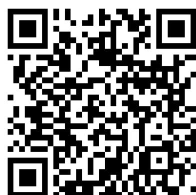


Publicação disponível em: https://blook.pt/publications/publication/079dbcfa6aea/

INTRODUCTION TO THE DIGITAL SERVICES ACT, CONTENT MODERATION AND CONSUMER PROTECTION

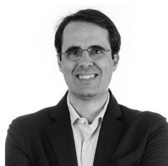
JORGE MORAIS CARVALHO FRANCISCO ARGA LIMA MARTIM FARINHA

REVISTA DE DIREITO E TECNOLOGIA, VOL. 3 (2021), NO. 1, 71-104

©Revista de Direito e Tecnologia

Obtido a: 24.05.2021 19:03

Electronic copy available at: https://ssrn.com/abstract=3852280



JORGE MORAIS CARVALHO
NOVA School of Law / NOVA Consumer Lab

FRANCISCO ARGA E LIMA
NOVA School of Law / NOVA Consumer Lab

MARTIM FARINHA
NOVA School of Law / NOVA Consumer Lab

Introduction to the Digital Services Act, Content Moderation and Consumer Protection*

ABSTRACT: In December 2020, the European Commission presented the Digital Services Act with the stated aim of ensuring a safe and accountable online environment. It mainly consists of a Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services. This article provides an analysis of the historical and systematic context of this proposal, including a guided tour of its content and an overview of the relationship with other European legislative instruments. The issue of con-

* We would like to thank Maria Clara Paixão, Joana Campos Carvalho, Paula Ribeiro Alves and Paulo Lacão for having read a draft of this text and for their suggestions.

Electronic copy available at: https://ssrn.com/abstract=3852280

tent moderation in digital services is also further addressed, referring to the historical context of the legal regime now proposed. The different EU and US perspectives are outlined. The topic of consumer protection is also dealt with in the text, with emphasis on the most relevant provisions in this field and the problems that may arise therein.

Keywords: (i) digital services; (ii) digital market; (iii) data protection; (iv) consumer protection

1. Introduction

The digital market, especially digital platforms, have been intense topics of discussion for the past years. This is due, not only to the exponential development of technology we have been dealing with for the past decades, but also due to the possible risks for consumers that derive therefrom.

For that reason, the European Institutions have had a long history of adopting legislative efforts to make the digital environment a more secure place, namely when it comes to the Fundamental Rights enshrined in the Charter of Fundamental Rights of the European Union, like the respect for private and family life (article 7). This focus has been over-arching, but most heavily focused on consumer law and data protection, where the European legal acquis now contains a considerable amount of consumer law directives[1] and the General Data Protection Regulation (GDPR)[2].

Very recently, the Commission presented a new proposal to be added to the list of European legislation related to the Digital Mar-

[1] For example, 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) – e-Commerce Directive.

[2] 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).

Electronic copy available at: https://ssrn.com/abstract=3852280

ket: the Proposal for a Digital Services Act[3] (hereafter DSA). Here, it mainly focuses on regulating intermediary services, thus complementing the consumer law and the data protection rules already put in place.

Thus, the aim of this article is to explore this proposal's history, structure, as well as its relation with other European directives and regulations, so as to ascertain its accomplishments and situations where it does not go far enough. In particular, we shall focus on content moderation as well as the way in which it aims at protecting consumers' rights, how much it protects consumers and if that is enough. For that reason, Chapter 2 will focus on an analysis of the Digital Services Act, from its origin and the reasons that led the Commission to present it, to the main provisions that are embodied therein and the relation it establishes with the existing legal framework, especially the GDPR. In Chapter 3 we will approach specifically the topic of content moderation, in order to ascertain if the progress presented by the Digital Services Act adequately answers the problems identified in prior legislation (in the European Union and the United States), and what is already done in practice, namely by digital platforms. Lastly, on Chapter 4 we will analyse how the Proposal reinforces consumer protection, when it comes to five main aspects: traceability, pre-contractual information and product safety information, advertisement transparency, recommender systems and the general principle of non-liability of hosting service providers.

2. Historical and systematic background of the Digital Services Act

The Proposal for a Digital Services Act has been the culmination of years of technological innovation that needed to be accompanied

[3] 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 (COM/2020/825 final). Available at EUR-Lex: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

by the necessary legislative updates[4]. In fact, according to the Commission, there were three main motives that led to this proposal. Firstly, ever since the adoption of Directive 2000/31/EC, the development of new digital services reached ever-increasing heights that demanded the update of the European legal framework in what concerns the digital market[5]. Secondly, the constant usage of these new services and platforms has become a source of new risks, both to consumers as well as society as a whole, being thus necessary to regulate them in order to mitigate these potential dangers[6]. Lastly, the current pandemic scenario in which we are submerged has also raised attention to the importance of digital technologies in our daily lives. As the Commission puts it "[i]t has clearly shown the dependency of our economy and society on digital services and highlighted both the benefits and the risks stemming from the current framework for the functioning of digital services"[7].

Due to this need to regulate the digital market and service providers, the Commission presented in December a legislative package composed by two proposals: the Digital Markets Act[8] and the Digital Services Act. While the first aims at ensuring fair economic outcomes with regard to digital platform services, as well as to complement the application of articles 101 and 102 TFEU to these specific platforms[9], the Digital Services Act aims at harmonising conditions for innovative cross-border services to develop in the

[4] In that sense, see EPRS, *Digital Services Act* (March 2021), 1-4. Available at Europarl: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf. (last accessed 14 April 2021).

[5] 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*, (COM (2020) 825 final), Brussels, 15-dez.-2020, 1. For the need to review the e-Commerce Directive as stated by the European Parliament, see the brief summary in EPRS, *Digital Services Act* cit., 2-3.

[6] European Commission, *Digital Services Act* cit., 1.

[7] European Commission, *Digital Services Act* cit., 1.

[8] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act),* (COM (2020) 842 final), Brussels, 15-dez-2020.

[9] European Commission, *Digital Markets Act* cit., 16.

Electronic copy available at: https://ssrn.com/abstract=3852280

EU, addressing and preventing the emergence of obstacles to these activities, as well as providing for adequate supervision to the provided services[10]. For that reason, it sets due diligence obligations on different types of digital service providers in order to ensure that those services are not misused for illegal activities and that operators act responsibly[11].

With these two proposals, it becomes evident that the Commission wants to tackle the problems that arise from two main situations. When it comes to the Digital Markets Act, the Commission justifies its need on the characteristics that core platform services have, namely extreme scale economies, network effects, the ability of connecting many business users with end users through the multi-sidedness of these services, etc[12]. These characteristics combined with unfair commercial practices have the potential of undermining the contestability of the core platform services, as well as the general fairness of the business and end users of such services[13]. Thus, with the Digital Markets Act proposal, the Commission aims at providing appropriate regulatory safeguards throughout the Union against unfair behaviour, facilitating cross-border business throughout the Union, improving the functioning of the internal market[14].

The Digital Services Act, however, has a different scope. Even though it aims at ensuring the proper functioning of the internal market, especially when it comes to cross-border digital services (mostly intermediary ones), here the focus is to foster the responsibility of intermediary service providers, to allow for the existence of a safe online environment, where citizens remain free to exercise their fundamental rights, namely the freedom of expression and information[15].

[10] European Commission, *Digital Services Act* cit., 2-3.

[11] European Commission, *Digital Services Act* cit., 18.

[12] European Commission, *Digital Markets Act* cit.,14-15.

[13] European Commission, *Digital Markets Act* cit., 14-15.

[14] European Commission, *Digital Markets Act* cit., 16.

[15] European Commission, *Digital Services Act* cit., 6; EPRS, *Digital Services Act* cit., 1-2.

Electronic copy available at: https://ssrn.com/abstract=3852280

2.1. Guided tour to the Digital Services Act

The Digital Services Act is an instrument aimed at reinforcing the responsibilities of intermediary services. How does the Commission concretely suggest achieving this goal? It does so through a Proposal for a Regulation divided into five chapters: General Provisions; Liability of Providers of Intermediary Services; Due Diligence Obligations for a Transparent and Safe Online Environment; Implementation, Cooperation, Sanctions and Enforcement; Common Provisions of Enforcement; Final Provisions.

The first chapter sets the general tone of the proposal, clarifying its subject matter, scope (article 1) as well as the definitions (article 2).

The Regulation will apply to part of the information society services, namely the intermediary services (article 1-1). An "information society service" is to be considered "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (article 1-1(b) of Directive (EU) 2015/1535). There are four conditions that should be met in order to comply with the concept: (i) remuneration; (ii) at a distance; (iii) by electronic means; (iv) at the individual request of a recipient of services. In the Uber Spain, Uber France and Airbnb Ireland cases[16], the CJEU established case-law according to which a service provided by a digital intermediation platform, in order to be classified as an information society service must not only comply with the four conditions mentioned, but also not to form an integral part of an "overall service whose main component is a service coming under another legal qualification". To answer this last question, the CJEU created a test which includes two decision criteria: (i) whether the platform has created a new market; (ii) whether the platform exercises a decisive influence on the service providers reg-

[16] CJUE 20-dez.-2017, case c-434/15 (*Judgment Uber Spain*); CJUE 10-abr.-2018, case C-320/16 (*Judgment Uber France*); CJUE 19-dez.-2019, case C-390/18 (*Judgment Airbnb Ireland*).

Electronic copy available at: https://ssrn.com/abstract=3852280

istered with it with regard to the conditions under which the service is provided[17].

Recitals 5 and 6 of the Proposal state that the regulation should apply to "providers of intermediary services". It is clarified that this application is restricted to intermediary services, not affecting the requirements established in European Union or national legislation "relating to products or services intermediated through intermediary services, including in situations where the intermediary service constitutes an integral part of another service which is not an intermediary service as specified in the case law of the Court of Justice of the European Union". This is a clear reference to the CJEU case law referred to in the previous paragraph. The regime of the Proposal applies irrespective of whether the information society service is part of an overall service whose principal element is a service with another legal qualification, provided that it is an intermediary service. The Regulation will not obviously cover the (other core) service, such as transport or accommodation, which is not an intermediary service[18].

The Regulation is intended to apply to intermediation services, simply defined by belonging to one of three categories of services: mere conduit, caching and hosting. The hosting services consist of the "storage of information provided by, and at the request of, a recipient of the service". Explicitly included among hosting services are online platforms. According to the definition in article 2(h) an online platform is (i) a provider of a hosting service which, (ii) at the request of a recipient of the service, (iii) stores and disseminates to the public information. It is not qualified as an online platform if the "activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the

[17] Jorge Morais Carvalho, *Airbnb Ireland Case: One More Piece in the Complex Puzzle Built by the CJEU Around Digital Platforms and the Concept of Information Society Service*, 6/2 ItalLJ (2020), 463-476, 473.

[18] Jorge Morais Carvalho, *Sentenças Airbnb Ireland e Star Taxi App, Conceito de Serviço da Sociedade da Informação e Regulação de Plataformas Digitais*, RDC – Liber Amicorum (2021), 481-510, 508.

Electronic copy available at: https://ssrn.com/abstract=3852280

other service is not a means to circumvent the applicability of this Regulation".

The definition of illegal content can be found in article 2(g) in conjunction with recital 12. Illegal content is any information that – irrespective of its form, which by itself or in reference to an activity (that can include the sale of goods and provision of services) – does not comply with Union law or the law of a Member State. It is a purposely vague definition, that is intended to be interpreted in a broad manner, due to the horizontal scope of application and the objectives of the Proposal. The task of defining illegal content is left to the competent jurisdictional authorities, in reference to the applicable legislation to each case. Illegal content can therefore include "illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law"[19].

Chapters II and III of the Digital Services Act delve deeper into the responsibilities attributed to providers of intermediary services (article 2(f)).

Chapter II regulates a subject which is currently provided for in the e-Commerce Directive. It sets the general rules, namely on what concerns exemption of liability[20]. Concretely, it gives the general conditions that must be respected for providers of mere conduit (article 3), catching (article 4) and hosting services (article 5) to be exempt from liability due to third-parties' information they transmit and store. Furthermore, it also seems to exclude the possibility of liability of these service providers if they conduct their own investigations aimed at detecting, identifying, removing, disabling access to illegal content or take the necessary measures in

[19] See Recital 12.

[20] For a general overview of the adopted structure for the Digital Services Act, see European Commission, *Digital Services Act* cit., 13-16.

Electronic copy available at: https://ssrn.com/abstract=3852280

order to comply with the rules set out by EU law in general (article 6). Lastly it sets two final obligations: the prohibition of general monitoring or active fact-finding (article 7) and the obligation to respect orders from national judicial or administrative authorities to act against illegal content and to provide information (articles 8 and 9).

Chapter III sets out due diligence obligations for a transparent and safe online environment, through five different sections. Here, the Commission regulates the different intermediary services according to their activities and sizes, imposing obligations proportional to those two criteria.

The first section consolidates the foundation of the due diligence obligations every intermediary service provider should comply with: the need to establish a single point of contact to facilitate direct contact with state authorities (article 10), the need to designate a legal representative in the Union, for those providers that are not established in any Member States, but who provide their services inside the territory of the European Union (article 11), the obligation of setting out on their terms and conditions any restrictions they may impose on the use of their services as well as to act responsibly when applying them (article 12) and, lastly reporting obligations when it comes to the removal and the disabling of information considered to be illegal or contrary to the provider's terms and conditions (article 13).

From then on, the next sections regulate specific types of intermediary services providers, additionally to what is already enshrined in Section 1. Section 2 regulates providers of hosting services, obliging them to put in place mechanisms allowing third parties to notify the presence of potentially illegal content (article 14) as well as the obligation to state the reasons for the removal or disabling of access provided by a recipient of the service (article 15). Sections 3 and 4 regulate online platforms, as complements to Sections 1 and 2. Therefore, while Section 3 lays general rules applicable to them, namely in what concerns complaint-handling systems and dispute resolution (articles 17 to 19), protection against illegal usage of the platform (articles 20 to 22) and information obligations (articles 23 and 24), Section 4 adds further due diligence responsibilities to

Electronic copy available at: https://ssrn.com/abstract=3852280

very large online platforms[21]. These concern mainly two additional aspects: obligations of security and control (articles 26 to 28 and article 32) and further responsibilities of information and access (articles 29 to 31 and article 33).

Lastly, Section 5 contains general provisions regarding due diligence obligations, like the framework for the development of codes of conduct (articles 35 and 36) and crisis protocols to address extraordinary circumstances that may affect public health or security (article 37).

Chapter IV focuses mainly on the implementation and enforcement of the previous provisions. Through five new sections, it regulates (i) the national competent authorities – Digital Services Coordinators – responsible for ensuring the correct implementation of the Digital Services Act as well as the attributions they must possess, (ii) the European Board for Digital Services[22], (iii) the supervision of very large online platforms by the Commission, (iv) information-sharing between the Digital Services Coordinators, the European Board for Digital Services and the Commission as well as (v) the adoption of delegated and implementing acts in accordance with articles 290 and 291 of the Treaty on the Functioning of the European Union.

Lastly, we have Chapter V containing the final provisions of the Regulation, related with amendments to other Directives, its evaluation and entry into force.

[21] According to article 25 these are "online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million (...)".

[22] Article 47 states that the European Board for Digital Services is an "[a]n independent advisory group of Digital Services Coordinators on the supervision of providers of intermediary services(...)", responsible for: "[c]ontributing to the consistent application of this Regulation and effective cooperation of the Digital Services Coordinators and the Commission with regard to matters covered by this Regulation", "coordinating and contributing to guidance and analysis of the Commission and Digital Services Coordinators and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation" and "assisting the Digital Services Coordinators and the Commission in the supervision of very large online platforms".

Electronic copy available at: https://ssrn.com/abstract=3852280

This being the structure of the regulatory framework offered by the Proposal, we cannot forget that in order to fully understand it, one must take into account the remaining legal acquis that has been adopted in regard to the Digital Market and Digital Services in particular.

2.2. The Digital Services Act in the European legal system

The Digital Services Act offers an update to the current EU framework regulating the digital market and intermediary services in general. However, it is not an isolated legislative instrument.

In fact, and as stated by the Commission in the Proposal, the most important piece of legislation when it comes to digital services is the e-Commerce Directive[23]. Accordingly, the Digital Services Act is meant to build on the provisions enshrined therein, especially when it comes to article 3 and the internal market principle[24]. However, as already mentioned, the provisions on the exemption of liability of providers of mere conduit, caching and hosting services are moved to the Digital Services Act, and the corresponding provisions of the e-Commerce Directive are repealed. It may be a good idea to also use the Digital Services Act to fundamentally amend the e-Commerce Directive, as its rules are already dated. They were drafted with reference to a fledgling digital market and we now have rampant technological developments linked to new regulatory challenges. The COVID-19 pandemic has further accentuated this need to update the e-Commerce legal regime. If this Proposal is upheld, the existing provisions and principles on the freedom of establishment, the duty of information, commercial communications and contracts concluded by electronic means will remain in force. It also does not solve the problem raised by the aforementioned Uber and Airbnb judgments of the CJEU, which rule out

[23] European Commission, *Digital Services Act* cit., 3.

[24] Furthermore, we may see that the material scope of the Digital Services Act is broader than that of the e-Commerce Directive, since the draft rules apply to online intermediary services. In that sense, see EPRS, *Digital Services Act* cit., 5.

Electronic copy available at: https://ssrn.com/abstract=3852280

the application of all the e-Commerce Directive in cases where a platform is not qualified as providing an information society service and not only the application of the internal market principle (as is the aim of that case law). We believe there is no reason not to apply the provisions on information duties, commercial communications and contracts concluded by electronic means to platforms such as Uber. The problem is identified in the Proposal, but resolved only here and not also with regard to the e-Commerce Directive.

The Digital Services Act also aims at complementing sector-specific instruments, which act as *lex specialis*. This proposal is for instance without prejudice to Directives such as Directive 2010/13/EC, as amended by Directive (EU) 2018/1808, on video-sharing platform providers[25], in as much as it goes beyond what is stated by the Digital Services Act[26]. The same logic applies to Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services, which also acts as *lex specialis* to the Digital Services Act[27].

This proposal is also intended to complement the consumer law acquis. Consumer protection is the topic of an autonomous section of this text, where the analysis of this question is referred to as well.

2.3. The Digital Services Act and the General Data Protection Regulation

The GDPR complements the Digital Services Act, namely when it comes to the right of information, and online advertisement[28]. In

[25] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), 1-24.

[26] European Commission, *Digital Services Act* cit., 4, 5 and 19.

[27] European Commission, *Digital Services Act* cit., 4, 5, 19 and 20.

[28] European Commission, *Digital Services Act* cit., 5, 19 and 20; EDPS, Opinion 1/2021 (10.02.2021), 7. Available at EDPS: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

fact, the link between the Digital Services Act and the GDPR has already been explored by the European Data Protection Supervisor (EDPS) earlier this year.

If we start with the additions that the Digital Services Act brings in terms of the right to information, article 12-1 complements and is without prejudice to articles 12 to 14 of the GDPR, thus increasing the transparency of content moderation practices[29]. This way, the information that must be given to data subjects is reinforced in the context of digital services, through the joint application of the legal regimes.

Regarding online advertisement, articles 24 and 30 of the Proposal clearly complement what is enshrined in data protection law, by bringing additional transparency and accountability to targeted advertisement, without prejudice to the application of the relevant GDPR provisions and the need for consent[30].

There are other sectors where the Proposal for a Digital Services Act touches the GDPR. For instance, the EDPS mentions the need to coordinate article 15 of the Proposal with article 22 of the GDPR, which imposes strict conditions on decisions based solely on automated processing[31]. It is also important to mention that the complaint mechanism enshrined in article 17 of the Proposal is without prejudice to the rights and remedies available to data subjects and provided for in the GDPR[32].

Having in mind the relations between the GDPR and the Proposal, the EDPS welcomes the former, but suggests additional measures in order to strengthen even more the rights of individuals, especially when it comes to content moderation and online targeted

[29] EDPS, Opinion 1/20 cit., 9.

[30] EDPS, Opinion 1/20 cit., 15.

[31] It is important to mention that in this context, the EDPS suggest that in order to promote transparency, article 15(2) of the Proposal should "state unambiguously that information should in any event be provided on the automated means used for detection and identification of illegal content, regardless of whether the subsequent decision involved use of automated means or not" (see EDPS, Opinion 1/20 cit., 11-12).

[32] European Commission, *Digital Services Act* cit., 30-31; EDPS, Opinion 1/20 cit., 12.

Electronic copy available at: https://ssrn.com/abstract=3852280

advertising[33]. Thus, the EDPS focuses on the fact that profiling for the purpose of content moderation should be prohibited unless the online service provider shows that such measure is necessary to address the risks identified by the Digital Services Act[34]. Furthermore, it considers that there should be a ban on online targeted advertising based on pervasive tracking, as well as a limitation on data collected for the purpose of targeted advertising[35].

Thus, it seems that even though these two documents complement each other in key areas related to the digital market, there is still a way to go and ideas to be discussed in order to reinforce the rights of data subjects in a digital context, namely when it comes to advertising, content moderation and profiling. These issues will be further addressed in the following chapters of this article, dedicated to content moderation and consumer protection.

3. Content Moderation in Digital Services

3.1. The exemption of liability for illegal content as a fundamental cornerstone for the provision of digital intermediary services

Content moderation in online intermediary services has always been a tricky topic to address, because, unlike traditional media, these services do not aim to restrict the publication of content with strict editorial norms and limitations on capacity – quite the contrary, the objective is to facilitate, democratize access to an avenue

[33] EPRS, *Digital Services Act* cit., 9; EDPS, *Press Release: EDPS Opinions on the Digital Services Act and the Digital Markets Act, Brussels* (10.02.2021), 1. Available at EDPS: https://edps.europa.eu/system/files/2021-02/edps-2021-01-opinion-on-digital-services-act-package_en.pdf (last accessed 14 April 2021).

[34] EPRS, *Digital Services Act* cit., 9; EDPS, *Press Release: EDPS Opinions on the Digital Services Act* cit, 1.

[35] EPRS, *Digital Services Act* cit., 9; EDPS, *Press Release: EDPS Opinions on the Digital Services Act* cit, 1.

Electronic copy available at: https://ssrn.com/abstract=3852280

for publication, storage and communication of information – they therefore tend to assume the role of passive intermediaries[36].

From the beginning, the sheer amount of content generated and uploaded by users (text, images, audio and video) was already extremely challenging to analyse, classify and detect if there were problems with it. And, as the years progressed, so did technology: with massive improvements in internet speed, memory storage and file compressing (just to name a few) accompanied by much wider societal access to personal computers, smartphones and internet, the task of moderating online content became "humanely" impossible – in 2015, more than 400 hours of video were upload every minute on YouTube[37].

However, as many have pointed out, alongside the exponential growth of online communications, user generated content and its wide societal, political and economic effects, so did the resources, tools and power of Internet-enterprises that operate these intermediary services and collaborative platforms.

The rise of disinformation, cybercrime, elections-meddling incidents, "cancel culture" and concerns over data protection and copyright have, once again, after 20 years, brought the spotlight onto the role of these service providers – in both sides of the Atlantic Ocean.

In Europe, the DSA's legislative process represents a timely opportunity to review the policy choices made in the e-Commerce Directive in 2000, in the infancy of the Internet, and ascertain the best model for the distribution of liability and content moderation duties over communications performed by users on intermediary services.

So, how did we get here?

[36] For further insight on the reasons behind this dichotomy between the publisher and hosting model, see pp. 3 and following of Peggy Valcke/ Marieke Lenaerts, *Who's author, editor and publisher in user-generated content? Applying traditional media concepts to UGC providers*, 24/1 Int'l Rev L Comp & Tech (2010), 119-131.

[37] Available at Tubefilter: https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute. (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

In the late 1990s, with the signature of the two WIPO treaties, several States started initiatives to regulate the role of the then early intermediary digital services. Several approaches were considered: strict liability, negligence liability, liability under safe harbour conditions, immunity from sanctions, immunity from sanctions and injunctions. And, concerning the applicable sanctions, should the intermediaries be subject to the same civil, administrative, or criminal sanctions applied to their users, or different sanctions, lower or of a different kind (merely administrative in nature and not criminal, for example)[38]?

There are several arguments to justify and argue against the imposition of secondary liability to service providers. In favour of more responsibility, we have:

1) The need to ensure the protection of the victims whose rights (reputation, privacy, intellectual property, …) have been violated, and their due compensation. It is almost impossible to guarantee compensation from the primary infringers: their identity is masked with pseudonyms, they are not reachable, they may reside in completely different jurisdictions and legal systems, and it is nearly impossible to ascertain whether they are not insolvent in the first place. To attempt to hold the primary offenders accountable is a costly endeavour with little to no prospects of reparations which hardly justifies the case itself.
2) By holding the intermediaries accountable to some degree, they are economically incentivized to adopt measures to block and terminate illegal activity or even prevent them in the first place (through upload filters, for example).

[38] Giovanni Sartor, *Providers Liability: From the eCommerce Directive to the future*, Directorate General For Internal Policies Policy Department A: Economic And Scientific Policy (2017), 9. Available at Europarl: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf (last accessed 14 april 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

Against this rationale, we have the following main considerations:

1) Secondary liability may be a burden too heavy for these intermediaries to provide their services. The sanctions that would arise might render their business models unviable and excessively risky, forcing them to either abandon or strongly limit them. This is especially notorious for free services provided in a non-profit model, not based on advertising revenue, such as Wikipedia.
2) Without an exemption of secondary liability, in order for the service to continue to operate with the possibility of countless cases and sanctions, it might be forced in direction of adopting measures which excessively constraint the behaviour of their users. In order not to be held liable for not preventing or terminating illegal activity, the intermediary pre-emptively obstructs and blocks all activity that may be perceived as potentially suspicious, excluding completely lawful activities of their users or even the exercise of their fundamental rights.[39] This overdeterrence is the natural reaction to the uncertainty that many kinds of content represent in regards to the law: certain communications can be considered hate speech or defamation, in some cases and not in others. Certain reproductions of copyright protected works can be allowed under fair use (in the US) and the exceptions and limitations of article 5 of the InfoSociety Diretive (in the EU)[40]. Context is key.

This last concern was already a preoccupation as early as 1995, when it was coined as "Collateral Censorship" by Meyerson[41]. Combined with a policy view that innovation should not be stifled and

[39] Giovanni Sartor, *Providers Liability* cit., 12.

[40] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

[41] Michael I. Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" Within the New Media*, 71/1 Notre Dame L. Rev. (1995), 116, 118.

Electronic copy available at: https://ssrn.com/abstract=3852280

that the "Internet Companies" of the time were mere start-ups and medium size undertakings, the regulations of the late 1990s adopted a very protective approach to the provision of intermediary digital services.

In the United States, the legislature followed these concerns and decided on a mixed approach through two complementary acts: the Communication Decency Act (CDA) (1996) and the Digital Millennium Copyright Act (DMCA) (1998).

In the CDA, intermediaries are never considered as publishers or speakers for the content of their users (Section 230 (c) (1)), and are able to police and remove content that they may consider as obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, without being liable for it, if the removal is conducted in good faith (Section 230 (c) (2)) – also known as the "Good Samaritan" clause). In the DMCA, the choice was clearly for a liability under safe harbour limitations, that is, liability that requires a clear specific omission, such as failure to respond to removal requests from authorities and third private parties. Not to be held liable, the intermediary must have no actual knowledge that the material is infringing, it cannot be receiving a financial incentive from it, and upon notification from the rightsholder, it must block the allegedly infringing content.

In the EU, this matter was addressed in the e-Commerce Directive 2000/31/EC, a horizontal directive addressing the first main matters of e-Commerce and long-distance digital contracts. In this directive, the main provisions to be transposed to the Member States' legal systems, pertaining to the intermediary liability and content moderation, can be found in articles 12 to 15. Not only does the European regulation address the matter of illegal content as a whole, without creating a different framework for copyright infringement liability, it also differs from the American Acts by distinguishing different categories of services, with different conditions.

For services of mere conduit of data, the Directive establishes that service providers can be protected from liability if they assume a passive role in relation to the data being transmitted (when they do not initiate the transmission, select the receiver or modify any of the receiver's information). For all intents and purposes, it treats

Electronic copy available at: https://ssrn.com/abstract=3852280

all transmissions in the same manner. Only if properly notified by a court or administrative authority, does it need to take an action to terminate or prevent an infringement – which also applies to the remaining services.

For caching services, the conditions for protection change slightly. Besides the previous requirements, the provider is also expected to comply with the conditions of access, not interfering with lawful uses according to industry standards, maintaining the service updated. They are also expected to remove or disable the access to illegal content if they become aware of it.

Finally, for hosting content, the intermediary is not liable if it does not have actual knowledge of the illegal content or the facts or circumstances from which the illegality derives; only in case the so-called illegality becomes apparent or the provider is made aware of it, should adequate action be taken in order to remove such content.

The Directive also enshrines the principle of no general obligation to monitor and seek illegal activity within their services in order to protect the fundamental rights of freedom and access to information. However, member states may create specific obligations[42] to report to the public competent authorities, certain kinds of alleged illegal activity or content on their service[43] – an obligation that is applicable even if the provider satisfies the conditions on article 14-1, and therefore is not liable[44].

These legal frameworks on both sides of the Atlantic, have shaped the last two decades – a long period of time, in which several factors changed in unforeseen manners. New business models appeared, and Big Tech companies became extraordinarily powerful and resourceful.

[42] Recital 47 Directive and CJUE 03-oct.-2019, case C-18/18 (*Glawischnig-Piesczek*), 34.

[43] The extent to which the injunction from the administrative authority can go is also limited. It cannot impose the adoption of specific measures, nor can impose an excessive burden on the provider. It needs to take in consideration the fundamental rights of all parties involved, including that it does not unnecessarily deprive access to internet users acting lawfully. See CJUE 27-mar.-2014, case C314/12 UPC (*Telekabel Wien*).

[44] Recital 45 Directive and CJUE 03-oct.-2019, case C-18/18 (*Glawischnig-Piesczek*), 24.

Electronic copy available at: https://ssrn.com/abstract=3852280

3.2. Self-regulation in practice: what did we learn from the last 20 years?

While neither the European legislation nor the American Acts imposed general duties for content moderation (the CDA gave a figurative sword for the policing of "obscene" content but no obligation to use it), several market factors pushed the larger companies – more exposed to litigation and boycotting from advertising companies, collective management organizations and other commercial partners – to take action on the proliferation of illegal content in their platforms.

Alongside these commercial pressures to tackle the rampant copyright infringement, the exponential growth of violent content related to terrorism worried many EU public authorities, and brought about a myriad of national and European legislations enforcing procedures to take down certain kinds of illegal content[45]. Finally, in the last few years, the rise of hate speech also placed an additional pressure on these providers to enforce their terms of service and take some preventive actions against this kind of behaviours.

From the early 2000s, the most immediate solution for moderation in platforms, in online forums or services alike, was the adoption of administrators ("admins" or internal officers in the provider) and moderators ("mods", trusted individual users of the service, but the nomenclature may change) with the function and powers to police message boards, receive complaints, solve disputes, analyse the conformity of flagged content, block it and either suspend or ban the user that posted it. This approach has shown to be ineffective and somewhat flawed: 1) it is not scalable and replicable

[45] For example, European Commission, *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online* (C(2018) 1177 final), 01-mar.-2018. Available at European Commission: https://www.ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online (last accessed 14 April 2021); European Commission, *The Commission Code of Practice on Disinformation*, 16-mar.-2021. Available at European Commission: https://www.ec.europa.eu/digital-single-market/en/code-practice-disinformation (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

in many services; 2) it relies heavily on the users themselves, susceptible to bias, power abuse and may promote the emergence of echo-chambers; 3) and it is not nearly effective enough for the volume of content uploaded by users. In a recent example, the social network Parler used a system where all notices of illegal content and infringements of the Terms of Service were evaluated by panels of users, in a sort of court by peers. Some of the above-mentioned flaws occurred with great effect[46]. This kind of system needs to be complemented with other mechanisms[47].

From the late 2000s, the big platforms decided to employ algorithmic moderation[48], that is, to employ automated means of recognising illegal content, and later, to even work together in consortiums, such as the Global Internet Forum to Counter Terrorism (GIFCT), to aid in the enforcement of the European Commission's code of conduct to combat illegal online hate speech[49] within their respective services. Most forms of algorithmic moderation, such as matching, hash-matching and classification, in conjunction with

[46] It has been reported by several media organizations and in the court filings of the still ongoing case Parler LLC v. Amazon Web Services, Inc before U.S. District Judge Barbara Rothstein in the Western District of Washington, that prior to 6th January, Parler had failed to take down violent hate speech and that it admitted to having a backlog of over 26.000 complaints unanswered. See https://www.cnbc.com/2021/01/13/amazon-says-violent-posts-forced-it-to-drop-parler-from-its-web-hosting-service.html. (last accessed 14 April 2021).

[47] For example, Facebook still complements their automated systems with human moderators. This has also shown that this task takes an heavy toll on the individuals' mental health. See: BBC, *Facebook to pay $52m to content moderators over PTSD.* Available at BBC: https://www.bbc.com/news/technology-52642633 (last accessed 14 April 2021); and The Verge, *The Trauma Floor – The secret lives of Facebook moderators in America.* Available at The Verge: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona. (last accessed 14 April 2021).

[48] For more information, see Robert Gorwa/ Reuben Binns/ Christian Katzenbach, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance,* BD&S (28-fev.-2020). Available at Sage: https://www.journals.sagepub.com/doi/full/10.1177/2053951719897945 (last accessed 14 April 2021).

[49] European Commission, *The EU Code of conduct on countering illegal hate speech online.* Available at European Commission: https://www.ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en. (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

constantly updated databases of copyright protected works and illegal content, have proven themselves to have some effectiveness in finding "matches" and blocking illegal content – especially copyright infringements and terrorism related content. The matter of hate speech has proven itself to be much more difficult to address, due to the limitations of algorithms in understanding the nuances of speech and context itself.

Nevertheless, even algorithms are still flawed tools. They are prone to false negatives (users can still find means to circumvent their detection) and, to a much greater effect, false positives, that is, blocking lawful content. This is especially grievous in copyright detection systems, such as Youtube's Content ID System[50]. Because of the way the American DMCA and the European e-Commerce Directive constructed the liability – without redress mechanisms for the recipients and consequences for misuse – the service providers have an incentive to, even when in doubt, always block content. Then, the recipient that provided it, will also not have access to adequate (non-automated) redress options to appeal the automated decision – resulting in the phenomenon that lawmakers were initially trying to mitigate in the first place: collateral censorship and the infringement of the fundamental rights of user.

3.3. The Digital Service Acts and content moderation

Contrary to many people's expectations, the Commission's proposal for the DSA does not tackle the problem of intermediary liability and content moderation by attempting to reinvent the wheel and forcing a bigger surveillance by service providers. Instead, it aims to shed greater transparency over the whole process and give concrete uniform provisions for the action and takedown of illegal content, and the means for the affected users to appeal against decisions, in order to mitigate the risks of erroneous or unjustified

[50] Robert Gorwa/ Reuben Binns/ Christian Katzenbach, *Algorithmic content moderation* cit., 7-8.

Electronic copy available at: https://ssrn.com/abstract=3852280

blocking of lawful speech – a problem that we saw arose from overzealous platforms and rightsholders abusing their positions.

The DSA repeals articles 12 to 15 of the e-Commerce Directive, related to the "mere conduit", "catching", "hosting" and "no general obligation to monitor content", and replaces them with its own version – namely articles 3, 4, 5 and 7 of the Commission's proposal, as per article 71.

When comparing the articles in both texts it stands out that for the services of mere conduit and catching, the conditions for the exemption of liability stay the same, while for hosting services there was a inclusion of a provision lifting the exemption of liability for violations of consumer law by certain online marketplaces, a topic which will be further developed in section 4.5 of this article.

The principle of no general obligation to monitor content also persists in the new version (albeit with a different text) – as it was stressed by the Commission in the proposal's text[51]: "The proposed legislation will preserve the prohibition of general monitoring obligations of the e-Commerce Directive, which in itself is crucial to the required fair balance of fundamental rights in the online world. The new Regulation prohibits general monitoring obligations, as they could disproportionately limit users' freedom of expression and freedom to receive information and could burden service providers excessively and thus unduly interfere with their freedom to conduct a business. The prohibition also limits incentives for online surveillance and has positive implications for the protection of personal data and privacy."

The regulation also includes a novel "Good Samaritan" clause in article 6, which maintains the protection from liability of articles 3 to 5, for voluntary investigations launched by the service provider itself.

For the takedown of content, the proposal aims at establishing new rules for the relationships between service providers, public authorities, and judicial bodies in the articles 8 and 9, and between

[51] See the sections "Consistency with existing policy provisions in the policy area", "Fundamental Rights", "Other Elements" and Recital 28 of the proposal.

Electronic copy available at: https://ssrn.com/abstract=3852280

the provider and other private parties in article 14 and following. Both now have to comply with a series of requirements absent from the Directive, improving the transparency of the communication, reasoning and redress process. Orders from public entities must have statements of reason why the content is illegal, the relevant provisions of national and European law, and the scope of the order to block access, and procedures for both the provider and the recipient of the service that provided the content to defend themselves. In article 14, for private individuals and entities, the request for takedown must contain their identification, the clear location of the alleged content (may require exact URLs), a statement confirming that they are acting in good faith, and a full and comprehensive statement of reasons, abiding by the requiring of article 15, explaining why they alleged that the content should be considered illegal (if it pertains to copyright infringement, proof of being the actual rightsholder, for example).

Then, the DSA introduces in articles 16 and following a much-needed set of requirements, not applicable to micro or small enterprises, aimed at countering the effects of frivolous and automated notices, and overzealous takedowns of content, mitigating the effects of collateral censorship[52]: free internal complaint-handling systems, which are user-friendly, that function diligently and in a timely manner, capable of reversing wrongful decisions of takedown, with limited automation (article 17), out-of-court dispute resolution (article 18)[53], the suspension of the notice and action mechanism for actors whose complaints are frequently unfounded (article 20-2), the suspension for users that frequently provide illegal content (article 20-1), and a close contact and cooperation with trusted flaggers[54] (article 19). Trusted flaggers are legal persons, private or

[52] See Recital 47.

[53] Conducted by certified bodies, whose fees should be reasonable, and fully reimbursed by the provider to the user, if the dispute is solved in their favour.

[54] This concept of trusted flaggers was also already present in European Commission, *Commission Recommendation* cit., recitals 29 and 34, paragraphs 4 (g) and 25 to 27, with some differences in relation to the DSA. For example, in the Recommendation, Trusted flaggers could be individuals, natural persons.

Electronic copy available at: https://ssrn.com/abstract=3852280

public, recognised by Member States and European agencies, that possess special knowledge and experience in the identification of illegal content[55].

Regarding content moderation, the DSA implements new transparency requirements and brings actual balance to the way notice and takedown actions occur, ultimately protecting consumers' fundamental rights. It takes away the existing incentives that lead to service providers to engage in rampant over-blocking of alleged illegal content denounced, for instance, by their commercial partners and collective management organizations. It achieves this by shifting part of the burden from the content recipient to the denouncer and service provider, which has to ensure both a reliable notice and action mechanism, with consequences for its misuse, and an adequate redress process for the recipient.

4. Consumer protection in the Digital Services Act

Although the Digital Services Act is not structured with a view to protect consumers, there are several provisions in it that strengthen their position.

First of all, it is important to note that it is expressly stated that the EU acquis in the field of consumer law is not affected (see recital 10 and article 1-5(h) of the Proposal). The recital makes express reference to Directive 93/13/EEC[56], Directive 98/6/EC[57], Directive 2005/29/EC[58] and Directive 2011/83/EU[59], all amended by Directive (EU) 2019/2161)[60].

[55] See recitals 36 and 46.

[56] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[57] Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers.

[58] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council.

[59] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011

Electronic copy available at: https://ssrn.com/abstract=3852280

The fact is that, while it is generally argued that the consumer protection directives remain applicable, the principle of neutrality of digital platforms may affect the practical application of consumer law in many cases where it might be justified to hold platforms liable. The very consideration that platforms merely provide hosting services is, from the outset, very doubtful.

However, this is the regime we have, and the essence of the approach already taken by the e-Commerce Directive is maintained.

The definitions of consumer and trader (article 2(c) and (e) of the Proposal) are unsurprising and correspond to previous EU legal acts. Apart from the trader, it is also important to realise that the consumer relationship can be established directly between the consumer and the online platform. The truth is that this B2C relationship is not addressed directly and fully adequately by the Act. This is, in fact, one of our main criticisms in this context.

We will now move on to a brief successive analysis of the themes that seem most relevant to us from a consumer law perspective: traceability, pre-contractual information and product safety information, advertisement, recommender systems and liability of online platforms.

4.1. Traceability

One of the provisions of the Digital Services Act that is most aimed at consumer protection and which may be particularly relevant to consumers is the one that imposes duties on platforms to ensure the traceability of traders (see recital 49).

on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[60] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

Electronic copy available at: https://ssrn.com/abstract=3852280

Article 22 applies only to online platforms that allow consumers to conclude contracts with traders. The platform operator shall ensure that traders can only be present in the platform if they provide a series of relevant information regarding their identification. Apart from this duty, the platform operator shall also "make reasonable efforts" to assess whether the information is reliable, request the trader to correct the information that is inaccurate or incomplete, and suspend the trader until that correction is made. The information shall be stored for the duration of the contractual relationship between the parties. The consumer has the right to access this information "in a clear, easily accessible and comprehensible manner".

This information can be very important for the consumer to be able to exercise his rights against the trader.

4.2. Pre-contractual information and product safety information

Lost in article 22 is a provision that deals not with traceability but with the interface design of digital platforms.

Paragraph 7 stipulates that the online interface of the platform shall be designed and organised "in a way that enables traders to comply with their obligations regarding pre-contractual information and product safety information under applicable Union law".

We are talking about the information duties that are basically contained in the consumer law directives. Recital 50 expressly refers, as an example, to articles 6 and 8 of Directive 2011/83/EU (consumer rights), article 7 of Directive 2005/29/EC (unfair commercial practices) and article 3 of Directive 98/6/EC (indication of the prices).

The platform is intended to make it easier for the trader to comply with these information duties, thus ensuring that consumers have easier access to the information in question.

One issue that seems to be left open here is that of the consequences if platforms fail to comply with this obligation.

Electronic copy available at: https://ssrn.com/abstract=3852280

4.3. Advertisement transparency

Another aspect tackled by the Digital Services Act concerns consumer protection regarding the principle of identifiability of advertising. Article 24 requires the consumer to be immediately able and to clearly perceive each advertisement message as such.

The legislation goes even further by also requiring an indication of the person on whose behalf the advertising message is issued, that is, as a rule, the trader, with whom the consumer may then conclude a future contract.

The main parameters used to define on what basis the advertisement was shown to that particular person and not to another should also be indicated. The automation and personalisation of advertising make it possible to select the recipients increasingly precise and rigorous way, possibly giving rise to problems of discrimination and non-transparent practices linked to the collection and processing of consumer data.

In addition to the GDPR, this issue is also regulated by the Unfair Commercial Practices Directive, with which the Digital Services Act should be articulated in this field.

4.4. Recommender systems

The Digital Services Act also contains a provision to strengthen transparency around recommender systems (article 29). It is specially addressed to very large platforms, i.e. "platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million" (article 25).

Article 2(o) defines "recommender system" as "a fully or partially automated system used by an online platform to suggest in its online interface specific information to the service recipients, as a result of a search initiated by the recipient included, or otherwise determining the relative order or prominence of information displayed".

Electronic copy available at: https://ssrn.com/abstract=3852280

It is recognised in recital 62 that the prioritisation and presentation of the information is an important part of the platform's business. Examples of such practices include algorithmic suggestions, rankings and the order in which information is presented. Much of the success of these large platforms lies precisely in the way information is presented. This is what consumers most look for.

The Digital Services Act aims to ensure that, with regard to the information presented, consumers are, on the one hand, adequately informed about the criteria for presenting it in a particular way and, on the other hand, are able to influence the way it is presented. The online platforms must give consumers several alternative possibilities regarding the main parameters for prioritisation of information, including at least one that is not based on profiling. The possibilities should be easily accessible.

The possibility of these recommender systems being an instrument for the dissemination of fake news or other illegal information means that risk analysis and mitigation measures by very large online platforms should also take them into account (articles 26-2 and 27-1).

4.5. Liability

We now turn to the analysis of what seems to us to be the most relevant and innovative provision of the Digital Services Act in relation to consumer protection.

Under article 5-3, the general principle of non-liability of hosting service providers shall not apply "with respect to liability under consumer protection law of online platforms allowing consumers to conclude distance contracts with traders, where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue in a way that 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".

We present three main criticisms of this provision.

Electronic copy available at: https://ssrn.com/abstract=3852280

Firstly, it is not at all clear what is meant by "where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue". It will probably be the information that can be accessed on the online platform, in which case, we think it can be stated in rather a clearer way.

The second problematic element in this very important rule is the effective materialisation of the concept of "average and reasonably well-informed consumer", which leads to some legal uncertainty. Although there is already some CJEU case law on the matter, the boundaries are very blurred. Relying on this concept for this purpose, which is so relevant, seems that it might not be the best solution.

The same can be said about the concept of "acting under its authority or control", which is the decisive element of this provision. Does Airbnb exercise control over hosts? We would say yes, under the terms of this provision, but we suspect many people, certainly including Airbnb itself, will say no. We are presented a concept which raises this kind of difficulties in relation to a platform like Airbnb, which clearly has a control over hosts, or at least should have some degree of responsibility, because of the importance it has in the contract entered into through it. And the truth is that at this moment it is virtually impossible to say what the interpretation of the regulation will be[61].

Another issue that can be raised here is the actual scope of the liability exemption when consumer protection provisions are at stake. At least as regards consumer sales and the supply of digital content or digital services it seems possible to hold platforms liable for the lack of conformity of the digital good, digital content or digital service even in cases not foreseen in this article of the Digital Services Act.

Using Directive 2019/771 as a reference, it follows from its recital 23: "Member States should remain free to extend the appli-

[61] On this issue, see the article 20 of the ELI Model Rules on Online Platforms, which impose the liability of the platform operator with predominant influence. See Joana Campos Carvalho, *Online Platforms: Concept, Role in the Conclusion of Contracts and Current Legal Framework in Europe*, 12/1 CDT (2020), 863-874, 873-874.

Electronic copy available at: https://ssrn.com/abstract=3852280

cation of this Directive to platform providers that do not fulfil the requirements for being considered a seller under this Directive", i.e., platforms that are providing hosting services as intermediaries between the consumer and the trader[62]. Member States may thus provide that the platform is liable for the lack of conformity of the goods sold by a third party.

5. Conclusion

The Commission's proposal reveals itself both too ambitious and not ambitious enough. As we have outline in this text, it serves neatly its purpose of uniformization of many horizontal matters in e-Commerce, successively updating many principles and provisions for Digital Services in the European Internal Market. It also aims to complement the GDPR in several areas, namely the right of information, data collection and tracking for profiling in advertisement and recommender systems – but in this regard, the EDPS raised some criticisms that should be considered during the legislative process.

On the matter of content moderation, we have showcased the existing legal framework, its origins and flaws, and how the DSA attempts to correct them by building upon the e-Commerce Directive's principles and codifying many provisions from the Commissions' recommendation of 2018 – with a great focus on transparency and redress procedures on decisions to block access to alleged illegal content. If implemented, these changes will certainly cause a great effect worldwide due to the objective scope of the regulation and the value of the European Single Market – even if other legal orders (such as the United States) do not address these issues, the so-called Brussels effect[63] will push private enterprises to comply and give rise to similar legislative initiatives.

[62] Jorge Morais Carvalho, *Sale of Goods and Supply of Digital Content and Digital Services*, 5 EuCML (2019), 194-201, 196.

[63] For more information regarding the soft power of European regulation worldwide, see https://www.brusselseffect.com.

Electronic copy available at: https://ssrn.com/abstract=3852280

Yet, as the EDPS is critical of the provisions regarding data protection in the DSA, many others have also been disapproving on its approach to content moderation, claiming that it does not "go far enough". Some warn of the dangers to freedom of expression posed by systems of privatised content control and that the rules on enforcement and redress should be improved[64], while others in the European Parliament call for an expansion of its scope to include "harmful content"[65]. The next phases of the legislative process might become the opening of the Pandora's Box on this regard, and the nature of its impact (whether positive or negative) is still unclear.

Finally, we have also addressed how the provisions regarding consumer protection are welcomed and flawed in many instances. The regulation should have consumer protection as an explicit objective, reflected in its provisions[66]. Many of the proposal's provisions lack clarity and use concepts that will leave many consumers without protection and in legal uncertainty, especially those regarding platform's liability. While innovative, the DSA clearly struggles on this regard and should articulate better with the existing European consumer law acquis.

The next phases of the legislative procedure of this regulation will prove to be crucial. There are very different policy views regarding the matters addressed in the proposal, present in both the European Council and the Parliament. For now, the Commission's initiative will mark the agenda, but the upcoming debates will certainly be very interesting. On the other side of the Atlantic, the political will to initiate the legislative process is also brewing.

We shall continue to pay close attention to this topic.

[64] EPRS, *Digital Services Act* cit., 8-9.

[65] See the European Parliament resolution on the Digital Services Act and fundamental rights issues posed doc. 2020/2022(INI), 20-oct.-2020 and the EPP position. Available at EPP: https://www.eppgroup.eu/newsroom/publications/epp-group-position-on-the-digital-services-act-dsa (last accessed 14 April 2021).

[66] BEUC, *EU proposals to shape the digital landscape, a step forward for consumers*. Available at BEUC: https://www.beuc.eu/blog/eu-proposals-to-shape-the-digital-landscape-a-step-forward-for-consumers/ (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

Reference List

BBC, *Facebook to pay $52m to content moderators over PTSD*. Available at BBC: https://www.bbc.com/news/technology-52642633 (last accessed 14 April 2021).

BEUC, *EU proposals to shape the digital landscape, a step forward for consumers*. Available at BEUC: https://www.beuc.eu/blog/eu-proposals-to-shape-the-digital-landscape-a-step-forward-for-consumers/ (last accessed 14 April 2021).

Carvalho, Joana Campos, *Online Platforms: Concept, Role in the Conclusion of Contracts and Current Legal Framework in Europe*, 12/1 CDT (2020), 863-874.

Carvalho, Jorge Morais, *Sale of Goods and Supply of Digital Content and Digital Services*, 5 EuCML (2019), 194-201.

Carvalho, Jorge Morais, *Airbnb Ireland Case: One More Piece in the Complex Puzzle Built by the CJEU Around Digital Platforms and the Concept of Information Society Service*, 6/2 ItalLJ (2020), 463-476.

Carvalho Jorge Morais, *Sentenças Airbnb Ireland e Star Taxi App, Conceito de Serviço da Sociedade da Informação e Regulação de Plataformas Digitais*, RDC – Liber Amicorum (2021), 481-510.

EDPS, Opinion 1/2021 (10.02.2021). Available at EDPS: https://edps.europa.eu/system/files/2021-02/21-02-10opinion_on_digital_services_act_en.pdf (last accessed 14 April 2021).

EDPS, *Press Release: EDPS Opinions on the Digital Services Act and the Digital Markets Act, Brussels* (10.02.2021), 1. Available at EDPS: https://edps.europa.eu/system/files/2021-02/edps-2021-01-opinion-on-digital-services-act-package_en.pdf (last accessed 14 April 2021).

Gorwa, Robert / Binns, Reuben / Katzenbach, Christian, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance,* BD&S (28-fev.-2020). Available at Sage: https://journals.sagepub.com/doi/full/10.1177/2053951719897945 (last accessed 14 April 2021).

Sartor, Giovanni, *Providers Liability: From the eCommerce Directive to the future*, Directorate General For Internal Policies Policy Department A: Economic And Scientific Policy (2017), 9. Available at Europarl: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf (last accessed 14 April 2021).

Electronic copy available at: https://ssrn.com/abstract=3852280

The Verge, *The Trauma Floor – The secret lives of Facebook moderators in America*. Available at The Verge: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona. (last accessed 14 April 2021).

Valcke, Peggy / Lenaerts, Marieke, *Who's author, editor and publisher in user-generated content? Applying traditional media concepts to UGC providers*, 24/1 Int'l Rev L Comp & Tech (2010), 119-131.

Electronic copy available at: https://ssrn.com/abstract=3852280