f0-en#page2

automated means. Providers shall inform the complainants, without undue delay, about the decision taken in respect of the complaint submitted along with the possibility of out-of-court dispute settlement and other redress means available.

- **Out-of-court dispute settlement.** The out-of-court dispute settlement is another mean available for the owners of the removed content (or whose access has been disabled) to assert their reasons if the dispute has not been solved yet. The recipients of the moderation action are entitled to select any out-of-court dispute resolution body, that shall be impartial and independent with respect the two parties of the controversy, it needs to have expertise and is capable of solving the dispute in a efficient, swift and transparent way. If the dispute is settled in favour of the recipient of the service, the platform have to reimburse the costs of the proceedings, otherwise if the final decision is in favour of the online platform, no reimburse is required to the recipient. Again, the Commission wants to protect the weaker part that is supposed to be the owner of the considered infringing content, in order to allow everyone that is firmly convinced about the unfairness of the removal to act against the abuse by the platform.

- **Trusted Flaggers**. The Regulation proposal wants to introduce the figure of trusted flaggers, specialised entities with specific experience in detecting illegal content online. Despite the figure of the trusted flagger had been mentioned for the first time by the Commission in 2017 in the Communication on 'Tackling Illegal Content Online' ("the Guidance")[20],

[20] 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, 2017 COM/2017/0555 final https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A52017DC0555

the Digital Services Act, if approved, will be the first legally binding document where this role will be considered. According to the Article 19 of the draft, the Digital Services Coordinator of the Member State where the applicant is established can acknowledge the status of *trusted flagger* to any applying entity, and not individual, under some conditions. The entity, as mentioned above, needs to have "particular expertise and competence"[21] in identifying infringing content, needs to be independent from online platforms and embody collective interests and, finally, has to notify illegal activities in a timely and objective way. Online platforms are obliged to treat notifications submitted by trusted flaggers with priority and without delay, since these figures are reliable when notifying a specific content as illegal and they can become a very useful mean to tackle infringing content online more quickly and effectively. The requirement to treat trusted flaggers with priority is without prejudice to the responsibility of platforms to decide upon all notices submitted diligently and without undue delay.

- **Suspicions of criminal intent.** Online platforms are also required to promptly inform competent enforcement authorities in case they "become aware of of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place"[22] as it is stated in the Article 21. The Commission brings as an example the offences specified in Directive 2011/93/EU of the European Parliament and of the Council. [23]

[21] Digital Services Act, Article 19.
[22] Digital Services Act, Article 21.
[23] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 is about combating the sexual exploitation and abuse of children and child pornography.

- **Traceability of traders.** Another novelty of the DSA is the introduction of the 'know your business customer' principle[24]. Online platforms that allow consumers to conclude a distance contract with external sellers shall first obtain information about the seller identity. In particular, platforms need to gain information about the name, address, telephone number and e-mail, the identification document or equivalent document, the bank account details and the registration number if the trader is recorded in a trade register or other public register. They also have to make reasonable efforts to assess the reliability of the information provided by the seller for instance by using freely online official databases or asking the traders to provide reliable documents. However, the platform cannot be required to carry out excessive costly investigations such as on-the-spot verifications. Whether the sellers didn't provide trustworthy documents, the platforms shall suspend the service of the seller until they fulfil their duties. At the same time a platform that made reasonable efforts cannot be held responsible for the trader. OP[25] providers, finally, shall share the information they obtained about vendors when it is required by a competent authority.

Again, Section 3 does not apply to micro or small enterprises that can be defined as online platforms. Articles 23 gives provisions about the additional information that online platforms have to include in the yearly reports (that are mandatory for all providers of intermediary services[26]). Finally, online platforms shall ensure transparency when they display an advertising banner, since the online advertising can contribute significantly to create an unsafe online environment. The advertising, in fact, can be illegal itself when it displays illegal information (for example the sale of counterfeit goods), it can offer financial incentives for the spreading of illegal content or activities,

[24] Briefing on the Digital Services Act, by Tambiama Madiega, March 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf
[25] OP stays for Online Platform.
[26] Digital Services Act, Article 13.

or it can be discriminatory and having "an impact on the equal treatment and opportunities of citizens" (Recital 52). To avoid the display of harmful content the Commission stated that online platforms shall make clear that what is displayed as an advertising, provide the name of the company or the person by on whose behalf the advertisement is displayed and give "information about the main parameters used to determine the recipient"[27] of the advertisement (Article 24).

3.3 Systemic Risks and Very Large Online Platforms (VLOPs)

3.3.1 Define very large online platforms

The DSA draft propose additional and more burdening provisions for very large online platforms, also called VLOPs, that are according to the Article 25 those platforms who reach a number equal to or higher than 45 million of average monthly active users. As it has already been explained in the explanatory memorandum, this number has been computed considering the 10% of the current Union's population and in the event the EU population increases or decreases the number will be adjusted. Given the rapid rate of growth that online platforms may have whenever successful, the Digital Services Coordinators have to verify at least every six months the number of recipients of online platforms established in the Member State they are responsible for. Then, the Commission shall ensure to keep updated the Official Journal of the European Union with the list of designated very large online platforms.

The Commission decided to burden VLOPs with the full scope of the proposed Regulation due to the heavier impact that they may have – and currently have – on the society and on the global economy if compared to other smaller online platforms. Furthermore, as a briefing of the European Parliament explains, the Commission believes that these platforms may have an important role and responsibility with regard

[27] Digital Services Act, Article 24

to the spreading of infringing and harmful content through the online environment[28]. The wide utilisation of such platforms can strongly affect the online safety for users, the online trading, the public opinion and behaviour, as well as small and medium enterprises businesses and much more. If left without an appropriate and proportionate control, very large online platforms can set the rules of the game and their impact on such a wide user base may lead to systemic risks that can damage the economy and society. The legislator task in this subject is particularly difficult since it has first to identify which are the not always so evident risks that may arise and then to mitigate the societal harm that very big platforms can generate.

3.3.2 Define Systemic Risks

Article 26 of the Regulation requires very big online platforms to identify, assess, analyse and evaluate, at least once a year, the systemic risks that my arise as a result of the dissemination of their services across the European Union. Specifically, the legislator identified three categories of systemic risks that the platform shall include while conducting the assessment.

(i) The potential misuse by users of their services with the purpose to **spread illegal content online** that may vary from pedopornography, to the sharing of copyright protected content or the sale of counterfeit goods. The dissemination of infringing or harmful content can become a systemic risk as long as the access to such content can be shared very quickly among users and reach a large-scale of people.

(ii) The **negative impact** of their services **on fundamental rights** listed in and protected by the Charter of Fundamental Rights[29], including the freedom of expression and information, the right to privacy, the

[28] Briefing on the Digital Services Act, by Tambiama Madiega, March 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf

[29] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2012/C 326/02) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=IT

prohibition of discrimination and the rights of the child. The legislator recognises the risk that, for instance, their algorithmic system may damage the freedom of expression by avoiding to display specific contents, maybe with the purpose to hinder competitors.

(iii) The **intentional manipulation** of their services, for instance by the creation of fake accounts, the use of bots or other automated systems with the purpose to mislead users or to gain a quick and wide spread of information that might be fake or even illegal. The result can be a negative effect on the protection of minors, on the public health and security and it can even affect electoral processes[30].

Therefore, very large online platforms are required to take appropriate mitigating measures that must be proportionate and effective. However, this process of risk-mitigation may not be as easy to reach as it seems. Platforms could need to consider whether to change and enhance the functioning of their content moderation or even to make adjustments to their content moderation algorithmic recommender systems and online interfaces with the purpose to discourage the spread of infringing content. The Commission in the preliminary notes of the Digital Services Act even suggests platforms to adopt corrective measures to disadvantage infringing behaviours, such as ceasing the advertising revenue for users who are involved with illegal information or "improving the visibility of authoritative information sources"[31] with the objective of helping in the fight against misinformation. Then it is obviously required, if necessary, a strengthen of the inner supervision on their activities and a close cooperation with trusted flaggers or other online platforms. The Commission strictly recommends the cooperation among platforms and particularly it suggest very big online platforms to contribute in helping other online platforms to identify and tackle systemic risks through, for instance, the creation of codes of conduct and crisis protocols. However, despite these innovative

[30] Digital Services Act, Recital 57 is fundamental to have a better understanding of what the legislator means by "systemic risk".

[31] Digital Services Act, Recital 58. In this Recital the Commission clarify what VLOPs can concretely do to manage and mitigate the systemic risks.

suggestions it will be very difficult to assess whether the very big platforms put into practice such recommendations effectively and with the concrete aim to minimize all the systemic risks they identified.

Another sensitive aspect related to the impact of very large online platforms is their potential power to undermine the free competition. Given the huge user base that VLOPs can reach, a lot of small and medium companies use them as their only channel to reach the segment of the market they need. Let's think for example about Facebook, who, in the first quarter of 2021, recorded in Europe 423 million monthly active users[32]. Most companies that want to expand their business online – and nowadays is almost the only way to stay competitive in the market – have to totally rely on these platforms since it is almost the only mean they have to reach their customers. If the platform unjustly deletes the advertising or suspend the SME's account it can significantly damage the company, and to counter this negative aspect the draft Regulation, as mentioned above[33], established for platforms the need to have a functional internal complaint-handling system (Article 17). However, aside from the removal or suspension as consequence of a mistake, the SMEs can be also damaged from the algorithm itself or from an unfair behaviour put in place by the VLOP that may favour a company over another or to hinder competitors at the expense of the freedom of competition. This risk is very concrete and, as stated above, difficult to monitor, since VLOPs should reveal substantial information about how their algorithm works and, then, disclose sensitive information to vetted researchers and regulators to allow an independent assessment.

3.3.3 Independent Audit

Very large online platforms have to be subject to a verification by independent experts to assess their compliance with the provision of the Digital Services Act, at least

[32] The source of data is Statista, Facebook: quarterly MAU in Europe Q4 2012-Q1 2021
Published by H. Tankovska, May 21, 2021.
https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/

[33] Article 17 of the DSA has been explained in the paragraph 3.2.3 "Additional provisions applicable to online platforms"

once a year and at their own expenses. These audits have to be independent from the platform, they need to have expertise with regard to the risk management and adequate technical skills, along with a "proven objectivity and professional ethics" (Article 28). Platforms are required to provide the auditor with the access to all the information and data necessary to carry out the audit adequately and, at the same time, auditors have to maintain the confidentiality about the information disclosed (for example trade secrets and restricted information about how the algorithm works). The auditor has to develop a report in which it states if the very large online platform complied with the Regulation's obligations and if the judgement is not positive it can give recommendations on which measures the platform should undertake to achieve compliance.

3.4 Digital Services Coordinators

The digital services coordinator is an independent authority designated by each Member State to supervise if the online platforms that are established in that specific State comply with the provisions of the Digital Services Act. Coordinators of different Member States have to cooperate with each other and with competent national authorities, with the Board and the Commission, they have to be impartial and transparent and have to be provided with all the means necessary to carry out their tasks properly. They will be granted specific oversight powers such as (at least) the power to require the sharing of specific information within a determined time period, the power to carry out on-site inspections and the power to ask explanations to anyone working for the platform. They can also order the cessation of infringements and impose fines whenever necessary. If the coordinator has reason to believe that a specific infringement persists despite the request to cease it and that it is causing serious harm, he can request the competent authority to order the temporary restriction of access of recipients concerned by the infringement (Article 41).

3.5 Penalties

The rules about penalties as concerns infringements by provisions of this Regulation are decided by Member States. However, the DSA draft will bring an important innovation to the online world: the principle of proportionality for fines.

We all remember the scandal who involved the giant online platform Facebook and the online marketing and consulting firm called Cambridge Analytica. In that case there was an illicit exchange of data that the society was not supposed to share and Facebook took a stand against this abuse only when the news became public knowledge. The case concerned also few Italian users and in June 2019 the Italian autority *Garante per la protezione dei dati personali*[34] applied a penalty of 1 million euros to the platform[35]. In the previous year, the same big online platforms was sanctioned by Antitrust, for a total amount of 10 million euros, for not informing users adequately, at the time of registration, of the platform activity of collecting their data for commercial purposes. These two cases are great examples of the inadequacy of the penalties imposed to such big online platforms, since 1 and 10 million euros are almost nothing for a platform who is supposed to have a revenue of more than 20 million dollars daily[36] and such modest sanctions do not have the feature of dissuasiveness.

With the introduction of the new Regulation the amount of fines will be defined case by case since they have to be "effective, proportionate and dissuasive" (Article 42).

[34] "Il Garante per la protezione dei dati personali" is an independent Italian administrative authority that ensure the protection of fundamental rights and freedom and the respect for dignity in the processing of personal data.
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9121352

[35] It is important to highlight that one month after the Italian *Garante della privacy* decision, on July 2019, for the same case who involved Facebook and Cambridge Analytica the Federal Trade Commission imposed to Facebook Inc. a fine of $5 billion (approximately 4,5 billion in euro).
https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[36] Source of data "Facebook, Inc. (Nasdaq: FB) today reported financial results for the quarter ended March 31, 2021" Menlo Park, Calif., 28 April 2021, source PRNewswire.
https://www.prnewswire.com/news-releases/facebook-reports-first-quarter-2021-results-301279518.html

However, the Commission also stated that the amount of penalties imposed to the platform cannot exceed the 6% of its annual income.

3.6 The Board and Enhanced supervision over VLOPs

This Regulation gives provisions for the establishment of the European Board for Digital Services (also called "The Board"), an independent group of Digital Services Coordinators with the purpose to ensure the effective coordination between Member States' Coordinators and the Commission, as well as a concrete help in the consistent application of the new measures.

Finally, the European Commission can intervene when an infringement has not been identified by the coordinators or when the infringement persists. The Commission will be empowered to carry out investigations, interviews and on-site inspections, it can ask platforms to adopt specific binding measures and if the non-compliance persists it can impose fines or periodic penalty payments[37].

[37] According to article 60 the periodic payments, whose amount can be at maximum the 5% of daily earnings, can be required, for instance, for violations of the Regulation, or for the supply of incorrect information or for until they consent to submit to an on-site inspection.

Part II

ILLEGAL CONTENT ONLINE

Chapter 4

The Spreading of Illegal Products online in the last years and during the Covid-19 Pandemic

In recent years, the sale of illegal products and contents has increased like never before. In 2019 the European Union Intellectual Property Office (EUIPO) published a detailed analysis[38] of the value, extent and economic and social consequences of the sale and distribution of counterfeit IP protected material inside the European market. The study estimated that in 2016 the volume of international trade in **counterfeit and pirated goods** represented up to 3.3% of the global trade, while in 2013 it was estimated to be the 2.5%,[39] . These data highlight a very significant growth rate for the market of illegal products, while, during the same time frame, the global overall trade was slowing down. It has been estimated that the five countries most affected by trade in counterfeit and pirated products at global level are the USA, France, Italy, Switzerland and Germany. Considering data about the European Union, the imports of pirated and counterfeit products represent up to 6.8 % of total EU imports. At the same time, the findings of another study[40] have revealed that the 45% of the GDP (gross domestic product) comes from IP-intensive industries[41] and that the same industries generate jobs for the 29% of total EU employment (and another 10% comes from industries strictly related to IP industries). As a consequence, the resulting damage caused to the economy of the

[38] The study has been published in 2019 but it considered the data gathered between 2013 and 2016. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf

[39] These data (3.3 and 2.5%) consider only traded counterfeit products and it did not include counterfeit products produced and sold inside the County as well as copyright protected digital content sold without the owner consent.

[40] The study is of EUIPO with the contribution of the EPO (European Patent Office).
EPO/EUIPO, IPR-intensive industries and economic performance in the European Union, third edition, September 2019. Available at: https://euipo.europa.eu/ohimportal/en/web/observatory/ip-contribution.

[41] Are industry that have an "above-average ownership of Intellectual Property Rights per employee" as defined in the report IPR-intensive industries and economic performance in the European Union of the EUIPO available at the link: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/IPR-intensive_industries_and_economicin_EU/WEB_IPR_intensive_Report_2019.pdf .

Internal Market is huge. Further studies have estimated that the sale of infringing IPR products has provoked losses for more than 83 billion euros per year between 2013 and 2017 as well as a loss of about 671000 jobs inside the EU. Moreover, the revenues deriving from this illegal market are estimated to be very substantial even though they are difficult to measure due to a lack of detailed data. The Organized crime groups (OCGs) that are involved with the sale of counterfeit products are attracted by the very high profits and the lower risks[42] connected to such illegal activity if compared to the others. Often these OCGs re-invest the profits deriving from IP infringement related activities to finance other more dangerous criminal affairs such as money laundering, forced labour and child labour, drug production and trafficking, human trafficking, manslaughter, illegal weapons possession and even to support terrorist organizations as has been revealed by a document of Europol and EUIPO[43]. The earnings also finance bribery and corruption, document fraud and cybercrime.

The nature of products subject to counterfeiting is of the most different types and they can be found in a growing number of industries even with regards to cutting edge products. Counterfeit products range from common consumer goods such as toys, cosmetics, clothing and footwear, to luxury items such as jewellery, expensive watches, designer bags and clothes, to IT products such as fake phones and batteries, to also industrial products like bulk chemicals and spare parts. [44] Although these products are causing a severe economic damage in the Internal Market, the harm caused to the safety of European citizens, to the public health and the environmental consequences are even

[42] The risks have to be intended as the risk in terms of likelihood to be discovered or caught, as well as the punishments that may derive whether detected.

[43] The report who revealed the linkages with the terrorist organisation is "IP Crime Threat Assessment 2019" available in the EUIPO archives: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report_Exec_Sum_EN.pdf

[44] Data comes from the report OECD/EUIPO (2019), Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade, OECD Publishing, Paris/European Union Intellectual Property Office. https://doi.org/10.1787/g2g9f533-en
available in the EUIPO archives at the link https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/trends_in_trade_in_counterfeit_and_pirated_goods/trends_in_trade_in_counterfeit_and_pirated_goods_en.pdf

more serious. The *Qualitative Study on the risks posed by counterfeiters to consumers*[45] of 2019 has highlighted that 97% of counterfeit goods reported as dangerous were evaluated to create a serious threat for the health of consumers. For instance, let's think about a farmer working with a non-compliance pesticide or herbicide, he can poison himself and create a serious harm to the health of people living in the same area, as well to consumers that will buy and eat the products he treated, not to mention the environmental damage that will result from the poisoning of soil, animals and groundwater.[46] The exposure to hazardous chemicals and toxins may cause both acute or long-term diseases and health issues whether the contact is immediate or a long-term exposure. The harms also include the choking hazard (mainly considering non-compliance toys for children), the risk of fire, electric shock (electronic devices) and many other types of injuries. Additionally, a very serious and actual harm to the public health derives from the sale of counterfeit pharmaceutical products. These are not only vitamin supplements and 'lifestyle' medicines[47] but also medicines who cannot be sold without a medical prescription, such as medicines used to treat severe diseases and antibiotics. Since the origin of such fake medicines is not known and they have not been subjected to any control, there is no guarantee that they actually contain the active substances in the required amount.

The sale of counterfeit medical products has experienced an exponential growth **during the Covid-19 pandemic** of the last year. OCGs have been able to exploit the shortages of the healthcare sector and the collective fear caused by the pandemic at their own advantage with an incredible promptness. In March 2020, the European Anti-Fraud Office (OLAF) identified more than 800 suspicious companies that were performing as intermediaries and providing the European Market with counterfeit pandemic-related products. Data have shown that illegal activities are highly adaptable

[45] EUIPO's Qualitative Study on the risks posed by counterfeiters to consumers – Available at the link: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers_Study/2019_Risks_Posed_by_Counterfeits_to_Consumers_Study.pdf

[46] Falde acquifere.

[47] Farmaci di conforto.

in terms of shifting focus from one product to another following the public demand, even quicker than official suppliers. During the Covid crisis illegal vendors have focused particularly on the sale of alcohol-based disinfectants and sanitisers, medical equipment (mainly non-compliant face masks and gloves), pharmaceuticals, fake corona test kits, unproven treatments and, lately, even counterfeit "known" vaccines[48]. All these goods are completely useless or does not comply with the safety standard required, putting at risk the lives of citizens as well as the safety of frontline workers and of the whole personnel of the healthcare and other essential sectors. Many medicines that were believed to have a positive effect on the treatment of the Covid-19 have been provided punctually on the illegal pharmaceutical websites as soon as the news of the discovering of a new possible treatment were mentioned by media. To bring an example, the illegal sale of *chloroquine*, a pharmaceutical product usually used to treat people affected by malaria that had shown some positive effect also for the treatment of Covid-infected people[49], has increased significantly immediately after the news of it being a potential cure spread to the public.[50]

Criminal organisation can certainly rely on a consolidated system of distribution channels which consists of diaspora communities[51] as well as online platforms and websites. The majority of illegal products, especially the pharmaceutical ones, sold during the pandemic are suspected to originate from India and China, two countries well-known for having many chemical and pharmaceutical industries[52]. Counterfeit products are trafficked using containers and, with the purpose of hiding the effective place of origin, they transit across different countries, and different Member States,

[48] Article of BBC "Coronavirus: Pfizer confirms fake versions of vaccine in Poland and Mexico", 22 April 2021, https://www.bbc.com/news/world-56844149

[49] The actual effectiveness of such treatment for Covid-19 is yet to be proved officially.

[50] Covid-19 Treatment Guidelines, October 9, 2020. Chloroquine or Hydroxychloroquine With or Without Azithromycin https://www.covid19treatmentguidelines.nih.gov/antiviral-therapy/chloroquine-or-hydroxychloroquine-with-or-without-azithromycin/

[51] Diaspora communities that are involved with the traffic of counterfeit goods usually maintain strong ties with their origin country an with criminal groups there.

[52] The source is a report of Europol about "Viral Marketing, counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic"
Available at https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic.

before reaching the ultimate destination. Diaspora communities that are involved with the traffic of counterfeit goods usually maintain strong ties with criminal groups in their original Country and they play a key role in the distribution of such goods inside the EU. Companies involved in the trade of counterfeit products are the most various and often have a front company[53] to hide their real illegal activities. In fact, the names and addresses of such companies are often used for a short amount of time, making very difficult for authorities to carry out the investigation and get to the organization at the top.

However, the most important distribution channels for counterfeit and IPR infringing products are online sales platforms. Particularly, during the last year, lots of new websites have been established with the express aim to sell counterfeit medical products. These websites are established bot in the surface web and in the dark web and they admit various payment methods such as the use of payment platforms, cryptocurrencies, credit cards and even payment on delivery. Some vendors even sell their products privately through social media or instant messaging application (i.e. Telegram).

Needless to say that the IPR infringements are not only related to counterfeit physical products but to **digital products** as well. During the Covid-19 pandemic criminal groups took advantage of the increasing number of online users as a natural consequence of the continuous governmental lockdowns. Particularly, criminals expanded their businesses to the illegal sharing and streaming of IPR protected contents, mainly illegally providing access to Internet Protocol Television (IPTV). Servers are often located in countries different from where the service is sold and for this reason the detection of the source is particularly difficult for competent authorities. These criminals selling digital content are also often organised at global level, with largely spread networks. Piracy of digital products is deleterious for the Internal Market, at least as much as the counterfeiting of physical products, or even more since it is more difficult

[53] Società di facciata.

to detect and fight piracy online. In the last years digital piracy increased a lot creating a real parallel economy that is causing a huge economic damage for the EU. A study of 2019 revealed that 60% of internet users regularly access to illegal content up to eleven times a month provoking an estimated loss of 2437 million euros[54]. The piracy in the music sector has been assessed to have created a damage of 29 billion USD in 2015 and it is expected that the economic loss will amount to approximately 53-117 billion USD in 2022. [55] Additionally, e-book readers that choose to draw on[56] illegal e-books are the 21% of all e-readers in Germany and the 92% of all e-book readers in China and Russia.[57] The spread of illegal content is also strictly related to the dissemination of malware and other harmful programs. These programs can enter in the device of users surfing in illegal websites without them even noticing it and trick them into revealing their sensitive data such as credit card details and other personal information. The recent study *Piracy Observatory and Digital Content Consumption Habits*[58] has revealed that most of piracy consumers[59] have serious difficulties in differentiating between legal and illegal websites and for this reason they are often not aware of being surfing in a not safe website. Another 57% of users of illegal websites stated they don't want to pay for some content they could not like after and more than 50% explained that they already pay for the internet connection and that the original content is too expensive for them. Another important issue that will be explained in detail in the next chapter is how people access to illicit contents. More than 60% of piracy consumers who participated in the study affirmed to use searching engines like Google, Being and Yahoo, while about 30% admitted to use direct downloading systems through portals or websites. The study also

[54] Data from "Piracy Observatory and Digital Content Consumption Habits"
Available at the link: http://lacoalicion.es/wp-content/uploads/executive-obs.piracy_en_2019.pdf
[55] Frontier Economics Ltd, "The Economic Impact of Counterfeiting and Piracy. A Report Prepared for BASCAP and INTA", p.28-33 (2017).
Available at the link: https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAPFrontier-report-2016.pdf
[56] Attingere a
[57] MUSO report, Available at the link: https://goodereader.com/blog/technology/online-pirate-websites-received-300-billion-visits-globally .
[58] See note 54
[59]60% of piracy consumers said they can't distinguish which platforms are legal and which are not.

highlighted a relevant aspect: in 2019 the access through Social Networks, mainly Facebook, YouTube, Whatsapp and Instagram, has increased.

The main source of income for illegal digital portals is advertising. When accessing the illegal website it is often filled with banner and pop-up ads that usually lead to betting websites, online gaming, sales platforms and so on (9 out of 10 internet users affirmed they had advertisings inside illicit websites). At the same time 2 out of 10 illicit websites ask users to pay to download the pirated content or to have access to it, obtaining in this way access to their payment details. A lot of piracy websites also require users to register, thus they have to provide the platform with their personal and sensitive data that the platform will likely store and sell later. [60]

The European Commission on December 14, 2020, the day before the official releasing of the Digital Services Act draft, published the document "*Counterfeit and Piracy Watch List*"[61] reporting the results of stakeholder consultations about the spreading of counterfeit and digital illicit content across marketplaces, service providers and online platforms. *The Watch List*, hence, contains the list of providers that have been reported as being involved with or benefiting from the sale of counterfeit goods and online piracy. The Commission also mentions in this paper the service providers, mainly big online platforms, that even without being directly involved with illicit activities play a key role in the dissemination of illegal content "for the reason they are reported to allegedly lag behind in efforts to combat piracy or counterfeiting"[62]. In this way the Commission wants to help and encourage all the involved parties, service providers and big platforms, competent authorities and governments, to take an active role in reducing and combating the availability of IPR infringing goods, both physical and digital goods.

[60] Data from "Piracy Observatory and Digital Content Consumption Habits"
Available at the link: http://lacoalicion.es/wp-content/uploads/executive-obs.piracy_en_2019.pdf
[61] Commission Staff Working Document "*Counterfeit and Piracy Watch List",* Brussels 14.12.2020
Available at the link: https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf
[62] See note 61

Chapter 5

Different types of illegal content online

The Watch List mentioned in the previous chapter highlight an enormous variety of different types of online service providers and physical markets – such markets more and more often rely on illegal online stores to sell their counterfeit products – that play a significant role in the dissemination of pirated goods and services. Particularly, the Commission identified:

- online service providers that offer or facilitate, directly or indirectly, the access to IPR-protected content, such as social media platforms, illegal streaming websites, piracy apps providers and many others,
- electronic commerce (e-Commerce) platforms, that facilitate the distribution of infringing physical products on the Web,
- illicit online pharmacies and online providers selling or facilitating the sale of all kind of medicines and healthcare-related products without any permission or quality control,
- physical marketplace selling counterfeit goods, that continue to be rampant around the world despite the increasing significance of online commerce.

It is important to underline that the interests in countering the dissemination of illegal content are not only of copyright owners. There are many stakeholders that are directly or indirectly involved because they are more or less damaged by falsification of goods and online piracy. Obviously, for what concerns physical goods, there are brand owners who have to face a huge economic loss as well as a damage to the brand image. Copyright holders, such as music producers, online magazines' owners and e-book writers, have a significant decrease in earnings due to the illicit consumption of their digital products. The financial damage also extends to all legal companies that are selling the same products available on piracy websites. The sale of counterfeit or sub-standard medicines and other health-related devices may cause a serious harm to public health.

Citizens that get damaged are not only those buying and consuming the counterfeit medicines, but also the whole community, let's think for examples about the risk of contracting Covid-19 deriving from the utilization of non-compliant facemasks or the severe consequences that may result from the wrong usage of antibiotics.[63] Not to mention the loss for the society in terms of R&D investments, since if the IPR is not properly protected companies will be encouraged to invest on innovation, the loss in terms of taxes that the governments would have reinvested for the benefit of citizens and the loss of jobs. Hence, even the final user consuming the pirated good has an interest – although indirect – to prefer the legal alternative.

However, illegal websites and the presence of copyright infringing content on platforms is mainly notified by copyright owners and organisations that represent them. The dissemination of illegal content on the online environment is so common that most users who come across it don't even think about notifying it to the competent authorities. This is one of the reasons why one of the most relevant provision of the Digital Services Act is the requirement for hosting services providers to introduce on their platform the notice and action mechanism, an automated user-friendly mechanism that should allow users to notify to the provider the presence of illegal content[64]. Moreover, online service providers as well as both the online and physical marketplaces listed in *The Watch List* all result to be located outside the European Union. This means that the owner of the website or platform that is at some level involved with the traffic of pirated contents is known or supposed to be resident abroad, independently of where the domain of the website is registered and of the residence of the hosting provider or the country where the service is offered. Hence, the owners of some illicit websites are very difficult to identify and detect, not to mention the possibility to effectively carry out a criminal prosecution. With the purpose to cope with this problem, the

[63] A misuse of antibiotics may lead to antibiotic resistance (bacteria are more resistant to antibiotics). The consequence is that an increasing number of infections, such as pneumonia, tuberculosis, gonorrhoea and salmonellosis, are becoming harder to treat.

[64] The notify and action mechanism has been deeply analysed in the previous chapter particularly at the paragraph 3.2.2 "Additional provisions applicable to providers of hosting services, including online platforms"

Commission, through the Digital Services Act, whether approved, will introduce a significant change in this subject. Digital service providers that are established outside the European Union who want to offer their services to citizens inside the Internal Market shall appoint a legal representative in one of the Member States where they provide their services. [65] The aim is to establish a *point of contact* between the providers and the authorities, in order to "ensure an effective oversight and, whether necessary enforcement"[66] as the DSA states.

Finally, it is important to highlight that The Watch List is a document without any legal effect. As mentioned earlier, the main aim is to raise awareness among the public, competent enforcement authorities, right holders, owners and governments and to help them to take the appropriate measures to tackle illegal content online. However, despite it not being a legally binding document, the *2018 Watch List*[67] (the first edition of The Watch List) managed to have a beneficial impact on the fight against the IPR infringing content dissemination. In fact, many right holders, service providers and authorities took actions against the illicit content on websites and platforms by obtaining the removal of the infringing content, by introducing a more efficient and stringent policy for sellers using their platforms (is the case of the Thai platform *Lazada*) or even by forcing illegal websites to shut down (for example *Openload* and *Torrentz2*).

5.1 Intellectual Property Infringements and Counterfeit Goods

The infringements in the sector of the Intellectual Property Right protected material have covered all kind of digital services and products as well as physical goods. However, the damage has been higher for some categories compared to others.

[65] The legal representative mentioned here has been treated in the previous chapter at paragraph 3.2.1 "Provisions applicable to all providers of intermediary services".
[66] Digital Services Act, Explanatory Memorandum, 2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY
[67] The Watch List considered in this paper has been published on December 2020. However, the first edition of The Watch List (Counterfeit and Piracy Watch List) was published in 2018.

The Creative Industry and the right owners of the audio-visual, broadcasting and music sectors have suffered a significant damage from piracy and for this reason they contributed considerably to the detection of pirate sites and illicit content. Particularly, the last years recorded an increasing proliferation of websites broadcasting sports events or providing unlicensed IPTV services. More and more often the links to access to these illegal websites are shared using the most popular social networks that are certainly blamed for a lack of effective control over this illicit traffic. Most of users in fact reported how some of these service providers facilitate piracy on their platform or don't take adequate measures to counter the IPR infringing content. Another debated role is the one played by Content Delivery Networks (CDNs). CDNs are proxy servers with a wide geographic distribution that store and replicate content and facilitate its transmission. Their role is very important for the correct and safe functioning of the Internet, but they have been criticised because the IP address of their clients is hidden and not accessible to the public, making the detection of infringing content providers more difficult.

Brand owners and brand associations have been damaged mainly by e-Commerce platforms and physical marketplaces. In the reported e-Commerce platforms, that are more than 60, it is in fact very easy to find counterfeit products of any kind: fashion, electronics, luxury items, toys and even chemicals and pesticides. Also in this context has emerged a growing concern about the role that some social networks played in the distribution of counterfeit goods. Particularly, social media platforms have been reported for the fraudulent and misleading advertisements that lead to illegitimate e-commerce websites. Furthermore, during the Covid-19 pandemic there has been an increasing number of new domains registered for illicit purposes and containing the most searched terms as "corona", "virus" and "covid". The European pharmaceutical industry counted more than 600 websites that were selling counterfeit medicines and sub-standard medical equipment.

Let's now analyse which are the various distribution channels and the extent to which they have been reported to be involved in the dissemination of IPR infringing contents.

5.1.1 Online Services providers offering or facilitating access to copyright-protected material

The place where the most consumption of pirated goods took place is the online environment. However, not all the involved websites and platforms play and active role in disseminating infringing contents. Illegal content providers have necessarily to rely on other related services for example payment networks (to obtain payments for their illegal activities), domain service providers, proxy service providers and caching services. It appears clear that many providers are just indirectly involved but still monitored for facilitating the access to pirate content. For some illicit platforms and websites the sale of pirate contents is the main source of income, while others carry on a legal business as principal activity but have some revenues or benefits in providing access to illicit contents.

The following list mentions the main categories of service providers that offer or facilitate the access to IPR infringing content. Moreover, some of the reported examples are providers who are indirectly involved but do not act to prevent illicit content providers from using their service or their response is not adequately strong.

- **Cyberlockers.** Cyberlockers play a fundamental role in the digital environment. They provide a cloud service and enable the uploading, storage and sharing of contents. Additionally, they create URL links that allow clients to access and download or stream the content. Some of these cyberlockers are used to encourage users to upload popular content by offering a reward based on the amount of times that the content has been streamed or downloaded by the public. This obviously encourage users to upload any kind of popular content irrespective of

copyright violation. Often the URL links that lead to the pirate content are shared and promoted using other channels such as social media, spam emails, other websites[68] and online blogs. Many cyberlockers have been reported by right owners primarily for not removing the illicit content they store despite the several notifications and secondly for hiding the identity and the location of their operators, not allowing authorities to find and persecute the natural person behind the infringing activity. With regards to the revenue stream of cyberlockers, 70% of revenues are estimated to come from the sale of premium accounts to consumers and 30% from the display of advertising banners. There are many cases of cyberlockers, whose content is accessible in Europe, who store and contribute significantly in the dissemination of IPR-protected content.

- *Uptobox* mainly store movies and videogames without the right owner consent. Many pirate websites contain links that re-direct to the content uploaded in *Uptobox.* When the infringing content is notified it takes usually more than 140 days to remove it. Then, the owner identity is hidden using a reverse proxy service and authorities are not able to link the illicit activity with a natural person.
- *Rapidgator* is a very popular cyberlocker operating from Russia that offers access to music, movies, books, games and TV programs and rewards users uploading popular contents. Even though it allows right holders to report the specific infringing content, it makes no effort to delete the same content located in another place or to prohibit the same infringing file from being uploaded again immediately after.

[68] The "Linking or Referring Websites" are analysed in detail later.

- **Stream-Ripping Services** are the primary source of pirated content at global level. They consist of apps, software and websites that allow consumers to download the file they want from online – legal – streaming platforms. In this way the user gets a permanent copy of the content without the owner consent. Hence, stream-ripping services are platforms capable to circumvent the protection measures that the most known streaming platforms apply to avoid their content from being pirated. It often happens that, in addition to the desired file, the stream-ripping service also disseminates malware putting the users' personal data security at risk[69]. Most known and utilized stream-ripping services in Europe are:
    - *Y2mate and YouTubeconverter* which, as the name suggest, enable users to copy the link of a YouTube video (and other video sites) , paste it and download the corresponding mp3 or mp4 file containing the desired music track or video;
    - *Savefrom* is a software that, after being installed in the user pc, allows him to download audio mp4 files from YouTube.

- **Linking or referring websites** are websites that bring together and organise a list that address to content stored on pirated sites. The content mainly consists of Tv series, movies and music. In detail, these websites often have a search tool that allow users to easily find the desired content. Then users are redirected to other sites where they can effectively stream or download the content. Some of these websites despite receiving notices to remove the infringing files did not answer and neither took down the content. The most popular websites belonging to this category and monitored in The Watch List are:

[69] Usually, malwares are downloaded by mistake while closing advertising pop-ups. The malwares may cause serious damage to the devices and most of them try to obtain the bank payment details of users.

- *Fullhdfilmizlesene* that is a Turkish website displaying movies (also pre-release movies) that are illegally stored in other websites. The owner's identity and location are hidden but the server is hosted in Turkey.
- *Seasonvar* is a Russian website which links users to more than sixteen thousand pirated files. It provides the access to illicit content for free and even with a premium subscription. Despite it being blocked in Russia and Spain it still is available in the rest of Europe.
- *Rlsbb* is a website that publishes movies' – and other type of contents' – reviews and articles, including links referring to cyberlockers who store the infringing content. The website barely take action to remove the links leading to the infringing content and, even if the link is removed, the website invites users to add new links in the comments. The access to the website has been blocked in some Member States (Italy, Belgium, Portugal and Denmark) but is still available in the rest of the EU.

- **Peer-to-peer and BitTorrent indexing websites** base their business on the peer-to-peer technology that allows users to share content. Particularly, users that are connected using a peer-to-peer system can serve as both server and client. In other words each user may receive and initiate an exchange of data, so every users that store a specific content can help others to download it. In this case, the website is a hub of links that allow users to download files stored in other users' devices. The most reported peer-to-peer websites in Europe are:
  - *The Pirate Bay.* It has various domains hosted in many different countries in order to remain operative even if the authorities blocked some of them (domains). It permits the sharing between

users of a wide range of content, from e-books to software, and it is one of the most popular BitTorrent websites used at global level.

- *Rarbg* is a website facilitating the access to music, movies, Tv programs and many other kinds of content. It actually acts to remove the infringing content after it has been notified but it does not take any measure to avoid that the content is uploaded immediately after the removal.

- **Unlicensed downloads sites** are websites where users can download the content they want in exchange for payment of a fee. In general prices on these illicit websites are considerably lower compared to their licensed competitors[70]. Moreover, users often are led to think that these websites are legal since they accept payments with the most known payment systems (PayPal, Visa, Mastercard, etc.) or they display the official covers for music albums or movies. Two popular examples of websites permitting the download of unlicensed material are:
  - *Music Bazaar.* It is one of the most popular unlicensed pay-per-download websites selling music tracks. Users have to register and create an account, then they can use the search bar to find the tracks they want to download. Once they have paid for a specific content, they have it available on their account for a limited period of time during which they can download the content on as many devices as they want.
  - *Sci-hub.* It is a website that provide access to a huge amount[71] of academic papers, reports and articles. The documents are obviously made available without any authorisation from the

[70] Competitors who pay royalties.
[71] It is estimated to have an availability of 55-60 million documents.

legitimate right holders. The website presumably obtains the access to the infringing content by using the accounts of users who have been subject of phishing frauds[72].

- **Piracy Apps' Websites** are websites where users can find apps that provide access to pirated content, mainly movies, TV series and programs. An example can be *Popcorn Time*, a piracy app that provide access to a wide array of series, cartoon and movies without the legitimate owner consent.

- **Hosting providers** are services that provide websites with the infrastructure necessary to operate. Actually, most of hosting providers have policies against the IPR infringements and other illicit activities and promptly act against websites using their services for piracy activities. However, other hosting providers have been reported for a lack of response when informed of illicit activities carried out using their services, for example *Private Layer*. This provider not only hosts pirate websites, but also does not take any action when right holders notify the illicit content.

- **Unlicensed IPTV services.** As mentioned earlier, this category refers to all the websites or mobile applications that offers unauthorised access via streaming to a wide array of TV channels, including premium content and sport events. These services are usually provided in exchange for the payment of a subscription fee and for this reason often users are not

[72] *Phishing* is a computer fraud that consists in sending an e-mail with the counterfeit logo of a credit institution or an electronic commerce company, in which the recipient is invited to provide confidential data (username and password, credit card number, etc.), stating the request is necessary for technical reasons. Often, with regard to Universities and other institutions, students as well as academic personnel have been victim of phishing frauds. For instance, emails claiming that access to the academic library was going to expire and it was required to urgently "update" the login credentials through the provided link.

aware of the illicitness of the streaming service. Furthermore, since most of the streamings are broadcasted on apps installed on the users devices (rather than online) and since these apps are available in "unofficial" app stores or websites it is very difficult to monitor the actual extent of the dissemination of this service. The most active unlicensed IPTV services in Europe are *King365tv.com* and *VolkaIPTV.com* and both provide access to international Tv channels and video-on-demand (VoD) content without rightful permission.

- **Social Media.** Social media are obviously indirectly involved with the dissemination of IPR infringing content since the sharing of pirated content is not their main activity nor their business model is based on copyright infringing activities. However, users often create and use groups on social media platforms for the sharing of IPR infringing contents or even more harmful illicit content. Especially during the year of the covid pandemic the authorities reported an increasing number of this kind of groups on social platforms. As broadly explained in the previous section of this paper, social media play an unwanted but fundamental role in the dissemination of unauthorised content and often their reaction to counter piracy is too soft. Some platforms more than others have been mentioned for a lack of efforts to combat piracy and illicit content, such as:

    - *V Kontacte.* VK.com is a Russian social network with more than 500 million of active accounts. Users on this platform can easily access groups where they can share as well as upload and download unauthorised content. Due to the numerous reports by right holders, the platform acted to prevent external applications and websites from accessing and downloading the content stored

on their servers. However, V Kontacte still stores a high number of infringing files and it not always takes proper action to take down content when it is notified. The platform has been monitored for long time and, although much can still be done, it did improve in efforts to protect copyright holders for instance by arising awareness among its users through the notification of the need to respect copyright before every upload of a file. V Kontacte received an impressive number of 1.75 billion visits in June 2020 and has been ranked[73] as the 14th most trafficked website at global level.

- *Telegram.* Telegram is a desktop and mobile app offering an instant messaging service. The application allows the creation of public channels accessible to an unlimited number of users who are similar to social media. Often these channels are used to share unauthorised IPR infringing content such as movies, tv series, documents and to promote links to illegal external websites. Recently Telegram has also been reported for the presence of numerous groups storing child pornography and non-consensual pornography (also known as *revenge porn*), particularly the case of revenge porn will be analyse in Chapter 6 paragraph 6.1.

5.1.2 E-commerce Platforms

During the last year, due to the COVID-19 pandemic, people preferred to make purchases online rather than going to physical shops as a natural consequence of both the governmental lockdowns and to reduce the risk of being infected. Hence, the distribution of merchandise on E-commerce platforms increased exponentially, as well as the sale of counterfeit goods using them as the main distribution channel. Many

[73] SimilarWeb rank.

merchants even sell these counterfeit products inducing the customers to believe that they are genuine. The authorities during the covid crisis had difficulties in tracking down and confiscating the counterfeit goods since more and more often they were shipped in small parcels, via post or courier services. These products are a serious threat for the citizen's health as well as for the European market, particularly because there is the concrete risk for consumers to buy goods that may not offer any protection, that may be hazardous or of poor quality. In addition, they damage the economic interests and brand image of the EU reliable companies not to mention the fact that they make e-commerce platforms looking like a not secure place to make purchases.

On 1 March 2018 the Commission published the "Recommendation on measures to effectively tackle illegal content online"[74] in order to contrast the many problems caused by this threat and in order to detect illegal content, delete it and prevent it from reappearing. The Recommendation encourages online platforms to put in place procedures and more effective tools to identify and erase illegal content and urges them to cooperate more with trusted flaggers, enforcement authorities and right holders. The main concepts of this Recommendation have also been embedded in the Digital Service Act that, whether approved, will have legal value. During the public consultation, stakeholders pointed out that some e-commerce platforms should adopt more effective measures against sellers that use their platforms to sell counterfeit products. In this regard, the Commission through the DSA introduced the implementation of the 'know your business custumer' principle by asking providers to gather information about the identity of vendors selling products on their platform[75] – .

However, some e-commerce platforms more than others have been mentioned in The Watch List and are monitored for different reasons: they have a wide supply of counterfeit merchandise, they do not carry out effective enough measures to block

[74] Commission's "Recommendation on measures to effectively tackle illegal content online" is available at https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[75] This concept has been analysed in detail in Chapter 3, paragraph 3.2.3 "Additional provisions applicable to online platforms", Traceability of traders.

fraudulent offers and do not adequately cooperate with authorities and right holders. Some of those platforms have been reported also for having a lack of clarity in their terms of service about the prohibition of selling counterfeit goods.

On the other hand, some efforts have been done by many of the most known e-commerce websites, such as *Amazon*, *Alibaba* and *eBay*, to tackle the dissemination of illegal vendors using their platforms to reach the public. Therefore, even if a considerable quantity of counterfeit goods remains still available on their websites, these platforms actually implement measures to discourage the sale of illegal products. Furthermore, they are actively contributing to the development of new tools and methods to protect IPR more effectively and are willing to cooperate with right holders and competent authorities. Among the above-mentioned platforms, *Alibaba* is the most reported for issues related to the sale of counterfeit goods, in second place is *Amazon* followed by *eBay*. Then, in order to cooperate with law enforcement authorities, Europol and right holders, *Amazon* created the "Counterfeit Crime Unit" an online IPR investigative group. Finally, even if these have been removed from the Watch List, stakeholders keep demanding a to strengthen controls. Especially, stakeholders require platforms to (1) improve automated systems and tools that can link the details of new sellers to accounts that were already removed or restricted, (2) set a limit to the amount of identical goods that can be sold by a single account that is not a business seller and, in general, (3) control more accurately the identity of vendors that do sell a high quantity of products. Stakeholders also think that operators on these platforms should guide the seller into uploading higher quality and more specific photos of the product, in order to discourage the use of catalogue photos and modified images.

In addition to the above-mentioned well-known e-commerce platforms, many others are still monitored by the authorities for keeping infringing IPR. Some of these are:

- *Bukalapak*. The e-commerce platform *Bukalapak* is the most used in Indonesia. Many stakeholders reported this platform because apparently

it sells any kind of counterfeit goods, such as clothing, electronics, tobacco, industrial products and, more recently, even counterfeit pesticides. The greater part of the goods is manufactured in China. Particularly, *Bukalapak* has been reported for not implementing effective enough measures to block and remove infringing offers, for the excessively long amount of time necessary to delete these offers and for not banning the utilization of specific keywords, like "replica". In his own defence the platform stated that in its Terms and Conditions the sale of IPR-infringing goods is expressly prohibited and that the platform often takes down infringing offers as well as cooperates with authorities.

- *Dhgate* is the biggest business-to-business e-commerce platform in China which sells large quantities of any product category. It has been reported for a rampant lack of control over sellers and products as well as the lack of willingness to cooperate with the enforcement authorities.
- *Tiu.ru, Prom.ua, Bigl.ua, Deal.by and Satu.kz* are different e-commerce marketplace owned by the same company, the *EVO Company Group*, who sell mainly electronic products, car spare parts, material for repair but also clothing, footwear and books. These websites have been reported for the unreasonable administrative requirements and time necessary to take down the IPR-infringing offers.
- *Mercado Libre* is one of the most popular e-commerce platforms in South America. As the previous marketplaces, *Marcado Libre* has been reported for a lack of effective response when notifications are submitted as well as for the unjustified amount of time necessary to have the removal request approved. In response to the numerous complaints by right holders, in December 2019 the platform “launched an improved notice and takedown procedure”[76] – as it has been reported by The Watch List

[76] Commission Staff Working Document “Counterfeit and Piracy Watch List”, Brussels 14.12.2020 Available at the link: https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf

of 2020 – that should facilitate the removal and the reduce the time of response.

5.1.3 Online Pharmacies and Counterfeit Pharmaceuticals

The trade of counterfeit pharmaceuticals has increased dramatically in the last years since criminals are attracted by the high profit margins, the difficulties in being detected, the soft penalties whether identified and the ease in distributing such small products[77]. The global trade of counterfeit medicines is estimated to have reached EUR 38.9 billion in 2016, putting public health at risk and enriching criminal organisations while damaging the pharmaceutical industry. The most sold counterfeit pharmaceuticals are lifestyle medicines, sexual impuissance medicines, painkillers and antibiotics but the illicit traffic includes also life-saving medicines and pharmaceuticals to treat serious diseases such as HIV and AIDS, diabetes and cancer. There is no guarantee of the quality of these falsified medicines that may contain too much, too little or none of the active ingredients with the medical properties, creating in this way a serious threat for the public health. The Covid-19 pandemic of the last year increased the illicit traffic of counterfeit pharmaceuticals even further, adding to the already existing offer of counterfeit products a wide supply of sub-standard medical equipment (i.e. ventilators), individual protection equipment (face masks, gloves), covid-test kits and even unproven Covid-19 treatments. As already mentioned, during the first months of the pandemic the number of online pharmacies has grown exponentially. Particularly, in March 2020 a huge number of websites selling counterfeit pharmaceuticals and pandemic-related products were registered using in the domains words as “covid” “corona” and “virus”, 90% of which were registered anonymously making the identification of the owner very difficult. To make enforcements authorities’ work even harder is the reluctance of domain registrars to cooperate and suspend the domain name of illicit pharmacies,

[77] More than 95% of seized counterfeit pharmaceutical products has been shipped through postal services.

while social media have been very reactive in the removal of illicit offers on their platform. Usually, a multitude of illicit websites selling counterfeit products have at their source the same well-established illegal online pharmacy and most of these websites just re-address the user to the main illicit vendor. At the same time, online pharmacies have at their disposal a wide array of domains and some of them are just "sleeping" websites ready to be used when an active site is detected and shut down by authorities.

Hence, to fight illegal pharmacies, authorities have to focus on the domain name registrars that continuously provide criminals with the means to keep running their unauthorised activities. The infringing registrars that have been reported are:

- *CJSC Registrar R01*. It is a registrar that despite the many notifications keep serving *EVA Pharmacy* and *PharmCash*, two online pharmacy networks who sale counterfeit pharmaceuticals as well as medicines without the required prescription. The network consists of a multitude of referral websites that lead the user to the main less visible pharmacy. The registrar did not cooperate with authorities nor right holders despite the orders to discontinue the illicit networks.
- *EPIK Inc*. It is the registrar providing domains to *RxProfits*, another online pharmacy working thanks to a network of referring websites. Again, these websites (approximately 500) re-direct the user to a less visible site[78] where the counterfeit pharmaceuticals are sold. The registrar stated that it act when ordered by courts but that it is unable to determine whether the registrants notified by right holders are actually involved into criminal activities.
- *ZhuHai NaiSiNiKe Information Technology Co*. It is a registrar providing domains to *PharmaWeb,* an illicit online pharmacy network that mainly ship to US but medicines are distributed also in other countries, such as Italy, United Kingdom, Switzerland and South Africa.

[78] The *anchor site.*

5.2 Child Sexual Abuse

As reported by the annual reports of INHOPE, between 2018 and 2020 the number of notifications of child sexual abuse material (CSAM) in Internet has increased significantly. Although it is believed that this growth has been influenced by the pandemic and the numerous lockdowns worldwide, there is not reason to suppose that this illicit trend will decrease in the next future. In addition to the horrible rampant cases of sexual abuse material having as object children under the age of 13 (about 77% of reported cases in 2020[79]), there has been a growth of self-generated content with regards to pubescents between 14 and 17 years. The victims are often, but not only, girls that are not aware of the risks that may derive from "sexting" and from the live-streaming of explicit behaviours through, for instance, social networks. At the same time, the encryption of digital communication services makes difficult for authorities to detect and counter the dissemination of illegal material in general and CSAM as well. Another relevant problem that does not allow to have a homogeneous removal of CSAM is the fragmented legislative framework worldwide. In fact, besides the worst child abuse material that is considered illegal in every country, there are other "categories" such as the self-generated sexual material, the digitally generated images representing a minor involved in a sexually explicit context, drawnings and textual descriptions of child abuse that can be considered illegal or not on the basis of the national law. [80]

With regards to Europe, the European Union for the period 2020-2025 planned a strategy to fight child sexual abuse and CSAM more effectively. As we mentioned earlier the Covid crisis worsen the problem under many aspects, first of all for minors who live with their abusers. Then minors spent more time surfing online, without a

[79] Data have been published by INHOPE Association in the Annual Report of 2020. Available at the link https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf

[80] According to the INHOPE analysis (see footnote 79) a more complete list of the different sub-categories is: Drawing/manga/artistic interpretations of CSAM, Digitally generated CSAM/realistic images representing a minor engaged in sexually explicit conduct, Apparent self-generated sexual material, Sexualised modelling or posing, Sexualised images of children, Text depictions of CSAM, Fictional text depictions of CSAM, Manual on Child Sexual Abuse, Declaration of committing Child Sexual Abuse, Laud of paedophilia or child sexual abuse.

proper supervision from parents, increasing the risk of being contacted by online predators. Finally, the general increase of time spent online also increased the demand for child sexual abuse material (in some Member States the growth has been of 25%[81]) as well as the production of such material that obviously led to new abuses. Most of time the CSAM is shared using messaging platforms, groups on social media and less often emails[82]. Unfortunately, the end-to-end encryption besides being fundamental to guarantee the privacy of users in the online environment also provides criminals with a useful tool to hide their activity and hinder the investigations. The European Union recognises the need to face this issue, while balancing two fundamental rights such as the protection of personal data and child protection. The EU strategy consists of eight initiatives, all of them with the aim to detect and counter child sexual abuse material more effectively.

(1) The implementation and a better development of the current rules, particularly with regards to the *Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography*[83]. The Directive 2011/93/UE has been the first tool of the EU with a global approach to lead all the Member States in the fight against child pornography. The crimes considered are both offline and online such as the vision and dissemination of online child sexual abuse material, grooming[84] and sexual abuses via webcam. Although Member States have made considerable progress in implementing the Directive since its release, they still did not fully achieve an effective implementation of all its aspects. For this reason, in 2019 the Commission opened infringement procedures against 23 Member States that did not satisfyingly comply with the directive. Going into in-depth analysis, Member States still have difficulties in

[81] Europol, Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19 June 2020.
[82] A recent investigation in Germany has detected a chat group with more than 30000 users sharing CSAM, advice on how to lure the minors and on how to produce new explicit material.
[83] Directive 2011/93/UE, Available at the link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0093
[84] Grooming is soliciting children for sexual purposes.

prevention programs for people who committed or think they are going to commit an abuse, in defining crimes and the level of penalties and in supporting and protecting child victims.

(2) Ensuring that EU laws enable an effective response against child sexual abuse. While evaluating whether the above-mentioned Directive shall be updated, the Commission acted promptly to solve the conflict between the possibility of online companies to conduct voluntary investigations to detect child pornography and the need to protect the privacy of online users. In particular, the e-Privacy Directive of 2002[85] ensures the protection of privacy in the electronic communication sector. Article 15 establishes a derogation from its provisions, stating that Member States can adopt measures to restrict the right to privacy (in particular, with regard to article 5, 6, 8 and 9 of the Directive) when it is necessary and required for the safeguard of national security, for defence and public security and for the "prevention, investigation, detection and prosecution of criminal offences". Hence, the e-Privacy Directive does not provide online companies with a legal basis to voluntarily look for child sexual abuse material unless Member States expressly and specifically adopt measures according to the conditions stated in the Article 15. However, the Commission recognised the importance of own-initiative investigations carried out by online services providers in order to detect child sexual abuse material, report it to the authorities, identify the responsible and investigate them to prevent further abuses. Furthermore, the Commission is considering to make a sector-specific legislation to counter child sexual abuse online better, particularly it aims to create mandatory obligations for the detection and notification of that illegal material. In the

[85] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

meantime, the Commission proposed a Regulation[86] to temporary derogate the provisions of the e-Privacy Directive and allow number independent interpersonal communications service providers[87] to use technologic tools for the processing of user personal data with the unique aim to counter child sexual abuse online.

(3) Identifying legislative gaps, best practices and priority actions. When Member States implemented the directive to counter child sexual abuse, few of them integrated additional laws not mentioned in the directive, making it clear that the directive could be further improved. [88] With this purpose the Commission is willing to work to identify the legislative and implementation gaps, considering the issue of encryption and anonymity as well as new issues that could arise.

(4) Strengthen the law enforcement efforts at national and EU level particularly with regards to the communication and collaboration among involved parties. In order to achieve a better efficiency in countering child sexual abuses, the Commission realised the need empower Member States with specialised units and to engage them with international investigations. Furthermore, the Europol will set up an *Innovation Hub and Lab* to provide Member States with better technical tools and knowledge, particularly with regards to digital investigations.

(5) Enable Member States to provide a better protection for children through prevention. Prevention was one of the weakest points identified by the

[86] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online. https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0568/COM_COM(2020)0568_EN.pdf

[87] On 21 December 2020, the European Electronic Communications Code (EECC) entered into force replacing the definition of electronic communications services with a new definition that includes number-independent interpersonal communications services. Since this date, such services will be covered by the e-Privacy Directive not allowing them to conduct own-initiative investigations as we mentioned.

[88] An example can be the requirement for professions that involve a strict direct with children to request the criminal records.

Commission. To solve it, the Commission is preparing a prevention network to guide and support Member States. The prevention plan is addressed to both "offenders and people who fear that they might offend"[89] (particularly it is willing to analyse better the circumstances in which a person with a paedophilic disorder can effectively become an offender) and children (through the need to raise awareness of the risks and teaching them of to react).

(6) The establishing of a European centre to prevent and counter child sexual abuse. The Commission will start immediately to work for the creation of such centre, to provide Member States with an holistic support as well as a coordinated and multi-stakeholder approach gathering information and experience from similar centres worldwide.

(7) Galvanise industry efforts to ensure the protection of children in their products. Some providers of specific online services are in the best position for the detection of child abuses online. One above all, Facebook, in 2019 sent about 16 million reports (the 94% of the total child abuse notifications in the same year). However, the company announced its willingness to introduce the end-to-end encryption that will reduce the amount of reports significantly since the actual detection tools cannot work on communications exchanged using such encryption. At the same time, the Commission believes that certain online providers, given their important role in the sharing and dissemination of child sexual abuse material and in the effective detection of abuses on minors, shall take responsibility for protecting kids according to the EU fundamental rights. For this purpose, the Commission will work with the *EU Internet Forum*[90] to investigate about the possible technical solutions

[89] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU strategy for a more effective fight against child sexual abuse 24.07.2020

[90] The EU Internet Forum since 2015 has a key role in the fight against terrorism online and it is composed by the EU Home Affairs Ministers, high-level representatives of major internet companies, the European Parliament and Europol.

that could allow the detection of child sexual abuse online despite the utilisation of end-to-end encrypted communications, as well as other possible solutions for the operational and regulatory challenges that may arise.

(8) Enhance protection of children globally through multi-stakeholder cooperation. Since the child sexual abuse is a global problem, it requires a global strategy. The EU will keep encouraging other countries to develop more effective plans to counter child sexual abuses offline and online. Particularly it will keep contributing to increase global standards by supporting the cooperation through the *WePROTECT Global Alliance*, and through dedicated funding.

5.3 Terrorism

On April 29, 2021 the European Parliament and the Council approved the Regulation 2021/784[91] about how to address the dissemination of terrorist content online and it shall apply from 7 June 2022. The proposal was submitted by the Commission in September 2018, given the very actual problem of the terrorist content online and the serious harm that it may cause to the society as well as the negative impact on the reputation of online platforms and the damage it causes to the trust that citizens have on the Internet. In fact, the spreading of terrorist content has contributed to the radicalisation of the so-called "lone wolves" and inspired terrorist attacks inside the EU. Online services providers have put in place different measures to detect and counter terrorist content on their platforms. Besides acting when required by the competent authority, some of them carried out voluntarily investigations and followed the guidelines of the *EU Internet Forum* that promoted the cooperation between Member States and hosting services providers. However, since the collaboration with

[91] REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=en

the *EU Internet Forum* is voluntary, not all the providers are actively participating in it, and in general the efforts carried out by platforms are not tackling the problem with the promptness and effectiveness required by the delicate situation. For this reason, the Commission recognised the need to give "a minimum set of duties of care on hosting providers"[92] since the fundamental role that such providers have in the dissemination of terrorist content online and the power they have to put in place effective measures to detect, identify and remove it.

The new Regulation at Recital 11 gives a detailed definition of what can be considered "terrorist content". Terrorist content is "material that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences, solicits someone to participate in activities of a terrorist group, or glorifies terrorist activities including by disseminating material depicting a terrorist attack"[93]. The definition includes also content that gives instructions on how to create and use explosives and weapons or other dangerous substances. The terrorist content may consist of images, audio and video recordings, text and live transmission of terrorist offences. The content shared for research, educational, journalistic and artistic purposes shall not be considered terrorist content, as well as radical opinions that may be expressed during a public debate.

The provisions of the new Regulation applies to all providers of information society services who provide storage of information and disseminate it to the public[94], hence "mere conduit" and "caching" services providers are excluded. Since often such terrorist content is disseminated by providers established in third countries, the

[92] Proposal of the Commission for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online, 12.9.2018. https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF

[93] Recital 11 of REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=en

[94] disseminate to the public means making the information available to a potentially unlimited number of persons.

Regulation applies to all providers that offer their services inside the EU, irrespective of the place of establishment of the provider.

The Regulation establishes that each Member State has the power to issue a removal order, hence each Member State's competent authority can order to a hosting service provider to remove a specific content or disable the access to such content in all the EU. The hosting service providers have to remove the content as soon as possible and in any case within one hour from the order[95](Article 3). The Commission decided to harmonise the removal procedure for all the Member States and to require an almost immediate removal because the promptness of the action is essential to avoid the further dissemination of a content that can potentially cause serious harm to the society. The order to remove the content must include the identification details of the authority that ordered it, a detailed motivation of the reason why such content is considered terrorist content, the exact location of the content (url address), the legal basis of the removal, the date, time stamp and electronic signature of the competent authority and information about the redress available. The Regulation also requires hosting services providers that have been exposed to terrorist content to include in their terms and conditions provisions against the use of its services for the dissemination of terrorist content and to adopt specific measures to tackle terrorist content, such as the use of staffing or technical means/tools, an user-friendly mechanism to allow users to notify alleged terrorist content and other means. At the same the legislator repeat the necessity to balance the need of having a prompt removal with the need to protect the fundamental rights such as the freedom of expression, the respect for private life and protection of personal data. Again, like in the Digital Services Act and the Directive 2000/31/CE, there is not for hosting service providers a general obligation to monitor the content they transmit or store.

The hosting service providers which had to take action against the dissemination of terrorist content have to create and make available to the public a "transparency

[95] Article 3 of the REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online.

report" including data about the measures it implemented, the number of items of terrorist content removed or disabled, the complaints received and other information (Article 6). Also, competent authorities are required to publish annual transparency reports containing information about the number of removal orders issued, the number of removal orders who needed a further administrative control and other information.

5.4 Illegal Hate Speech

The need to tackle illegal hate speech online is a particularly controversial issue that has been criticised for the concrete risk to restrict freedom of expression. Article 10 of the Human Rights Act of 1998 protects the freedom of expression, however it also states that, since that freedom carries with it responsibilities and duties, it may be subject to conditions and restrictions as well as penalties to protect the national security, public safety and to prevent disorders or crimes (Article 10)[96]. Later, in November 2008 the EU Council published an Act on combating racism and xenophobia and providing what is considered a more detailed definition of hate speech, particularly it states that the conduct of who publicly incites to violence or hatred against a group of people defined by religion, race, skin colour or ethnicity is punishable (Article 1)[97]. Such definition has been further integrated by Member States that extended it to other grounds for instance gender identity, sexual orientation and disability. At the same time, the Commission in the "Code Of Conduct on Countering Illegal Hate Speech Online"[98] emphasized the necessity to protect the right to freedom of expression, that, as stated by the European Court of Human Rights, 'is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of

[96]Human Rights Act 1998.
https://www.legislation.gov.uk/ukpga/1998/42/schedule/1

[97] ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY, COUNCIL FRAMEWORK DECISION 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:328:0055:0058:en:PDF

[98] Code of conduct on countering illegal hate speech online, 30 June 2016.
https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

indifference, but also to those that offend, shock or disturb the State or any sector of the population'[99].

According to ECRI, the European Commission against Racism and Intolerance, countering all the forms of *hate speech*, online and offline, is fundamental because it can lead to acts of violence and conflict, threatening the safeguard of human rights and the cohesion of a democratic society. Nevertheless, it is also essential to keep a balance between countering hate speech and protecting freedom of speech.

With the purpose to prevent and tackle the dissemination of illegal hate speech in the online environment, in 2018 some of the largest online companies together with the Commission agreed on the creation of the "Code of conduct on countering illegal hate speech online". The initial signatory companies were Microsoft, Facebook, YouTube and Twitter, followed by Instagram, Snapchat, Dailymotion, Jeuxvideo.com and TikTok between 2018 and 2020. The signatory online companies are committed to (1) clarify on their terms and conditions that they do no tolerate incitement to violence or hate, (2) put in place an effective procedure to check notifications of illegal hate speech on their services, (3) review the notification within 24 hours and (4) remove or disable the accesso to such content whether necessary. However, since the codes of conduct are not legally binding, the crime of "illegal hate speech" will be regulated by the Digital Services Act, whether approved. Since its approval, the obligations to counter illegal content online (including illegal hate speech) will apply to all the providers of intermediary services and not only to those who took part in the above-mentioned Code of Conduct. Until then, the implementation of the Code of Conduct will be assessed through monitory rounds that highlights how much this "tool" is needed. In fact, the last report showed that companies managed to deal with the 90% of reported content within 24 hours, and more than 70% of such content was removed because it actually fell under the definition of illegal hate speech.

[99] CASE OF HANDYSIDE v. THE UNITED KINGDOM, paragraph 49.
Available at the link: http://hudoc.echr.coe.int/eng?i=001-57499

Chapter 6

Not illegal but harmful content online

The Digital Services Act defines "illegal content" as what is illegal under the EU law or the Member States' law and clear examples of illegal content has been mentioned in the previous chapter. Nevertheless, there is a broad category of content that, even if it is not considered illegal according to the definition of "illegal content", can cause harm to both an individual and the society. A definition of "harmful content" is given in a Communication of the Commission of 1996[100], and it is defined as "various types of material" that "may offend the values and feelings of other persons: content expressing political opinions, religious beliefs or views on racial matters etc." With years the idea of harmful covered a broader range of content, for instance the spreading of misinformation online, cyberbullying and non-consensual pornography. The legislator decided not to include the "harmful content" category in the removal obligations of the DSA, since according to the stakeholders it could lead to a serious restriction of the freedom of expression. At the same time, the harmful content surely falls within the category of the systemic risks that Very Large Online Platforms shall assess and counter, however the DSA does not give a definition of "harmful content" and it does not provide the details of how VLOPs are supposed to tackle it. On the other hand, the DSA leaves the responsibility to tackle what is considered not illegal but harmful content to the "Codes of Conduct", encouraging and giving provisions for the creation and implementation of such voluntarily codes (particularly in the articles 35 and 36 of the DSA).

[100] Illegal and harmful content on the Internet, Communication from the Commission, 16.10.1996 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF

6.1 Non-consensual pornography

A very actual problem that raised concerns in the last years is the spreading of *non-consensual pornography* or *non-consensual diffusion of intimate images (NCII*). It can be defined as the sharing or dissemination of private images or videos depicting the victim naked, posing in a sexual provocative way or engaged in a sexual behaviour, without the victim consent. Often, in addition to images, it is provided also the name, the social media account, the phone number or the address of the victim or other personal data, always with the purpose to cause distress or embarrassment to the victim. In the last years the phenomenon has increased significantly and during the year of the covid pandemic many new groups sharing private images of girls and even under-age girls appeared online, particularly in "channels" purposely created for the sharing of such content on the instant messaging application Telegram. [101]

The phenomenon is also known to the public with the name of "revenge porn" that is not appropriate for two main reasons. First, the word "revenge" suggest that the victim did something wrong to deserve such abuse, giving space to forms of slut-shaming and victim-blaming[102], while often the images are shared without the victim doing anything wrong, maybe the images are just private images of a (partner or) ex-partner (mainly girls) or they have been stolen from the private accounts of the victim. Secondly, the term "porn" has the side effect to narrow the focus on the "pornographic" aspect instead of the emotional damage and distress caused to the victims, attracting even more interest in the wrong way, in fact between May (when the news of revenge porn channels broke) and November 2020 the number of "revenge porn" groups on Telegram in Italy increased from 29 to 89.

The European law does not expressly protect victims of non-consensual pornography. However, this offence can be covered by the "right to be forgotten", of

[101] https://www.repubblica.it/cronaca/2020/11/25/news/telegram_covo_di_pornografia_non_consensuale_e_revenge_porn_-275647052/

[102] The use of Telegram for non-consensual dissemination of intimate images: gendered affordances and the construction of masculinities. Silvia Semenzin, Lucia Bainotti.

article 17 of the Regulation 2016/679[103], which states that everyone has the right to have his personal data erased. In particular, the data subject has the right to have his data erased when the data are no longer necessary for the initial purpose they have been collected for, when he withdraws his consent to the treatment of his data or when data have been unlawfully processed, without prejudice to the collection of data for lawful purposes such as public health, public interest, exercise or defence of legal claims and so on. (Recital 65 of Regulation 2016/679). The right to erasure is also extended in a way that the controller who made the personal data public is obliged to inform the controllers processing data to erase any links or copy or replication of such content. (Recital 66, Article 17). Furthermore, such right has even a deeper basis on "The Chart" at article 8 about the protection of personal data: "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".[104]

Despite in the EU legislation there are not specific rules for the protection of NCII victims, Member States over years have recognised the problem and independently legislated on the subject. France, in 2016, introduced in the *Code penal* at article 226-1 a punishment for anyone that on purpose infringes the intimacy and private life of another person by capturing, recording or transmitting without his or her consent his /her words, images or location. [105] Germany manages the issue throughout a jurisprudential approach, by several judgements that have "created law" about the non-consensual pornography. Spain, in 2015, modified article 197 of the *Código Penal* adding at paragraph 7 that any person that, without the authorization of the person involved, disseminates, discloses or provides third parties with images or audio-visual recordings

[103] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1623545080464&from=EN

[104] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01), Article 8. https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[105] Article 226-1 de le Code pénal. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193566/

(of that person) that undermine the intimacy of such person shall be punished by imprisonment from three months to one year or to pay a fine[106]. In Italy, a law tackling the problem arrived only in 2019, particularly the article 612-ter of the *Codice Penale* states that is punishable anyone who, after having create or subtracted them, shares, publishes or disseminates images or videos with explicit sexual content, made for being private, without the consent of the depicted person. The same penalty is applied to anyone that after receiving such content contributes to its dissemination with the purpose to cause harm to the person depicted. [107]

6.2 Disinformation

Another not illegal but harmful content that can create serious damage to the society is the dissemination of disinformation on the online environment. According to the definition given by the Commission, "disinformation" is any "verifiably false or misleading information" which has been created and spread "for economic gain or to intentionally deceive the public" and that "may cause public harm" particularly with regards to the public health and security, but it can also cause a serious threat to the democracy. Disinformation is different from misinformation because the latest is spread without the purpose to mislead, and often users sharing it do think that such information is true.

Disinformation may cause a serious harm especially, but not only, when the dissemination is on a large scale. During the Covid-19 pandemic disinformation (and misinformation) risked to cause a huge damage to the public health through the sharing of, for instance, false assertions that drinking alcohol can protect from the risk of contracting the virus, or conspiracy theories claiming that the virus has been created and spread to reduce the population or that the vaccine is a mean of governments to

[106] Artículo 197 del Código Penal, https://www.conceptosjuridicos.com/codigo-penal-articulo-197/
[107] Art. 612-ter del Codice Penale. https://www.altalex.com/documents/news/2014/10/28/dei-delitti-contro-la-persona#art612ter

keep control over the population. In April 2018, some industries having a key role in the spreading of information online (Google, Facebook, Mozilla and Twitter in 2018, followed by Microsoft and TikTok respectively in 2019 and 2020) signed *the Code of Practice on Disinformation* through which they agreed on a voluntarily basis to self-regulate themselves in order to counter disinformation online. The code of practice set a broad variety of commitments: (1) scrutiny of ad placements, in which the "Signatories"[108] agreed on blocking or reducing revenues of the websites monetising thanks to false information; (2) political advertising and issue-based advertising, in which they ensured transparency of political advertising; (3) integrity of services, according to which Signatories are required to act against manipulative techniques, such as the creation and utilisation of bots or fake accounts, by using AI to detect and remove them; (4) empowering consumers, particularly giving to trustworthy sources of information a major visibility; (5) empowering the research community, by providing researchers with relevant data they need, also on the function of the platform services. In addition to such commitments, Signatories are required to write an annual report on their work of tackling disinformation.

After the covid pandemic, that highlighted the shortcomings of the Code, the Commission worked on a *Guidance to strengthen the Code of Practice on Disinformation*[109], that has been published on May 21, 2021. Particularly, with this document the Commission wants to (1) encourage a larger number or platforms, providers, relevant stakeholders in the online advertising and private messaging providers to join the Code; (2) demonetise disinformation completely, also through the sharing of information about the ads refused by one of the signatories, improving transparency about the advertising banners and precluding the possibility to publish ads to people that systematically publish fake or misleading content; (3) ensure the integrity of services, having a total understanding of all the existing and emerging forms of

[108] Companies and associations listed as signatories of the Code of Practice on Disinformation.
[109] European Commission Guidance on Strengthening the Code of Practice on Disinformation, 26.05.2021.
https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation

manipulative tools and behaviours that can be used to disseminate disinformation, such as fake accounts, bots, account takeovers and other means and putting in place all the necessary measures to avoid them; (4) empower users to understand and flag disinformation, providing them with information about how the recommender system works and with a tool to notify the disinformation (providing also the redress possibility), giving to trustworthy information source of public interest a better visibility; (5) enhance the coverage of fact-checking and giving major access to data to researchers; (6) improve the monitoring framework, utilising the key performance indicators (KPIs). Hence, the aims of such *Guidance* are the creation of a safe, reliable and more transparent online environment through an improvement and better implementation of the current Code of Practice. It also provides the opportunity to create appropriate measures and tools to address the systemic risk related to disinformation, in the light of the anticipated Digital Services Act risk evaluation and mitigation framework, as the Commission clarify on its website.[110]

[110] Code of Practice on Disinformation, Official EU website: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Part III

CONCLUSIONS

Chapter 7

Other relevant documents useful to face illegal and harmful content online

The online environment is dynamic and continually evolving. New technologies and services spread through the online networks very fast, providing new and useful tools to meet the human needs, to simplify lives, to bridge the physical distance by interconnecting people. The rapid growth of technology and information is an important resource for the development of economy and businesses, although it brings with it many challenges that require an equally rapid response. The dissemination of illegal and harmful content often run hand in hand with the introduction of new systems and technologies, creating a sort of parallel illicit network perfectly able to exploit any possibilities that have been left without a proper control. Institutions and governments have a great responsibility in mitigating and eliminating the harm that any kind of illegal content or information may cause to the society as a whole (citizens, companies, environment, etc) by the creation and implementation of an adequate legal framework to counter the problem. However, often the evolution of the online environment is so fast that the legal framework, once approved, fails to consider all the new tools, means and strategies that have arisen in the meantime to avoid and circumvent the ways provided by the law to counter specific problems. For this reason, it is fundamental that all the online providers, especially the large and very large online providers, take responsibility of the key role they have in the fight against the illegal content online. The dissemination of illegal content is a large-scale problem that can be faced effectively only with the help of providers whose platforms are often used for the spreading of such content.

The institutions encourage big platforms to create and sign voluntarily Codes of Conducts with the aim to tackle specific problems that can arise in the online environment. Codes of Conducts are self-regulatory tools in which the involved companies, usually with the help of governments entities and stakeholders, highlight a

specific problem and lay down provisions to counter that problem. The signatories of the Code are committed to the observation of the rules in the document. The creation of such Codes is particularly important because they can be modified more easily compared to the legal framework and, even though they are not legally binding, they provide a valid mean to face the challenges deriving from the ongoing transformation of the online system. Furthermore, they can be signed also by smaller providers that can take advantage from the analysis and implementation systems put in place by big online platforms. In fact, big online platforms have the moral duty and responsibility to share their knowledge with smaller companies with the purpose to create a safer online environment. Especially because big providers have at their disposal human and physical resources that can lead to the creation of new tools to tackle illegal content more effectively.

The Commission recognised the extremely significant role of such Codes and included them in the Digital Services Act. At Article 35 the Commission encourages the creation of Codes of Conduct, particularly with regards to the assessment and identification of a systemic risk, and highlights the necessity to define clearly the objectives as well as the performance indicators to measure the extent to which the objectives have been achieved. Finally, the Commission stresses the importance of reporting regularly the measures taken along with the outcomes.

In addition to Codes of Conduct, institutions can also give Communications and Recommendations – both not legally binding documents – to suggest and encourage big companies to take an active role in the fight against illegal content online. For example, in 2018 the Commission issued a *Recommendation on measures to effectively tackle illegal content online*[111]. The aim of the document was to raise awareness and responsibility among the online platforms, proposing a common approach for the detection and removal of illicit content online. Such approach consisted in encouraging

[111] Commission Recommendation on measures to effectively tackle illegal content online, 1.03.2018, https://digital-strategy.ec.europa.eu/en/library/commission-recommendation-measures-effectively-tackle-illegal-content-online

platforms to introduce a clearer “notice and action” and proactive tools to avoid the re-appearance of removed content, ensure the respect of fundamental rights by avoiding unfair removals, cooperate with smaller companies by sharing experience and technology and cooperate with law enforcement authorities.

Codes of Conduct as well as Recommendations and other means represent already a valid method to counter illegal content online and they contribute to maintain a high pressure over the actions and performance carried out by the Web giants. In the last years, many big online companies agreed to take part to some Codes of Conduct that laid and could lay in the future the basis for the creation of a more effective legal framework. For instance, the recommendations of the Digital Services Act have been built considering the Recommendation on illegal content of 2018, the Code of Conduct against illegal hate speech of 2016, as well as other relevant but non-binding documents such as the Memorandum of Understanding against counterfeit goods and the findings of the EU Internet Forum.

Chapter 8

Conclusion

The Digital Services Act is a forward-looking legislative proposal thanks to which big online platforms, besides getting the enormous financial benefits deriving from covering a near monopolistic position, will have to take responsibility for the importance of the role they have in keeping the Web a safe environment. The legal framework that in the last years regulated the online environment is the e-Commerce Directive, that dates back to the 2000s. At that time, the "Internet" and the technology were very different, just think that Google was a simple searching engine, Amazon was an online bookstore and smartphones did not exist yet. In the past 20 years the online scenario has been shaken by enormous changes, but the international and national law failed in keeping up with times that have never changed so fast. Europe has been the first country who recognised the compelling need for a Regulation able to deal with many of the modern society problems deriving by the use of technology in everyday life and by the enormous power in the hands of very few *gatekeepers* of the Internet. The Digital Services Act and the Digital Markets Act are parts of a jigsaw that started with the introduction of the General Data Protection Regulation in 2018 and that is far from being complete. This regulatory package has the aim to lead the European Union in a unique direction, harmonizing the legal framework and making the online environment safer, more competitive and more respectful of the human rights. In addition to this, EU really aims to become a global leader by driving the change for the digital economy. The new obligations that the Regulation, whether approved, would apply to online providers will be particularly burdensome, especially for very big online platforms, and the deep changes required will surely affect not only Europe, but the whole digital system worldwide. The many innovative aspects of the Regulation, such as the need to put in place an effective and user-friendly notice and action mechanism, the traceability of traders, the assessment of the systemic risks, the publishment of annual reports and a strengthen control over VLOPs, will help to tackle illegal content online more promptly and effectively, making the online world a safer place. The Vice-President of the

European Commission Vestarger, during a press conference in Brussels, stressed that consumers should be able to do shopping in a safe manner and to trust the news they read online as well as offline because “what is illegal offline is equally illegal online”. The Digital Service Act is the legal tool that should allow users to feel safe when using online services.

However, the approval of the Digital Services Act will have to go through a long and difficult path that could last years, during which the online scenario could change significantly again. At the same time, whether the final text will exactly reflect the proposal of the Commission or not, it still has few points that could be improved. The text of the proposal only considers “illegal content”, leaving the issue of the harmful – but not illegal – content to not-binding tools such as the Codes of Conduct. As we mentioned above, harmful content, such as non-consensual pornography, cyberbullying, online harassment and disinformation, can damage seriously the public health and security (just think to the disinformation and fake news during the pandemic or the suicides of many teenagers after being victim of cyberbullying or revenge-porn). The reason why the Commission decided to exclude the harmful content category from the Regulation is that, by defining what is “harmful content” and how to deal with it, it would have risked of making the approval of the content of the DSA even more difficult. In fact, the extension to the removal of harmful content by automated means or by notify and action mechanism could risk of resulting in a limitation of the freedom of expression and, so, in the infringement of one of the human rights protected by “The Chart”. In the DSA, the Commission tried to balance the need to have an effective content moderation with the need to protect the freedom of speech. This concern is manifested by the many provisions in the Regulation that require platforms to put in place a redress mechanism and inform users about the redress possibilities available, to protect users whose content could have been unfairly removed. In fact, one of the major critics that has been done to the proposal is the risk of damaging the freedom of expression. This because online services providers, in order to not risk of incurring in liability, could decide to remove also controversial material. Furthermore, the risk of

over-removal increase considering that the DSA contains specific provisions about automated tools for content moderation, considering that such tools are as essential as inaccurate and they can be easily circumvented. The Commission is aware of these problems and to cope with them it encourages big online companies to keep working on the creation of more effective tools. Another relevant issue that has not been considered in the DSA is the challenge of balancing the right of privacy of individuals with the need to counter illegal content online. Often communications are protected by using the end-to-end encryption, that makes very difficult for online platforms to carry out their duties in tackling illegal content, particularly with regards to the content that constitutes a serious threat for the safety of people such as terrorist content and child sexual abuses.

Besides few aspects that will likely be clarified by further communications of the Commission, the Digital Services Act is definitely a useful tool that can set the basis for an ambitious legislative reform. It gives proportionate provisions to tackle illegal content online more effectively, burdening mainly platforms that can be considered *gatekeeper* of the Internet and it provides a homogeneous legal framework that will help SMEs to enter in different Member States markets, giving a prompt to fair competitive conditions. Certainly, the road to fight illegal content online is still long and difficult and it requires also different approaches that cannot be laid down in Regulations, such as the need to raise awareness among the public of the many negative aspects of infringing IP rights and the urgent need to develop better tools. The Commission, however, is working in many ways not only to tackle the huge problem of illegal content disseminated on the Web, but also to foresee and prevent the new challenges that may arise from such an ever-changing online environment.

Bibliography and Web references.

Agenda Digitale, Maria Romana Allegri, (14 May 2021) "*Digital Services Act, il "rebus" dei contenuti illeciti: la Ue rischia di aumentare il caos*". Retrieved on June 2021 from https://www.agendadigitale.eu/mercati-digitali/digital-services-act-il-rebus-dei-contenuti-illeciti-la-ue-rischia-di-aumentare-il-caos/

BBC (22 April 2021) *Coronavirus: Pfizer confirms fake versions of vaccine in Poland and Mexico*. Retrieved on June 2021 from https://www.bbc.com/news/world-56844149

Code of Practice on Disinformation, Official EU website https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Code Pénal. Article 226-1, 30 July 2020. Available at https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193566/

Codice Penale, art. 612-ter, 19 July 2019. Available at https://www.altalex.com/documents/news/2014/10/28/dei-delitti-contro-la-persona#art612ter

Código Penal, Articulo 197. Available at https://www.conceptosjuridicos.com/codigo-penal-articulo-197/

Covid-19 Treatment Guidelines, (October 9, 2020), *Chloroquine or Hydroxychloroquine With or Without Azithromycin*. Retrieved on June 2021 from https://www.covid19treatmentguidelines.nih.gov/antiviral-therapy/chloroquine-or-hydroxychloroquine-with-or-without-azithromycin/ https://files.covid19treatmentguidelines.nih.gov/guidelines/covid19treatmentguidelines.pdf

EPO and EUIPO (2019), in *IPR-intensive industries and economic performance and employment in the European Union*, third edition, September 2019. Retrieved on June 2021 from https://euipo.europa.eu/ohimportal/en/web/observatory/ip-contribution.

EUIPO (June 2019), in QUALITATIVE STUDY ON RISKS POSED BY COUNTERFEITS TO CONSUMER. Retrieved on June 2021 from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers_Study/2019_Risks_Posed_by_Counterfeits_to_Consumers_Study.pdf

European Commission (10 September 2020), Proposal for a *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online*. Retrieved on June 2021 from https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0568/COM_COM(2020)0568_EN.pdf

European Commission (12 September 2018) Proposal of the Commission for a *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online*. Retrieved on June 2021 from https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission (2016), *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*.

European Commission (2017) "*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, 2017 COM/2017/0555 final, Brussels. Retrieved on May 2021, available at https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A52017DC0555

European Commission (2018), *Commission Recommendation on measures to effectively tackle illegal content online*. Retrieved on June 2021, available at https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

European Commission (24 July 2020), *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. EU strategy for a more effective fight against child sexual abus*e. Available at https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf

European Commission (26 May 2021), *Guidance on Strengthening the Code of Practice on Disinformation, (COM(2021) 262 final*). Retrieved on June 2021 from https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation

European Commission (30 June 2016), *Code of conduct on countering illegal hate speech online*. Retrieved on June 2021 from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

European Commission (6 December 2008), *ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY COUNCIL FRAMEWORK DECISION 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law*. Retrieved on June 2021 from

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:328:0055:0058:en:PDF

European Commission (Brussels 14/12/2020), *Commission Staff Working Document,* "*Counterfeit and Piracy Watch List".* Retrieved on June 2021, available at https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf

European Commission*, Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online*, available at https://digital-strategy.ec.europa.eu/en/library/commission-recommendation-measures-effectively-tackle-illegal-content-online

European Commission, *Proposal for a "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive" 2000/31/EC.* Available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

European Court Of Human Rights (07 December 1976*), CASE OF HANDYSIDE v. THE UNITED KINGDOM*. Retrieved on June 2021 from http://hudoc.echr.coe.int/eng?i=001-57499

European Union (2020), *Communication: Shaping Europe's digital future*, Publications Office of the European Union (19 February 2020). Retrieved on April 2021, available at https://ec.europa.eu/info/publications/communication-shaping-europes-digital-future_it

European Union Intellectual Property Office (June 2020), *2020 STATUS REPORT ON IPR INFRINGEMENT Why IP Rights are important, IPR infringement, and the fight against counterfeiting and piracy.* Retrieved on June 2021, available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf

European Union: Council of the European Union, *Charter of Fundamental Rights of the European Union (2007/C 303/01)*, 14 December 2007, C 303/1, available at https://www.refworld.org/docid/50ed4f582.html [accessed 20 April 2021]

Europol (17 April 2020), *Viral Marketing, counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic*. Retrieved on June 2021 from https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic

Europol (19 June 2020), Report: *Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*. Available at https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

EUROPOL and EUIPO (2019) in *INTELLECTUAL PROPERTY CRIME THREAT ASSESSMENT.* Retrieved on June 2021 from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report_Exec_Sum_EN.pdf

Federal Trade Commission, (24 July 2019), *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Retrieved on May 2021, available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Frontier Economics Ltd (2017), *The Economic Impact of Counterfeiting and Piracy. A Report Prepared for BASCAP and INTA*, p.28-33. Retrieved on June 2021, available at https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAPFrontier-report-2016.pdf

Garante per la protezione dei dati personali, (28/06/2019) *Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro*, Roma June 28, 2019. Retrieved on May 2021, available at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9121352

INHOPE Association (2020) in *Annual Report 2020.* Retrieved on June 2021 from https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf

Iñigo Palao and Lola Rodriguez, (2019), in *Piracy Observatory and Digital Content Consumption Habits*. Retrieved on June 2021 from http://lacoalicion.es/wp-content/uploads/executive-obs.piracy_en_2019.pdf

Judgment of the Court (Third Chamber) of 3 October 2019, *Eva Glawischnig-Piesczek vs Facebook Ireland Limited*, Case C-18/18. Retrieved on April 2021, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=1309

Kempt, Simon (2019), *Digital Around The World In 2019*, in *Digital 2019 Essential Insight into how people around the word use the internet, mobile devices, social media and e-commerce*. Kepios, We Are Social and Hootsuite publication. Retrieved on June 2021, available at https://p.widencdn.net/kqy7ii/Digital2019-Report-en

La Repubblica, Longo A. (November 25, 2020), *Telegram covo di pornografia non consensuale e revenge porn.* Retrieved on June 2021 from https://www.repubblica.it/cronaca/2020/11/25/news/telegram_covo_di_pornografia_non_consensuale_e_revenge_porn_-275647052/

Latham & Watkins LLP (March 2021), *The EU's Proposed Digital Services Act. New Obligations and Sanctions for Online Platforms*.

LEGGE 16 giugno 2016, n. 115, "L'aggravante di negazionismo". Available at https://www.gazzettaufficiale.it/eli/id/2016/06/28/16G00124/sg

Lexology, Lesley Hannah, Kio Gwilliam and Antonio Delussu, (25 May 2021), *The Digital Services Act: What are the key provisions, and does it strike the right balance?* Retrieved on June 2021, available at https://www.lexology.com/library/detail.aspx?g=4de1cbbb-a367-4224-8b60-ef391ea2a274

Michael Kozlowski (25 March 2018), *Pirate Websites Received 300 Billion Visits Globally*. Retrieved on June 2021 from https://goodereader.com/blog/technology/online-pirate-websites-received-300-billion-visits-globally

OECD (2019), *An Introduction to online platforms and their role in the digital transformation*, OECD Publishing, Paris. Retrieved on April 2021, available at https://read.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_19e6a0f0-en#page2 and https://read.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_19e6a0f0-en#page2

OECD/EUIPO (2019), in *Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade*, OECD Publishing, Paris/European Union Intellectual Property Office. Publishing. Retrieved on June 2021 from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/trends_in_trade_in_counterfeit_and_pirated_goods/trends_in_trade_in_counterfeit_and_pirated_goods_en.pdf

Official Journal C 326, p. 391–407, (26/10/2012), *Charter of Fundamental Rights of the European Union (2012/C 326/02).* Retrieved on May 2021, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=IT

Official Journal L 119, p. 1-88, (4/05/2016). European Union, *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, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Retrieved on June 2021 from
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1623545080464&from=EN

Official Journal L 178, p. 0001 – 0016, (*17/07/2000)*, *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 ('Directive on electronic commerce').* Retrieved on April 2021, available at
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

Official Journal L 201, p. 37-47, (31/07/2002), *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications*). Retrieved on June 2021, available at
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

Official Journal L 335, p. 1–14, (17/12/2011*), DIRECTIVE 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. Retrieved on June 2021, available at
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0093

Official Journal of the European Communities (18 December 2000), *CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION" (2000/C 364/01)* Retrieved on June 2021 from
https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Official Journal, L 172, p. 79-109, (17/05/2021), European Commission, *REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online*. Retrieved on June 2021, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=en

PRNewswire, Facebook, Inc. (28 April 2021), *Facebook Reports First Quarter 2021 Results*. Retrieved on May 2021, available at https://www.prnewswire.com/news-releases/facebook-reports-first-quarter-2021-results-301279518.html

Semenzin S., Bainotti L. (April 2020), *The use of Telegram for non-consensual dissemination of intimate images: gendered affordances and the construction of masculinities.*

Tambiama Madiega, (March 2021) "*Digital services act* ", Briefing on the Digital Services Act, European Union, First edition. Retrieved on May 2021, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf

Tankovska H., (21 May 2021) *Facebook's monthly active users (MAU) in Europe from 4th quarter 2012 to 1st quarter 2021*, the source of data is Statista. Retrieved on May 2021, available at https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/

The European Commission (2020), *Work stream on Measurement & Economic Indicators, Progress Report*; published by Expert Group for the Observatory on the Online Platform Economy. Retrieved on April 2021, available at https://platformobservatory.eu/app/uploads/2020/07/ProgressReport_Workstream_on_Measurement_and_Economic_Indicators_2020.pdf

UK Public General Acts, *The Human Rights Act 1998 (1998).* Retrieved on June 2021 from https://www.legislation.gov.uk/ukpga/1998/42/schedule/1