*“Sometimes it is the people no one can imagine anything of,*
*who do the things no one can imagine”*

- *Alan Turing, the father of internet*

# INDEX

# INTRODUCTION

Already since the late 20th century, European institutions, along with their American counterparts, commonly decided to embrace technological progress and the development of digital infrastructures, choosing to adopt a strategy of economic liberalism and relaxed regulations in the field of internet, with the aim of promoting the growth of new digital technologies for the benefit of human progress and to ensure the emergence of a vibrant and competitive economy within the dynamics of international relations.

Precisely by virtue of such autonomy, online intermediaries were left free to grow out of control by public regulators and expeditiously started to exert a "private" form of authority that combined private law and automated technologies, by massively subjecting users to their own corporate regulations, and thereby exercising dominance in the form of a quasi-legislative power.

As a result, in the absence of any regulation governing the manner in which such platforms can operate online, new risks and hazards to the security of online users have spread uncontrollably during the last two decades, jeopardizing the safeguarding of fundamental rights that were once taken for granted within Western democracies, alongside emerging rights within the context of the new digital economy, that include, for instance, freedom of expression, privacy, freedom to conduct a business, as well as the right to be forgotten and the protection of personal data.

Crimes such as incitement of violence and hatred, the dissemination of terrorist and violent extremist content, the creation of misinformation through fake news, and the distribution of child pornography have indeed become widespread realities on the platforms of major digital market operators globally.
These offenses have not only attracted the attention of leading European regulators dedicated to safeguarding the rights of online consumers, resulting in the imposition of new restrictions and exorbitant economic sanctions, but have also emerged as elements of significant strategic value for companies operating in the digital market, as they possess the power to influence

the success and outcome of huge multi-billion-dollar transactions and have the capacity to deceive the very course of financial markets.

Precisely due to this reason, the European institutions have decided to work towards the creation of a new legislative framework for the regulation of the digital economy, adopting a specific strategy for the establishment of a fair and competitive single market, titled "Shaping Europe's Digital Future", which, for the first time, outlined a roadmap towards what many have referred to as a true process of "Digital Constitutionalism".
Following in the footsteps of this strategy, on December 15th, 2020, the European Commission presented the proposal for a new "Digital Services Package", comprising its two components: the "Digital Market Act" for regulating competition in the digital market, and the "Digital Services Act" for regulating online content circulating on digital service intermediary platforms.

With reference to the latter, the DSA establishes a new regulatory framework aimed at fostering a safer digital environment within the European Union and at elevating the level of consumer protection for the benefit of a fairer and competitive digital market. In doing so, the Regulation imposes both a regime of accountability which is inspired by the previous model of the e-Commerce directive, and new due-diligence obligations on digital services providers, with a specific emphasis on "online platforms" such as social media and marketplaces, and "very large online platforms" (VLOPs) along with "very large online search engines" (VLOSEs), which include the well known tech giants belonging to the so-called GAFAM circle (Google, Apple, Facebook, Amazon, Microsoft).
The legislative objective behind such provisions is therefore to enhance both the transparency and liability standards applicable to these platforms.

Within the third chapter, the regulation on the civil liability of online service intermediaries is therefore outlined, starting from the need for an overall harmonization of the subject across the entire territory of the Union and from the premise of a lack of clarity in various parts of the e-Commerce Directive, which the DSA takes inspiration from, while leaving the majority of the provisions contained therein substantially unchanged.
After having provided a brief overview of the longstanding debate regarding the liability regime for online platforms in relation to third-party unlawful activities, this chapter proceeds to elucidate the series of developments that culminated in the establishment of the new

liability regime under the Digital Services Act (DSA), taking its first steps from the legislations originally enacted in the United States during the late 1990s, namely the Digital Millennium Copyright Act and the Communications Decency Act, and subsequently delving into a comprehensive analysis of the directive which serves as the fundamental cornerstone of the European legal framework on internet service providers' civil liability, namely the e-Commerce Directive. Throughout such analysis, a critical and detailed assessment is thus outlined on the various challenges emerged over the past two decades, underlining the various critical issues that have come to the fore in the context of both the national and European jurisdictions.

Among these, particular attention is devoted to certain issues such as the challenging distinction between so-called active intermediaries and passive intermediaries, as well as the problematic definition of the so-called "actual knowledge" of the unlawful act.

As for the first issue, the study begins with a careful evaluation of the liability regime outlined in the e-Commerce Directive, which, by providing a series of liability exemptions for certain categories of online intermediary service providers (known as safe harbors), implicitly draws the distinction between subjects that, operating in a passive and neutral manner, deserve protection from liability for third-party actions, and actors that, by employing more advanced techniques of control and monitoring within their platforms, can only be considered active subjects in their own online activities and, therefore, not eligible for any liability exemption if illegal content were to circulate within their platforms.
This distinction, that, although being implicitly understood in the legislative text, lacks explicit articulation within the e-commerce directive, has found however fertile ground for its elaboration within the multiple judgments of the Court of Justice of the European Union, being reaffirmed in several of its notable rulings, with the most significant ones undoubtedly being the L'Oreal and Google France cases.
The text further delineates how such a distinction runs also the risk of disregarding the current state of the art of online information services, which, being predominantly equipped with advanced search and monitoring mechanisms, based mostly on artificial intelligence systems, have now the potential to be categorized as active providers in the vast majority of cases.

Similarly, the cryptic definition of "actual knowledge" of illicit activities referred to in Article 14 of the same directive is thus taken into consideration. According to this provision, in the

absence of any good-faith action to remove the content or block the profile that may have caused harm, the service provider could be held liable for the third party's action and subject to sanctions under European law. However, lacking within the Directive any explicit guidance on how such knowledge could be acquired, it is taken under analysis the abundant case law developed over the past years on this specific topic, evaluating the solutions provided by both the European Court of Justice and the individual national jurisdictions, and giving particular attention to the recent Italian judicial rulings that have shaped the Italian legal landscape in recent years, in terms of civil liability of ISPs.

Particular attention is placed on the specific concept of a "diligent economic operator" developed by the Court of Justice of the European Union and subsequently embraced by several national supreme courts. This principle asserts that only an intermediary who is unaware of a specific illicit act, having acted in good faith and adhered to industry-specific professional standards, can be deemed exempt from liability, thus benefiting from the "safe harbors" provided by the legislation.

Specifically, at this regard, the question arises as to the likelihood that such a theoretical framework could effectively avoid the risk of discretion exercised by individual economic operators, which are primarily motivated by the economic objective of minimizing potential civil sanction costs, and therefore pushed to excessively remove online content, in order to safeguard themselves preemptively from accusations by European and national authorities.

The analysis ultimately proceeds to analyse the new regime of civil liability for online intermediaries, as incorporated within the DSA. The Regulation, while largely preserving the essence of the provisions previously outlined in the e-commerce directive, introduces some innovative elements based on the jurisprudential experience of the Court developed over the years and on the emerging needs associated with the ever-evolving technological advancements.

Therefore, the DSA primarily seeks to crystallize the principle of the "diligent economic operator", as already previously established by the CJEU, establishing that, in order to be exempt from liability, it is necessary that the intermediaries have no knowledge of illicit acts that could potentially involve them, while also acting duly, in accordance with industry practices and in good faith. Moreover, it further specifies that for a notification of illicit conduct by third parties to be deemed valid and thereby trigger awareness on the part of the intermediary, it is also necessary for the notification to be sufficiently precise and adequately substantiated.

As for the distinction between active and passive providers, while maintaining the same two categories already previously developed by the Court of Justice over the years, without particularly developing such concepts, the new Regulation provides some clarifications to better define the circumstances under which a provider can indeed be considered active or passive and therefore eventually responsible for illegal content circulating on its platform. Specifically, it incorporates the Anglo-Saxon concept of the "Good Samaritan", whereby, while the requirements of passivity and neutrality for providers to qualify for liability exemptions remain substantially unaffected, the online services intermediaries can now be shielded from liability, with reference to all those internal control and monitoring activities, necessary to identify and remove illegal contents promptly and without delay.
Thus, it is evident the substantial persistence of some of the issues that had already characterized the e-Commerce directive, particularly the ongoing inability to determine with certain and unequivocal criteria the elements by which a specific content can be deemed illegal by a provider, regardless of the specificity of external reports.

Lastly, the fourth chapter proceeds with an exposition of all the new due diligence obligations envisaged by the Regulation, which, undoubtedly, constitute the primary innovation introduced by the Digital Services Act, aimed at implementing new standards of conduct for companies operating in the digital sector, and at introducing a new concept of corporate sustainability, to the benefit of all the parties involved in the company's activities.
In this regard, we refer to the so-called "Russian Dolls" System, whereby the new obligations are assessed based on the size and social impact of the specific activities carried out by individual internet service providers, which are therefore divided into four major categories, each burdened with increasingly stringent obligations. These categories include "intermediary service providers", "hosting services providers", the new "online platforms", the "very large online platforms" (VLOPs) and the "very large online search engines" (VLOSEs).

# INTRODUZIONE

Già a partire dalla fine del XX secolo, le istituzioni europee, insieme anche a quelle americane, decisero comunemente di percorrere la strada del progresso tecnologico e dello sviluppo di nuove infrastrutture digitali, scegliendo di adottare una strategia di liberalismo economico ed un regime di laissez-faire nel settore di internet, allo scopo di promuovere lo sviluppo di nuove tecnologie digitali a beneficio del progresso umano, e di assicurare l'insorgere di un'economia vivace e competitiva, nell'ambito delle dinamiche dei rapporti internazionali.

Proprio in virtù di tale autonomia, gli intermediari online sono stati lasciati liberi di crescere al di fuori di controlli da parte dei regolatori pubblici e hanno iniziato rapidamente ad esercitare una vera e propria forma di autorità "privata", conciliante diritto privato e tecnologie automatizzate, sottoponendo in modo massiccio gli utenti alle proprie regole aziendali ed esercitando così un potere dal carattere quasi legislativo.

Di conseguenza, in assenza di una vera e propria regolamentazione che disciplinasse il modo in cui tali piattaforme possono operare online, nuovi rischi e pericoli per la sicurezza degli utenti si sono andati diffondendo incontrollabilmente online, nell'arco degli ultimi due decenni, mettendo a rischio la salvaguardia di diritti fondamentali, da tempo dati ormai per scontati nell'ambito delle democrazie occidentali, insieme ai nuovi diritti emergenti nel contesto della nuova economia digitale, tra i quali complessivamente possono essere richiamati il diritto alla libertà di espressione, il diritto alla privacy, la libertà di svolgere attività commerciali, nonché il diritto all'oblio ed alla protezione dei dati personali.

Crimini come l'incitamento alla violenza e all'odio, la diffusione di contenuti terroristici e di estremismo violento, la creazione di disinformazione attraverso fake news e la distribuzione di pornografia minorile sono ormai diventati realtà diffuse sulle piattaforme dei principali operatori del mercato digitale a livello globale.
Tali reati, non solo hanno attirato l'attenzione dei principali regolatori europei incaricati della tutela dei diritti dei consumatori online, portando all'imposizione di nuove restrizioni e

sanzioni economiche esorbitanti, ma sono anche emersi come elementi dal notevole valore strategico per le società operanti nel mercato digitale, dal momento che esse hanno il potere di influenzare il successo e l'esito di enormi transazioni multimiliardarie e la capacità di trarre in inganno l'andamento stesso dei mercati finanziari.

Esattamente per questa ragione, le istituzioni europee hanno preso la decisione di adoperarsi per la creazione di un nuovo quadro normativo per la regolamentazione dell'economia digitale, adottando una specifica strategia per l'istituzione di un mercato unico equo e competitivo, intitolata "Shaping Europe's Digital Future", la quale, per la prima volta, ha delineato un percorso verso ciò che molti hanno definito un vero e proprio processo di "costituzionalismo digitale".
Seguendo le orme di questa strategia, il 15 dicembre 2020, la Commissione europea ha presentato la proposta per un nuovo "pacchetto dei servizi digitali", articolato nelle due sue componenti: il "Digital Market Act" per regolare la concorrenza nel mercato digitale, ed il "Digital Services Act" per regolare i contenuti online che circolano sulle piattaforme di intermediazione dei servizi digitali.

Con riferimento a quest'ultimo, il DSA stabilisce un nuovo quadro normativo volto a favorire lo sviluppo di un ambiente digitale più sicuro all'interno dell'Unione europea e ad elevare il livello di protezione dei consumatori a vantaggio di un mercato digitale più equo e competitivo. A tal scopo, il Regolamento stabilisce sia un regime di responsabilità ispirato al modello della precedente direttiva e-Commerce, sia nuovi obblighi di diligenza per i fornitori di servizi digitali, con un'enfasi particolare verso le "piattaforme online", come i social media e i marketplace, e verso i fornitori di "piattaforme online di dimensioni molto grandi" insieme ai fornitori di "mortori di ricerca online di dimensioni molto grandi", i quali includono i noti giganti tecnologici appartenenti alla cosiddetta cerchia GAFAM (Google, Apple, Facebook, Amazon, Microsoft).
L'obiettivo del legislatore rispetto a tali disposizioni risulta quindi essere quello di migliorare sia gli standard di trasparenza che di responsabilità applicabili nei confronti di tali piattaforme.

All'interno del terzo capitolo viene quindi delineata la disciplina sulla responsabilità civile degli intermediari dei servizi online, a partire dall'esigenza di un'armonizzazione globale della materia su tutto il territorio dell'Unione e dal presupposto di una mancanza di chiarezza

in diverse parti della direttiva sull'e-Commerce, dalla quale il DSA trae ispirazione, pur lasciando sostanzialmente inalterate la maggior parte delle disposizioni in essa contenute.
Dopo aver fornito una breve panoramica sul dibattito di lunga data inerente al regime di responsabilità per le piattaforme online, in relazione alle attività illecite compiute da terzi, questo capitolo procede ad illustrare la serie di sviluppi che hanno portato all'istituzione del nuovo regime di responsabilità ai sensi del Digital Services Act (DSA), prendendo spunto dalle legislazioni originariamente emanate negli Stati Uniti verso la fine degli anni 90, vale a dire il Digital Millennium Copyright Act e il Communications Decency Act, e successivamente svolgendo un'analisi esaustiva della direttiva che avrebbe rappresentato la pietra miliare fondamentale del quadro normativo europeo sulla responsabilità civile dei fornitori di servizi internet, ossia la direttiva sull'e-Commerce. Nel corso di tale analisi, viene quindi presentata una valutazione critica e dettagliata delle diverse sfide emerse nel corso degli ultimi due decenni, sottolineando le diverse criticità emerse alla ribalta nel contesto di entrambe le giurisdizioni nazionali ed europee.

Tra queste, particolare attenzione è dedicata a questioni come l'ardua distinzione tra intermediari attivi e intermediari passivi, nonché alla problematica definizione della cosiddetta "effettiva conoscenza" del fatto illecito.

Per quanto riguarda il primo problema, lo studio inizia con un'attenta valutazione del regime di responsabilità civile delineato all'interno della Direttiva e-Commerce, il quale, prevedendo una serie di esenzioni da responsabilità per determinate categorie di fornitori di servizi intermediari online (conosciute come "safe harbors"), delinea implicitamente una distinzione tra soggetti che, operando in modo passivo e neutrale, meritano protezione dalla responsabilità per le azioni di terzi, ed attori che, mediante l'uso di tecniche avanzate di controllo e monitoraggio all'interno delle loro piattaforme, non possono che essere considerati soggetti attivi nelle proprie attività online e, pertanto, non idonei a qualunque tipo di esenzione da responsabilità nell'eventualità in cui contenuti illegali dovessero circolare all'interno delle loro piattaforme.
Tale distinzione, che, sebbene implicitamente compresa all'interno del testo legislativo, manca però di un'esplicita rappresentazione all'interno della Direttiva e-Commerce, ha trovato tuttavia terreno fertile per la sua elaborazione all'interno delle numerose sentenze della Corte di Giustizia dell'Unione Europea, che l'hanno ribadita in diverse pronunce, tra le quali le più significative sono, senza dubbio, i famosi casi L'Oréal e Google France.

Il testo delinea inoltre come tale distinzione comporti altresì il rischio di trascurare lo stato dell'arte dei servizi dell'informazione online, i quali, essendo principalmente dotati di meccanismi avanzati di ricerca e monitoraggio, basati principalmente su sistemi di intelligenza artificiale, hanno ora il potenziale per essere classificati come fornitori attivi nella stragrande maggioranza dei casi.

Analogamente, viene presa in considerazione la criptica definizione di "effettiva conoscenza" delle attività illecite, di cui all'articolo 14 della stessa direttiva. In base a tale disposizione, in assenza di azioni in buona fede per rimuovere i contenuti o bloccare il profilo che potrebbe aver causato dei danni, il fornitore di servizi potrebbe essere ritenuto responsabile per l'azione di terzi e soggetto a sanzioni ai sensi del diritto europeo. Tuttavia, in assenza nella direttiva di alcun esplicito riferimento circa le modalità con cui acquisire tale conoscenza, viene dunque analizzata l'abbondante giurisprudenza sviluppatasi negli ultimi anni su questo specifico argomento, valutando le soluzioni fornite sia dalla Corte di Giustizia europea che dalle singole giurisdizioni nazionali, e prestando particolare attenzione alle recenti sentenze giudiziarie italiane, le quali hanno plasmato il quadro legislativo italiano degli ultimi anni, in tema di responsabilità civile degli ISP.
Si presta poi particolare attenzione al concetto specifico di "operatore economico diligente" sviluppato dalla Corte di Giustizia dell'Unione Europea e successivamente adottato da diverse corti supreme nazionali. Tale principio afferma che solo un intermediario che non risulti essere a conoscenza di un atto illecito, avendo agito in buona fede e avendo aderito agli standard professionali specifici del settore, può essere considerato esente da responsabilità, beneficiando così dei "safe harbor" previsti dalla disciplina.
In particolare, ci si interroga circa le probabilità che un tale quadro teorico possa effettivamente evitare il rischio di discrezionalità esercitata da singoli operatori economici, i quali sono principalmente motivati dall'obiettivo economico di ridurre al minimo i costi potenziali delle sanzioni civili, e sono quindi spinti a rimuovere in maniera eccessiva i contenuti online, al fine di tutelarsi preventivamente da accuse da parte delle autorità europee e nazionali.

L'analisi procede infine ad esaminare il nuovo regime di responsabilità civile per gli intermediari online, così come incorporato nel DSA. Il Regolamento, pur preservando in gran parte l'essenza delle disposizioni precedentemente delineate nella Direttiva e-Commerce, introduce alcuni elementi innovativi basati sull'esperienza giurisprudenziale della Corte,

sviluppata nel corso degli anni, e sulle emergenti esigenze legate agli sviluppi tecnologici in continua evoluzione.
Pertanto, il DSA cerca principalmente di cristallizzare il principio dell'"operatore economico diligente", già precedentemente stabilito dalla CGUE, stabilendo che, al fine di essere esentati da responsabilità, è necessario che gli intermediari non abbiano conoscenza di atti illeciti che potrebbero coinvolgerli, ed agiscano correttamente, in maniera conforme alle pratiche del settore ed in buona fede. Inoltre, il DSA stabilisce ulteriormente che, affinché una notifica di fatto illecito da parte di terzi sia considerata valida e possa dunque innescare la consapevolezza dello stesso da parte dell'intermediario, è necessario che la segnalazione sia sufficientemente precisa ed adeguatamente motivata.
Per quanto riguarda la distinzione tra fornitori di servizi attivi e passivi, pur mantenendo le stesse due categorie già sviluppate dalla Corte di Giustizia nel corso degli anni, senza sviluppare particolarmente tali concetti, il nuovo Regolamento fornisce alcuni chiarimenti volti a definire meglio le circostanze in cui un fornitore potrebbe essere considerato attivo o passivo e quindi eventualmente responsabile dei contenuti illegali che circolano sulla sua piattaforma. In particolare, viene recepito il concetto di origine anglosassone del c.d. "buon samaritano", secondo cui, sebbene i requisiti di passività e neutralità per beneficiare delle esenzioni da responsabilità rimangano sostanzialmente invariati, gli intermediari dei servizi online possono ora essere protetti da responsabilità, con riferimento a tutte quelle attività interne di controllo e monitoraggio, necessarie per identificare e rimuovere tempestivamente e senza indugi i contenuti illeciti.
Dunque, risulta evidente la sostanziale persistenza di alcune delle problematiche che avevano già in precedenza caratterizzato la Direttiva e-Commerce, con particolare riferimento all'incapacità di determinare con criteri certi ed inequivocabili gli elementi attraverso i quali un determinato contenuto potrebbe essere considerato illegale da parte di un fornitore di servizi online, indipendentemente dalla specificità delle segnalazioni esterne.

Infine, nel quarto capitolo viene esposto l'insieme degli obblighi di diligenza previsti dal Regolamento, i quali costituiscono senza dubbio l'innovazione principale introdotta dal Digital Services Act, finalizzata a implementare nuovi standard di condotta per le aziende operanti nel settore digitale e ad introdurre un nuovo concetto di sostenibilità aziendale, a vantaggio di tutte le parti coinvolte nelle attività dell'azienda.
A tal proposito, si fa riferimento al c.d. sistema delle "bambole russe", in cui i nuovi obblighi vengono valutati in base alla dimensione ed all'impatto sociale delle specifiche attività svolte

dai singoli fornitori di servizi Internet, i quali vengono quindi suddivisi in quattro categorie principali, ciascuna gravata da obblighi sempre più stringenti. Queste categorie includono “prestatori di servizi intermediari”, “fornitori di servizi di hosting”, le nuove “piattaforme online”, le “piattaforme online di “dimensioni molto grandi” ed i “motori di ricerca online di dimensioni molto grandi”.

# Chapter 1

# THE ROLE OF DIGITAL PLATFORMS: TOWARDS A NEW APPROACH TO CORPORATE SUSTAINABILITY

## 1. Premise

After having become the biggest shareholder in Twitter, on the 4th April, 2022, with a stake of 9.2%, worth nearly $3 billion at the time, the visionary, eccentric billionaire, Elon Musk, gave rise to a long and controversial saga, spanning several months, which would have ultimately culminated in his complete acquisition of the Twitter platform, on the October 27th, 2022, for a total value of $54.20 per share, or $44 billion.[1] A price tag which, for many, would have led to consider this as one of the most overpaid tech acquisitions in the history of M&A deals.[2]

Prior to reaching the ultimate conclusion of the agreement, a series of events unfolded, marked by accusations and legal battles, which temporarily jeopardized the integrity of the whole transaction, leading to a substantial devaluation of the platform's worth. Already on May 13th, in fact, despite having managed to secure over $7 billion in external funding for the transaction, Elon Musk expressed some reservations on the prosecution of the transaction, announcing that the deal was being "temporarily suspended", at least until receiving comprehensive details on the reliability of Twitter's assertions that the percentage of spam or fake accounts among its users was lower than 5%.

---

[1] MILMO, *The twisty, drama-filled Elon Musk-Twitter saga: a timeline*, in *The Guardian*, October 28, 2022, https://www.theguardian.com/technology/2022/oct/28/elon-musk-twitter-saga-timeline;

[2] DANIEL, *Elon Musk's $44 billion Twitter purchase is 'one of the most overpaid tech acquisitions in history,' Wedbush's Dan Ives says. Twitter's fair value is only $25 billion*, in *Fortune*, October 27, 2022, https://fortune.com/2022/10/27/elon-musk-twitter-purchase-most-overpaid-tech-history-dan-ives-wedbush/;

Nonetheless, Musk affirmed his commitment to completing the acquisition. It was in fact not until May 17th that the position of the Tesla CEO became more resolute, as he declared that the deal could not proceed anymore until all concerns regarding the accurate calculation of spam accounts were resolved. The social media company, therefore, was required to substantiate that fake or spam accounts actually present on the platform were not exceeding 5% of the total, as already claimed by the company before. These accounts, commonly referred to as "bot accounts", operate automatically without the need for human intervention, taking advantage of reply functions and direct messages to disseminate advertisements or scams to users, as well as exerting influence over public discourse, by disseminating messages of political propaganda, and fraudulently enhancing the performance indicators of individual users, who can procure followers, likes and retweets from bot sellers that exercise control over a vast number of fake accounts, reaching into the thousands or even millions.
On the basis of such allegation, the billionaire would have then taken the formal decision to terminate the deal in the following months and, indeed, on July 8th, Musk publicly announced his withdrawal from the agreement, alleging that Twitter was "in material breach of multiple provisions" contained in the acquisition agreement.
Somewhat easy to predict, on July 12th, Twitter lodged a lawsuit in Delaware, the place of its incorporation, seeking to compel Musk to fulfil the deal on the agreed-upon terms and, surprisingly, after a failed attempt to countersuit the platform and to delay the trial, on October 4th, Musk ultimately offered to acquire Twitter as originally intended, adhering to the terms agreed upon in April, and successfully completing the transaction only on October 27th, 2022.

Even though at the end of this long and controversial saga, Elon Musk ultimately completed his $44 billion takeover of Twitter, taking control of the company and firing several top executives, including the previous chief executive, Parag Agrawal,[3] from the experience coming from this case it is possible to draw a significant conclusion concerning the weaknesses of large digital platforms operating online, which allows to analyse issues related to their transparency in managing users data and fake news, as well as problematics concerning the spread of fake accounts and illegal content. Such information, in fact, not only now represent elements of intrinsic commercial value, being capable of influencing the positive or negative trend of large online platforms and of misleading entire financial markets

[3] PAUL, *Elon Musk completes Twitter takeover and 'fires top executives'*, in *The Guardian*, October 28, 2022, https://www.theguardian.com/technology/2022/oct/27/elon-musk-completes-twitter-takeover;

based on potentially deceptive data, but they also represent indicators of enormous strategic relevance within the digital sector, as they can provide a picture of the companies' health status.

When the negotiation was still stalled due to the disagreements related to the bots issue and the agreement seemed ready to collapse at any moment, Musk declared that the information in question was fundamental to Twitter's business and financial performance, and was needed to finish the acquisition.[4] Accordingly, one of the biggest M&A transactions in the recent history of the high-tech acquisitions could have collapsed due to a simple lack of transparency regarding the internal management and algorithmic processes governing the platform's internal functioning.

This provides an understanding of how issues such as content moderation, user profiling, geolocation, and others have become integral aspects of these contemporary high-tech multinational entities. They are no longer mere ancillary elements of internal organization or supplementary services aimed at improving user experience. Nowadays, they represent the true core businesses of some of the world's largest corporations, and their proper management has become crucial for the success of multi-billion commercial transactions and the protection of users' rights. If on the one hand, in fact, it is evident that these platforms have facilitated significant global productivity growth and interconnected the world, thereby embodying the essence of the second industrial revolution, on the other hand, they have also assumed the role of enablers for harmful and illegal activities, including the incitement of violence and hatred, the dissemination of terrorist and violent extremist content, the creation of misinformation through fake news and the distribution of child pornography.[5] As a result, in recent years, the management of content has become a critical issue both in terms of business and financial evaluations, as well as in terms of regulation, social impact and human rights.

[4] PAUL, *Elon Musk withdraws $44bn bid to buy Twitter after weeks of high drama*, in *The Guardian*, July 9, 2022, https://www.theguardian.com/technology/2022/jul/08/elon-musk-buy-twitter-withdraw;

[5] PRISCO, *Finanza sostenibile, l'impatto ESG sulla gestione dei contenuti online: i nuovi standard SASB*, in *Agenda Digitale*, August 26, 2022, https://www.agendadigitale.eu/mercati-digitali/finanza-sostenibile-limpatto-esg-sulla-gestione-dei-contenuti-online-i-nuovi-standard-sasb/;

## 2. Historical Context

When approximately thirty years ago the world wide web began to develop into the pervasive tool we have become familiar with nowadays, a number of regulatory presumptions had been established with the explicit aim of ensuring its frictionless expansion.[6]
In contrast with other market sectors, which have been tightly regulated over the time,[7] for years the legislator has taken the conscious decision to reserve internet a considerable independence, without taking any remarkable regulatory action, but firmly grounding the web on three main positions, which have independently been assumed both in the EU [8] and in the USA. The first one of these positions was that regulations should have not been enacted to prevent hypothetical situations, but just to solve real existing problems. The second one, on the other hand, was based on the idea of a free electronic market with free electronic commerce, which removed the necessity for a regime of special authorizations, establishing, in particular in the EU, as the only applicable regime on the internet for services providers the one set by the state of origin's law. Lastly, the third choice made by the lawmakers was that the intermediaries should have not been considered responsible for the contents published from third parties, relieving them from the burden of an active monitoring, as well as from the risk of being sanctioned for those contents.[9]

The combination of these choices, together with the proliferation of digital devices and broad-band access, made it possible for the internet to spread all over the world frictionless, versatile and widely, bringing us to the current digital revolution in which businesses are mainly moved by a data-driven economy and digital platforms are the absolute and undisputed catalysts of such an economy.[10]

These platforms have made significant contributions to societal and economic changes in the European Union and around the world, as they have started not only to contribute in the

---

[6] SAVIN, *The EU Digital Services Act: Toward a More Responsible Internet,* in 24(7) *The J. of Int. Law,* 15-25, 15, (2021);
[7] MILLWARD**,** *Private and Public Enterprise in Europe: Energy, Telecommunications and Transport, 1830–1990,* Cambridge University Press*,* Cambridge, 2008, 163;
[8] European Commission, *A European Initiative in Electronic Commerce, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions*, COM(97)157, April 15, 1997;
[9] KOSSEFF, *The Twenty-Six Words*, 23;
[10] SAVIN, *The EU Digital Services Act,* 6; NUCCIO, GUERZONI, *Big Data: Hell or Heaven? Digital Platforms and Market Power in the Data-Driven Economy*, in 23(3) *Comp. & Ch.,* 312–328, 322, (2019);

accomplishment of the "Sustainable Development Goals",[11] by promoting environmental, social, and economic sustainability, but also to shape sociality in our human relationships, facilitating the development of distant communications,[12] and defining a new model of interactions, which sees the use of modern technologies always more at the center of our lives. Particularly with the coronavirus's outbreak, it has become even more evident how crucial digital technologies have become to modern life in all its facets,[13] providing societies with useful tools to counter the spread of the pandemic,[14] giving the possibility to increase productivity through virtual meetings and smart working,[15] and creating countless opportunities for online gatherings and acquaintances that have allowed people to stay close despite remaining distant.[16]

However, the enjoyment of those digital services has also given rise to new dangers for both the society and the users. If, on the one hand, in fact, this liberal approach sought to facilitate the development of the internal market following the advent of the Internet, on the other hand, such ideology has resulted in the consolidation of digital platforms as dominant actors in the online environment, raising new issues as for democracies and their functioning,[17] as well as for the protection of fundamental rights such as privacy,[18] data protection, freedom to conduct a business and freedom of expression.[19]

When the Internet was still at its infancy and digital technologies were in their early stages, a special regime of liability exceptions was in fact introduced both in the US and in the EU to acknowledge the non-involvement of online intermediaries in the creation of hosted or

---

[11] United Nations, A/RES/70/1, October 21, 2015;

[12] WIELSCH, *Private Law Regulation of Digital Intermediaries*, in 2 *Eu. Rev. of Priv. Law*, 197, (2019); IANNARELLI, *La regolazione privatistica delle relazioni di mercato nell'attuale contesto*, in *Riv. Cri. di Dir. Priv.*, 2020, 297, *ivi* 320;

[13] BENTATA, *COVID 2019 pandemic: a true digital revolution and birth of a new educational era, or an ephemeral phenomenon?*, in 25(1) *Med. Educ. On.,* (2020); Panel for the Future of Science and Technology (STOA), *Online Platforms: Economic and Societal Effects,* 18, (2021) ;

[14] HOWELL O'NEILL, *Apple and Google's Covid-Tracing Tech Has Been Released to 23 Countries*, in *MIT Technologies Review*, May 20, 2020, https://www.technologyreview.com/2020/05/20/1002001/apple-and-googles-covid-tracing-tech-has-been-released-to-22-countries/;

[15] ROBERTO, ZINI, FELICI, RAO, NOUSSAN, *Potential Benefits of Remote Working on Urban Mobility and Related Environmental Impacts: Results from a Case Study in Italy*, in 13(1) *Ap. Sci.*, 607, (2023); REMMEL, *Scientists want virtual meetings to stay after the COVID pandemic,* in 591 *Nat.,* 185-186, 185, (2021);

[16] OKABE-MIYAMOTO, LYUBOMIRSKY, *Social Connection and Well-Being during COVID-19,* in *World Happiness Report,* (2021), https://worldhappiness.report/ed/2021/social-connection-and-well-being-during-covid-19/;

[17] NEMITZ, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, in *Phil. Trans. of the R. Soc. A*, 376, (2018);

[18] QI, EDGAR-NEVILL, *Social networking searching and privacy issues*, in 16(2) *Inf. Sec. Tec. Rep.*, 74-78, 76, (2011);

[19] MENKES, *Freedom of speech in the age of digitalization - Opportunities and* threats, in *The Eu. Un. Dig. Sing. Mar. Eu.'s Dig. Transf.*, 35-62, 36, (2022);

transmitted content,[20] due to the necessity of promoting the growth of information society services, while also upholding economic freedom and freedom of expression.[21] This regime shielded intermediaries from liability so long as they remained unaware of the presence of illicit content on their digital premises. In the event that intermediaries were made aware of the existence of such content, they were instead obliged to remove it with immediate effect (i.e. delegated censorship).[22] Particularly in the EU, such regime was based on the presumption that these actors played a mere passive and neutral role in the transmission of the information, essentially having no control over the content published by their users and remaining in fact unaware of the activities carried out by them.[23]

Starting from the mid-2000s, however, digital platforms autonomously begun to develop new content moderation guidelines and policies, which were soon integrated into their corporate structures with the specific purpose to identify potentially inappropriate or dangerous content online and take adequate actions to limit or prohibit their dissemination through the internet (i.e. de facto private censorship).[24] Using a combination of private law and automated technologies, online intermediaries started to exert a "private" form of authority, which, by replacing legal norms with their own contractual standards, i.e. terms of service (ToS), ended up subjecting users just to their own corporate regulations,[25] as they were not legally bounded to establish any transparent procedure or redress mechanism provided by the law. In doing so, digital platforms de facto started to exercise a digital sovereignty in the form of a quasi-

[20] 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, 2000 O.J. (L 178) 1 (e-Commerce Directive); Communication Decency Act, 47 U.S.C. § 230; Digital Millennium Copyright Act, 17 U.S.C. § 512;

[21] Directive 2000/31/EC, recital 9; KOSSEFF, The Twenty-six words, 45; MANETTI, *Regolare Internet*, in *Media Laws*, 35, July 15, 2020, https://www.medialaws.eu/rivista/regolare-internet/; BETZU, *Libertà di espressione e poteri privati nel cyberspazio*, in 1 *Dir. Cost. – Riv. Quad.*, 117-233, 117, (2020); CUNIBERTI, *Potere e libertà nella rete*, in *Media Laws*, October 24, 2018, https://www.medialaws.eu/rivista/potere-e-liberta-nella-rete/;

[22] LYNSKEY, *Regulation by Platforms: The Impact on Fundamental Rights*, in BELLI, ZINGALES (eds), *Platform Regulation,* 83; GRIMMELMANN, *Speech Engines,* in 98 *Min. L. Rev.,* 868-952, 887, (2014); Council of Europe Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World,* 72, 2014, https://book.coe.int/en/commissioner-for-human-rights/7321-pdf-the-rule-of-law-on-the-internet-and-in-the-wider-digital-world.html; FLORIDI, TADDEO, *The Moral Responsibilities of Online Service Providers,* in 31 *L., Gov. a. Tech. Ser.*, 13-43, 23, (2017);

[23] Directive 2000/31/EC (e-Commerce Directive), recital 42;

[24] MONTI, *Privatizzazione della censura e Internet platforms:la libertà d'espressione e i nuovi censori dell'agorà digitale,* in 1 *Riv. Ita. di Inf. e Dir.,* 2019, 35-51, *ivi* 37; KLONICK, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in 131 *Har. L. Rev.*, 1599-1670, 1634, (2018); AMMORI, *The "New" New York Times: Free Speech Lawyering in the Age of Google and Twitter*, in 127 *Har. L. Rev.*, 2259-2295, 2274, (2014);

[25] BELLI, FRANCISCO, ZINGALES, *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police*, in BELLI, ZINGALES (eds), *Platforms Regulation*, 47;

legislative power,[26] essentially replacing public authorities in the regulation of the digital environment and substantially assuming a new role which went far beyond that of a mere passive intermediary.[27]

As a consequence, in order to ensure the enforcement of their rules, in the last decade digital platforms started to develop advanced and disruptive technologies, based mostly on artificial intelligence systems, which allowed them to further strengthen their authority in the digital sphere, gaining nearly a complete dominance over online content and information. As already demonstrated indirectly by the Cambridge Analytica scandal,[28] in fact, private actors can now process massive amounts of information[29] and acquire nearly a complete knowledge of individuals and their activities online, marking therefore the transition from the previous "information society", as it emerged in the late 1990s, to a new concept of "algorithmic society", which sees hosting providers like YouTube and Facebook at its center.[30]

In this evolved context, in which digital platforms have come to play a fundamental role in the regulation of the digital space and the protection of users' fundamental rights, the special regime of liability envisaged at the turn of the century has ultimately resulted in putting an increasing pressure on online intermediaries, so that they could guarantee, in the absence of any regulatory framework, the effective protection of fundamental rights and the concrete implementation of public policies in the digital sphere. Originally envisaged only for the few cases of effective involvement of platforms in the commission of online illegalities, in fact, such regime has paradoxically ended up making online intermediaries even more accountable, due to the obligation imposed on them to remove online content upon notice of its alleged illegality.

This has given rise to an enormous uncertainty online, which led to the formation of new concerns as for the protection of fundamental rights, particularly with regards to the safeguarding of freedom of expression. Given the technological advances allowing an overall

---

[26] FLORIDI, *The fight for digital sovereignty: what it is, and why it matters, especially for the EU*, in 33(3) *Phil. & Tech.*, 369–378, 375, (2020);

[27] TEUBNER, *The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors,* in 69(3) *Mod. L. Rev.*, 327-346, 327, (2006);

[28] HINDS, WILLIAMS, JOINSON, *"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica Scandal*, in 143 *Int. J. Hum. -Comp. Stud.,* 23, (2020);

[29] BAROCAS, HOOD, ZIEWITZ, *Governing Algorithms: A Provocation Piece,* in *SSRN,* 1-12, 6, (2013); DEVINS, FELIN, KAUFFMAN, KOPPL, *Law and Big Data,* in 27(2) *Corn. J. L. Pub. Pol.*, 357-413, 368, 2017;

[30] BALKIN, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation,* in 51 *Univ. Calif. Dav. L. Rev.*, 1149-1210, 1151, (2018);

control over information, the power of digital platforms to establish rules and balance opposite interests online has solely been based on the mere fear of being held accountable. Considering in fact that online platforms are privately operated entities, instead of pursuing a fair and impartial balance of interests for the protection of fundamental rights, these actors have been prompted to prioritize the reduction of civil liability, and therefore of their economic risks, by engaging in the preventive removal or blocking of content also in the cases where the content's illicit nature was not clearly apparent (i.e. "collateral censorship"),[31] such as in situations where groundless allegations were made by third parties, or simply ambiguous content were asked to be removed. This is because, when digital platforms decide to not remove or block a certain content brought to their attention, they risk being held accountable in the event that such content is subsequently found to be illegal by a public authority.[32]

Moreover, by increasing the risks of a complete removal of disputed content and of silencing operations, this delegation of powers to digital platforms has also turned into a higher threat for democracies themselves, by limiting ultimately the spaces for public debate in those environments such as Facebook and Google, which have progressively emerged as public arenas of fundamental importance, with political communication, information, the right to criticism and various other personal interactions circulating therein.

This trend has been further expressed in several occasions also by the CJEU fervent activism, which, in the notorious case of *Google Spain*,[33] in 2014, effectively entrusted private actors, specifically search engines, with the power to remove online content upon request from the concerned individual, considering them as the exclusive subjects capable of ensuring the enforcement of the right to be forgotten online, given their ability to manage the online spaces where the links to be removed are published. Accordingly, the CJEU held that the data subjects have the right to request that online search engines delete links to information related to them, from a list of web results based on their name.

---

[31] BALKIN, *Old-School/New-School Speech Regulation*, in 128(8) *Harv. L. Rev.*, 2296-2342, 2297, (2014); WU, *Collateral Censorship and the Limits of Intermediary Immunity*, in 87 *Notr.. D. L. Rev.*, 293-350, 341, (2011); BASSINI, *Fundamental rights and private enforcement in the digital age*, in 25 *Eur. L. Jour.*, 182-197, 185, (2019);

[32] ADLER, *The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship,* in 20(1) *Journ. L. Pol.*, 231-265, 252, (2011);

[33] Case 131/12 Google Spain v AEPD EU:C:2014:317;

This evolution has consequently made unclear the ways in which these platforms take decisions and process information, raising new issues as for their transparency and accountability.[34] Particularly, the implementation of new profiling methods and the provision of automated decision-making processes, such as pattern recognition mechanisms, have increasingly led to a significant reduction of the human oversight, casting serious doubts as for the legitimacy and the fairness of these systems. For instance, in taking automated decisions and processing all the information, these platforms may inadvertently perpetuate racial biases and cultural prejudices that were embedded in their functions during the original programming stage. There is indeed very little transparency about which elements are considered to be potentially problematic and for what reasons, making content algorithmic moderation a sort of "black box", whose mechanisms and programming details are mostly inaccessible and obscure, despite the profound social implications of their use.[35]

Especially in the last decade, such forms of content moderation have also ended up raising serious concerns from a constitutional perspective,[36] as they have implied a discretional activity of balancing fundamental rights, in the same way as a court would be asked to do.[37] When platforms receive requests from users to remove content or delist links, they are now called to determine which fundamental rights or interests should take priority in the evaluation of the specific case, performing a form of judicial balancing, which, in fact, is typical of real and independent courthouses. For instance, since 2006, YouTube has developed editorial criteria, often entrusted to individuals, to evaluate the impact of videos that, although violating policies on violence, remain important for public discourse. This happened for example in the cases of a video showing Saddam Hussein's hanging and of another showing the death of a protester from the "Green Movement" in Iran, which were

---

[34] BURRELL, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, in *B. D. & Soc.*, 1-12, 3, (2016); MITTLESTADT ET AL., *The Ethics of Algorithms: Mapping the Debate,* in *B. D. & Soc.*, 1-21, 3, (2016); GROZDANOVSKI, *In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law*, in 58 *Com. Mar. L. Rev.*, 99-136, 118, (2021); BERMAN, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation,* in 71 *Un. Col. L. Rev.,*1263-1310, 1282, (2000);

[35] PASQUALE, *The Black Box Society. The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge, 2015; TURILLI, FLORIDI, *The Ethics of Information Transparency*, in 11(2) *Eth. Inf. Tech.*, 105-112, 105, (2009); ZARSKY, *Transparent Predictions,* in 4 *Uni. Illin. L. Rev.,* 1503-1570, 1507, (2013); BENJAMIN, *Algorithms and Speech,* in 161(6) *Uni. Pen. L. Rev.*, 1445-1494, 1450, (2013); CUSTERS, CALDERS, SCHERMER, ZARSKY, EDS., *Discrimination and Privacy*, 17; VEALE, EDWARDS, *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in 34 *Comp. L. & Sec. Rev.*, 398-404, 400, (2018);

[36] TEUBNER, *Societal Constitutionalism: Alternative to State-Centred Constitutional Theory?,* in, JOERGES, SAND, TEUBNER EDS., *Transnational Governance*, 23; BLACK, *Constitutionalising Self-Regulation,* in 59(1) *Mod. L. Rev.*, 24-55, 28, (1996); DE GREGORIO, *From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society*, in 11(2) *Eu. J. Leg. Stud.* 65-103, 69, (2019);

[37] BALKIN, *Free Speech and Hostile Environments*, in 99(8) *Col. L. Rev.*, 2295-2320, 2312, (1999);

kept online despite violating guidelines on violence, and in the case of a video showing the beating of an Egyptian activist in a cell, which was first removed and then reinstated, following protests by journalists, politicians, and activists.[38] In all these cases, not only can the relevant policy determine which type of violence can be allowed and therefore make a content-related choice, but it can also create exception processes that lend themselves to being partly based on political motives, reflecting the ideological tendencies of the internet platforms themselves, as bearers of discretionary interests and values.

Standing from this point of view, a particular attention has been posed on the recent 2021 Capitol Hill events involving the former US President, Donald J. Trump, in which the major social networks' boards took the unprecedent decision to shut down even the profiles of arguably the most powerful individual on earth, that is the president of the United States.
At the dawn of Joe Biden's 46th US election victory, in the 2020, the outgoing former president Donald J. Trump addressed his supporters with a rousing message published on Twitter and other social networks, stating "Statistically impossible to have lost the 2020 election. Big protest in D.C. on January 6th. Be there, will be wild!".[39] Spreading like wildfire among far-right groups, the message came as the icing on the cake of a long and controversial series of statements, which were dropped by the former president of the United States on his social network profiles, during the whole period of his presidential term. Such statements ultimately ended up throwing several unfounded accusations of electoral fraud,[40] which provoked, on January 6th, 2021, what would have gone down in history as the "attack on Capitol Hill".[41] Following the riot, digital platforms took the historic decision to intervene, reaching the conclusion that the former US president officially became "digitally toxic",[42] due to the threat posed by his aggressive and incendiary messages, which frequently contained false or deceptive information. Accordingly, Trump's accounts were suspended on practically all the digital platforms (i.e. "deplatformization"),[43] such as YouTube, Facebook,

---

[38] KLONICK, The New Governors, 1619;
[39] SHEERIN, *Capitol riots: "Wild" Trump tweet incited attack, says inquiry*, in *BBC*, January 6, 2021, https://www.bbc.com/news/world-us-canada-62140410;
[40] EGGERS, GARRO, GRIMMER, *No evidence for systematic voter fraud: A guide to statistical claims about the 2020 election,* in 118(45) *Proc. Nat. Ac. Sci.*, 1-7, 1, (2021);
[41] Wikipedia, *January 6 United States Capitol Attack,* 2021, https://en.wikipedia.org/wiki/January_6_United_States_Capitol_attack; BUCHANAN ET AL., *How a Pro-TrumpMob Stormed the US. Capitol,* in *N.Y. TIMES*, January 7, 2021, https://www.nytimes.com/interactive/2021/01/06/us/trump-mob-capitol-building;
[42] FLORIDI, *Trump, Parler, and Regulating the Infosphere as Our Commons,* in 34 *Phil. & Tech.*, 1-5, 3, (2021);
[43] ROGERS, *Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media,* in 35(3) *Eu. J. Com.*, 213–229, 214, (2020); DI SALVO, *Deplatforming, l'attacco a Capitol Hill e la nuova sfera pubblica privatizzata*, in 18(3) *St. Cult., Riv. Quad.,* 2021, 449-458, *ivi* 452; CICCONE, *Deplatforming» Trump:*

Instagram and Twitter,[44] among which Twitter in particular also shut down accounts connected to QAnon and Pride Boys, the extremist groups loyal to Trump. The decision was met with both praise and criticism,[45] reigniting heated discussions surrounding the role of free speech and the power of online private entities to regulate content, even those of the president of the United States of America.

Hence, the original vision of a decentralized and democratic legal system for cyberspace, which was promoted by early libertarian scholars, [46] has been rapidly replaced by an oligopoly of private entities that exercise control over the flow of information and rule over its dissemination. [47] This shift has resulted in a model of platform-based regulation, which, by concentrating power in the hands of a few, has supplanted the earlier community-based approach,[48] wherein digital communities should have had the possibility to participate in the establishment of new customary rules, for the organization of the emerging digital landscape. As agreeably opined by Jeffrey Rosen, nowadays "lawyers at Google, YouTube, Facebook and Twitter have more power over who can speak and who can be heard than any president, judge or monarch".[49] Also from a Constitutional standpoint, the three fundamental powers of State have been all consolidated under the authority of these digital platforms, since they now have become capable to define the rules for assessing online content, make decisions on user complaints and enforce those decisions, without any separation of functions and in contrast with the Constitutionalism as theorised by Charles De Secondat,[50] based on the concept of the separation of powers. It has therefore emerged here a regime based on a private order, which does not adhere to constitutional provisions, but rather resembles the form of an

*la giusta decisione di Facebook e Twitter di bloccare gli account del presidente uscente*, in *Valigia Blu*, January 9, 2021, https://www.valigiablu.it/ deplatforming-trump-facebook-twitter/;

[44] ZUCKERBERG, in *Facebook*, January 7, 2021, https://www.facebook.com/zuck/posts/101126 81480907401; TWITTER, *Permanent Suspension of @realDonaldTrump,* in *Twitter blog,* January 8, 2021, https://blog.twitter.com/enus/topics/company/2020/suspension.html;

[45] NOOR, *Should We Celebrate Trump's Twitter ban? Five Free Speech Experts Weigh in*, in *The Guardian,* January 17, 2021, https://www.theguardian.com/us-news/2021/jan/17/trump-twitter-ban-five-free-speech-experts-weigh-in;

[46] BARLOW, *A Declaration of Independence of the Cyberspace,* in *Electronic Frontier Foundation*, February 8, 1996, www.eff.org/cyberspace-independence; JOHNSON, POST, *Law and Borders: The Rise of Law in Cyberspace,* in 48(5) *Stan. L. Rev.*, 1367-1402, 1371, (1996);

[47] MANSELL, JAVARY, *Emerging Internet Oligopolies: A Political Economy Analysis*, in MILLER, WARREN J SAMUELS EDS., *An Institutionalist Approach*, 165; MOAZED, JOHNSON, *Modern Monopolies*, 54;

[48] LOBEL, *The Law of the Platforms,* in 101 Min. L. Rev., 87-166, 87, (2016);

[49] ROSEN, *Who Decides? Civility v. Hate Speech on the Internet,* in 2(13) *A. Bar Ass.: Ins. L. & Soc.*, (2013);

[50] CHARLES DE SECONDAT, *L'esprit,* 347;

absolute power, to the point of leading some authors to suggest a resurgence of the feudalism,[51] or even a return to the ancién regime schemes. [52]

### 3. The CDR/ ESG Framework

In this context, a new concept of corporate digital responsibility (CDR) has been developing within the broader doctrinal and legislative framework surrounding the emerging concept of ESG (Environmental, Social, and Governance), which represents a new branch of corporate law supporting the establishment of a new sustainable capitalism for the benefit of the environment, society, and the long-term sustainability of businesses.[53]

Already for decades, scholars have been viewing corporations as political actors who contribute to the provision of public goods and safeguard the fundamental rights of citizens. Giving a "deliberative democratic interpretation" to the concept of CSR (corporate social responsibility), they have been emphasizing the role of corporations as active participants in shaping societal outcomes and promoting democratic decision-making processes in their commercial activities. Specifically, they have been arguing that corporations should address governance gaps in global business by engaging in democratic deliberations within multi-stakeholder initiatives and forums.[54]

In this regard, on February 23rd, 2022, the European Commission presented, for the first time, a proposal for a directive aimed at implementing new human rights and environmental due diligence obligations to minimize negative impacts in business activities,[55] while, at a national level, in Italy, a new Corporate Governance Code was issued in 2020 to update and enhance corporate governance practices on the Italian stock exchange, incorporating various provisions which introduced the new principle of "sustainable success". Such principle entails creating long-term value for shareholders while considering also the interests of other

---

[51] GRIMMELMANN, *Virtual World Feudalism,* in 118 *Y. L. Jour. Poc.*, 126-130, 127, (2009);
[52] BELLI, VENTURINI, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation,* in 5(4) *Int. Pol. Rev.,* 1-17, 4, (2016);
[53] HERDEN,, ALLIU,, CAKICI, *ET AL.*, *Corporate Digital Responsibility*. In 29 *NachhaltigkeitsManagementForum*, 13–29, 19, (2021);
[54] CRANE, MATTEN, MOON, *Corporations and Citizenship*, 133; SCHERER, PALAZZO, *The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy,* in 48 *J. Manag. Stud.*, 899-931, 907, (2011);
[55] European Commission, Proposal for a directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, COM(2022) 71 final, Brussels, February 23, 2022;

relevant stakeholders in the corporate context.[56] Specifically, although not legally binding, this principle is governed by the "comply or explain" approach, which requires companies that do not pursue the social interest, including in their use of technology, to adequately explain their reasons, in accordance with the notion of "sustainable success".[57]

Within this framework, Corporate Digital Responsibility (CDR) therefore assumes the function of a real tool for implementing ESG criteria in companies that intend to integrate sustainability factors through the lenses of the digital market. This concept applies in fact to all actors operating primarily in the field of online intermediary services, who consistently face new challenges posed by scientific and technological progress, in line with the continuous evolution of the market and the evolving demands of consumers. This involves scrutinizing its implications in several areas which includes that of IT infrastructure, data and privacy management, up to various business processes, such as manufacturing, automation and sales.

The levels on which a Corporate Digital Responsibility policy operates are the same outlined within the CSR pyramid as defined by Carroll,[58] namely economic, legal, ethical and discretionary, with the unique distinction that they are approached differently due to the specific digital perspective from which they are considered. If, in fact, on the economic level, the focus is on innovative business models capable of competitively withstanding market evolution, on the legal front compliance should encompass traditional regulations while integrating data protection, cybersecurity, intellectual property (IP) and ESG regulations. Similarly, ethical considerations should duly account for the impacts of technologies such as artificial intelligence, blockchain, and others, while the discretionary level may ultimately entail philanthropic programs, such as distance education, STEM education and social innovation initiatives.

From this perspective, an integrated CDR/ESG strategy should aim not only to prevent potential negative consequences of digitalization but also to capitalize on its advantages. There are in fact several examples of sustainable uses of technology, among which the use of Digital Social Innovation (DSI) systems particularly stands out, entailing the development and implementation of innovative products, services, processes and business models (in

[56] Codice di Corporate Governance, January 2020, 3;
[57] Codice di Corporate Governance, January 2020, 1;
[58] CARROLL, *The pyramid of corporate social responsibility: to- ward the moral management of organizational stakeholders,* in 34(4) *Business Horizons*, 39-48, 44, (1991);

which digital technology plays a central role) that strive to address issues with a social or environmental impact.

Furthermore, it is worth noting that the link between sustainable development and innovation is also emphasized by Goal 9 of the United Nations' 2030 Agenda.[59] This goal establishes that innovation should serve as the essential means for achieving various other sustainability objectives, such as, for example, the responsible consumption and production (Goal 12), the fight to climate change (Goal 13), the challenge of inequalities (Goal 10), the promotion of decent work and economic growth (Goal 8), and the creation of clean and accessible energy (Goal 7). As a result, innovation becomes the core focus for companies seeking to integrate virtuous social, environmental, and governance impacts alongside their economic performance.

Similarly, also the former Sustainability Accounting Standards Board (SASB), recognizing the intrinsic value derived from the proper management of digital services, as well as the associated costs in terms of content moderation and reputational harm resulting from the dissemination or use of illicit content, took action in 2018 (the year of the Action Plan on Sustainable Finance).[60] In light of the aforementioned risks and the growing concerns of investors, the board initiated a project to integrate industry-specific reporting standards for the IT and Media sectors, which involved the development of specific guidelines and metrics addressing content governance policies, user freedom of expression and the enforcement thereof. This project was aimed overall to address the contentious issue of platform liability for content, as well as the ineffectiveness of user-activated policies in this regard.
The analyses conducted by SASB in the tech industry, along with consultations involving companies and investors, led to the development of the first content governance taxonomy (Content Moderation Taxonomy) in November 2020.[61] This taxonomy highlighted the numerous social issues associated with harmful content, particularly concerning users' freedom of expression, and it defined "content moderation" as the set of processes and

[59] UN, *Transforming our World: The 2030 Agenda for Sustainable Development,* 2015, Goal 9, https://sdgs.un.org/2030agenda;
[60] PRISCO, *Finanza sostenibile, l'impatto ESG sulla gestione dei contenuti online: i nuovi standard SASB*, in *Agenda Digitale, https://www.agendadigitale.eu/mercati-digitali/finanza-sostenibile-limpatto-esg-sulla-gestione-dei-contenuti-online-i-nuovi-standard-sasb/;*
[61] Sustainability Accounting Standards Board, *Content Moderation Taxonomy: A Foundation for Standard Setting on Issue of Content Moderation,* 2020, https://www.sasb.org/wp-content/uploads/2020/12/Content-ModerationTaxonomy-v7b.pdf;

procedures used to identify and potentially intervene in illegal or unwanted content, especially on social media platforms.

It is precisely in this context of significant awareness that the European Union, in recent years, started a process of legislation in the field of the digital economy, aimed at implementing new regulations to counter the exercise of unfair practices and the abuse of dominant positions in the big tech markets, and to impose on online services intermediaries, whether of normal or very large dimensions, a greater responsibility for the control and moderation of digital content. The measures will try to ensure compliance with competition rules, protect consumer rights and promote a fair and transparent digital ecosystem.

### 4. The EU Digital Strategy: "*Shaping Europe's Digital Future"* Communication

Already since 2014, in order to give a boost to the data-agile economy, several actions have been undertaken by the European Commission, among which particular importance has been assumed by the "Regulation on the Free Flow of Non-Personal Data",[62] the "Cybersecurity Act",[63] the "Open Data Directive" [64] and the "General Data Protection Regulation".[65]
In 2018 for the first time an AI strategy was presented by the European Commission[66] and in April 2019 a high-level expert group on AI presented the "Ethics Guidelines for Trustworthy AI".
Also in 2019, the European Commission President Ursula von der Leyen in her Political Guidelines stressed the necessity of a "transition to a healthy planet and a new digital world", in the perspective of a twin transition, which is both a digital and a green transformation.

[62] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, (2018), OJ L 303, p. 59-68;
[63] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 *(Cybercecurity Act)*, (2019), OJ L 151, p. 5-69;
[64] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), (2019), OJ L 172, p. 56-83;
[65] 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) (Text with EEA relevance), (2016), OJ L 119, p. 1–88;
[66] European Commission, *Artificial Intelligence for Europe,* COM(2018) 237 final, Brussels, April 25, 2018;

In that context, the EC President also announced the beginning of a debate, during her first 100 days in office, on human and ethical AI implications and on the use of big data, aimed to create wealth for societies and business.[67]

Building on these political guidelines, on February 19th, 2020 the EU Commission finally announced its digital strategy for the following five years in the *"Shaping Europe's Digital Future"* communication, which aims to represent the Commission's plan for a digital transformation that works for all.[68]

The Communication aspires to reflect the best virtues of the European Union, represented as an open, diverse, fair, confident and democratic society powered by digital solutions, where people come first, new opportunities are opened up for business and trustworthy technologies are developed in order to boost a vibrant and sustainable economy.[69] The EU Commission balances in particular the power and the benefits of these technologies with a strong societal focus, usually expressed as an attention to common European values, care for human rights or consideration of ethics.[70]

In its strategy, the EC takes note that the European technological sovereignty must be considered a crucial priority for the European Union, in order to gain independence from the other global players and secure the means to shape Europe's own future.[71] However, this sovereignty must be reached not only developing and deploying European own capacities, with a stronger integrity of our data infrastructure, networks and communications, but also defining European own rules and values which empower the EU citizens, businesses and governments to regain control over the digital transformation.[72] It is in fact just within the framework of a "truly European project" that Europe is going to be able to set the global standards, where every single human being is respected and nobody is left behind.[73]

---

[67] Political Guidelines for the Next European Commission 2019-2024, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_en;
[68] European Commission, *Shaping Europe's digital future*, COM(2020) 67 final, Brussels, February 19, 2020;
[69] European Commission (2020), *Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence,* Press release, IP/20/273, February 19, 2020;
[70] KELLER, TARKOWSKI, *Digital Public Space – A missing policy frame for shaping Europe's digital future*, in *Open Future,* 5, (2021);
[71] TIMMERS, *Debunking Strategic Autonomy*, 1, https://directionsblog.eu/debunking-strategic-autonomy/;
[72] KELLER, TARKOWSKI, *Digital Public Space*, 5;
[73] European Commission, COM(2020) 67 final;

Such a European model might then likely become a competitive and viable option which, being alone among global actors in attempting this value-based approach to the digital sector, will also be able to compete in particular with China and USA's digital strategies.[74]
The strategy relies in particular on three key objectives: a) the uptake of technologies that really impact people's daily lives, with a competitive economy shaping technology in respect of European values (technology that works for the people); b) a frictionless single market that is globally competitive and allows companies to compete on equal terms and to scale up (a fair and competitive economy); c) a trustworthy digital environment that empowers citizens, enhances democratic values, respects fundamental rights and supports a sustainable economy (an open, democratic and sustainable society).[75]

Starting from these targets, a strong regulatory process has taken its first steps during the last two years, in the perspective of a policy reform program, which has been under development since the coming into office of the current Von Der Leyen Commission. Such a policy reform program defines a new legal framework, encompassing a wide range of versatile proposals that go from the "Artificial Intelligence Act" (AIA)[76] to the "Data Strategy",[77] together with the "Data Act" [78] and the "Data Governance Act" (DGA),[79] up to new digital platforms regulations and competition rules, introduced by the "Digital Services Act Package",[80] which consists of the "Digital Services Act" (DSA)[81] and the "Digital Market Act" (DMA).[82]

[74] FLORIDI, *The European Legislation on AI. A Brief Analysis of its Philosophical Approach*, in 34(2) *Phil. and Tech.*, 215-22, 217, (2021);
[75] KELLER, TARKOWSKI*, Digital Public Space*, 5;
[76] European Commission, *Proposal for a Regulation of the European Parliament and of the Council - laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts,* COM/2021/206 final, Brussels, April 21, 2021;
[77] European Commission, *A European strategy for data*, COM(2020) 66 final, Brussels, February 19, 2020;
[78] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)***,** COM/2022/68 final, Brussels, February 23, 2022;
[79] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 may 2022 on European data governance and amending regulation (EU) 2018/1724 (data governance act), (2022), OJ L 152, p. 1-44;
[80] European Commission, IP/20/273;
[81] 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, December 15, 2020;
[82] 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, December 15, 2020;

Additionally, also other types of regulatory measures might be considered falling within the scope of the present EU digital Strategy, such as an "EU Governments Interoperability Strategy",[83] an "European Democracy Action Plan" [84] and a "Digital Finance Package" [85] which includes a proposal for a "Markets in Crypto Assets Regulation" (MiCAR)[86], a proposal for a "Digital Operational Resilience Act" (DORA)[87] and a "Distributed Ledger Technology Regulation" (DLTR).[88]

The resulting regulatory frame, characterizing current EU digital policies, lays on the conception of a "digital constitutionalism", which aims to establish a new set of legislations protecting fundamental rights and granting a balance of power in the digital sector.[89] The scope of such legislations is to set new rules or to modify existing laws in order to address the challenges posed by the latest wave of the digital impact, generally framed in terms of "platformization" [90] or "datafication".[91]

.

[83] European Commission, *interoperable digital public services – european interoperability framework evaluation & strategy*, ref. Ares(2022)4789624, Brussels, June 30, 2022;
[84] European Commission, *On the European democracy action plan,* COM(2020) 790 final, Brussels, December 3, 2020;
[85] European Commission, *on a Digital Finance Strategy for the EU,* COM(2020) 591 final, Brussels, November 24, 2020;
[86] European Commission, *proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending directive (EU) 2019/1937,* COM(2020) 593 final, Brussels, November 24, 2020;
[87] European Commission, *proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending regulations (EC) no 1060/2009, (EU) no 648/2012, (EU) no 600/2014 and (EU) no 909/2014*, COM(2020) 595 final, Brussels, November 24, 2020;
[88] European Commission, *Proposal for a regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology*, COM/2020/594 final, Brussels, November 24, 2020;
[89] CELESTE, *Digital Constitutionalism. A New Systematic Theorisation*, in 33/1 *Int. Rev. of Law*, *Comp. and Tech.*, 76-99, 80, (2019); FLORIDI, *The European Legislation on AI,* 12;
[90] POELL, NIEBORG, VAN DIJCK, *Platformisation*., in 8(4) *Int. Pol. Rev.*, 2, (2019);
[91] VAN DIJCK, *Datafication, Dataism and Dataveillance. Big Data between Scientific Paradigm and Ideology,* in 12(2) *Surv. and Soc.*, 197-208, 198, (2014);

# Chapter 2

# AN INTRODUCTION TO

# THE DIGITAL SERVICES ACT (DSA)

## 1. The Origins of the Regulation

In its communication on the EU's digital strategy,[1] the Commission pledged to reform the horizontal norms that outline the obligations and responsibilities of digital services providers, paying particular attention to the so called "online platforms", which were lately also defined in the text of the DSA Proposal.[2]

The Commission considered the issues presented in the recent EU Parliament's reports and examined its recommendations.

Among the mentioned initiatives, the EU Parliament adopted, in accordance with the article 225 of the Treaty on the Functioning of the European Union (TFEU), the two resolutions on the *"Digital Services Act - Improving the Functioning of the Single Market"* [3] and on the *"Digital Services Act: Adapting Commercial and Civil Law Rules for Commercial Entities Operating Online",*[4] in addition to a resolution under the non-legislative procedure, namely the *"Digital Services Act and fundamental rights issues posed"*.[5]

In substance, the resolutions complement one another in many ways. They make a strong case for preserving the main tenets of the e-Commerce Directive, safeguarding fundamental rights in the online space, and, to the extent that it is technically possible, preserving online

[1] European Commission, COM(2020) 67 final;
[2] European Commission, COM(2020) 67 final, art.2, lett. H;
[3] European Parliament, Resolution on improving the functioning of the Single Market (2020/2018(INL)), P9_TA(2020)0272, October 20, 2020;.
[4] European Parliament, Resolution on adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), P9_TA(2020)0273, 20 October 2020;
[5] European Parliament, Resolution on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)), P9_TA(2020)0274, October 20, 2020;

anonymity. To fight illegal content online, they push for an increase of the legal burdens on the digital services' providers, imposing higher transparency standards, new disclosure obligations and a fair liability regime.
In addition, they also support the coordination of a public monitoring at both a European and a national scale, by increasing the cooperation between national authorities, particularly when dealing with cross-border issues.

With the resolution on the "Digital Services Act - Improving the Functioning of the Single Market", the EU Parliament intended to pursue a comprehensive overhaul of the EU legislation set by the e-Commerce Directive on the online services,[6] while preserving at the same time its main structure, mostly based on the definition of an accountability regime, the impossibility for Member States to require a general content monitoring, and the so called "internal market clause",[7] which is considered to be still in force.
In particular, with a call for action finalized at the protection of consumer's welfare, the resolution reaffirms the goals set by the e-Commerce Directive, especially by including a comprehensive section on online marketplaces, and ensuring consumer trust in the digital economy while respecting at the same time their fundamental rights.
New regulations are also expected from the resolution to support a competitive European marketplace in the digital sector and to find in the Digital Services Act a disruptive game changer in the setting of new global standards.[8]

As for what it regards the "Digital Services Act: Adapting Commercial and Civil Law Rules for Commercial Entities Operating Online", the resolution calls for increased fairness, transparency, and accountability for the digital services' content moderation processes, and advocates for independent access to the courts, with the intention of ensuring that fundamental rights are respected.
Furthermore, the resolution also calls for a structured "notice-and-action" system for illegal contents, for extensive guidelines addressing internet advertising, in particular targeted advertising, and for the ability to create and deploy smart contracts.[9]

[6] Directive 2000/31/EC;
[7] Directive 2000/31/EC*, art. 3, co.1;*
[8] European Parliament, P9_TA(2020)0272;
[9] European Parliament, Digital Services Act: adapting commercial and civil law rules for commercial entities operating online - European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), P9_TA(2020)0273, October 20, 2020;

Finally, the non-legislative resolution on the "Digital Services Act and Fundamental Rights Issues Posed" emphasizes the necessity of legal clarity for platforms and users as well as the respect for fundamental rights, in light of the quick advancement of technology.
It also demands for harmonized regulations, for dealing with illicit online content as well as for liability exemptions and content moderation, in addition to outlining clear responsibilities for both the platforms and the authorities as for the reporting and transparency obligations.

## 2. The Legal Framework

The first and most important legislation, which constitutes the current EU regulatory framework in the sector of the online digital services, is the e-Commerce Directive (ECD),[10] which, after more than twenty years since its introduction on 8 June 2000, has taken hold in the European Union in a disruptive way, becoming a real milestone of the European digital single market.[11]

Adopted in 2000, when the most part of the modern technologies were not yet even developed and the digital platforms were still at their very early stage of life, the ECD presents a very wide scope, which involves any digital service we are used to living with, resulting in a sort of general and horizontal discipline grounded on four main pillars, namely: a) freedom to provide information society services[12] in each Member State, subjected just to the laws of the Member State where the specific services provider is established ("state of origin" principle); b) the harmonization of EU rules concerning the consumer protection, with a particular focus on the applicable transparency regime; c) the liability regime for illegal contents,[13] subject to exemptions for some platforms under specific conditions; d) the promotion of strategic techniques for the regulation and the enforcement of the law.[14]

[10] Directive 2000/31/EC;
[11] DE STREEL, HUSOVEC, *The e-commerce Directive as the cornerstone of the Internal Market*, 9;
[12] CJEU, on the definition of "information society services: Case C-108/09, *Ker-Optika*, ECLI:EU:C:2010:725, Case C-291/13, *Papasavvas*, ECLI:EU:C:2014:2209, Case C-484/14, *Tobias McFadden v. Sony Music*, ECLI:EU:C:2016:689; Case C- 434/15 *Asociación Profesional Élite Taxi*, ECLI:EU:C:2017:981 or Case C-390/18 *Airbnb Ireland UC*, ECLI:EU:C:2019:1112;
[13] CJEU, Cases C-236/08 to C-238/08, *Google France and Google v. Vuitton*, ECLI:EU:C:2010:159; Case C-324/09, *eBay*, ECLI:EU:C:2011:474; Case C-70/10, *Scarlet*, ECLI:EU:C:2011:771; Case C-360/10, *Netlog*, ECLI:EU:C:2012:85; Case C-314/12, *UPC Telekabel Wien*, EU:C:2014:192; Case C-484/14, *Tobias McFadden*; Case C- 18/18, *Glawischnig*. ECLI:EU:C:2019:821;
[14] DE STREEL, HUSOVEC, *The e-commerce Directive,* 12 *;*

These pillars represent the essence of the current legislation in the European digital market and aim to incentivize the growth of new online platforms as well as the expansion of competitive e-commerce activities, while increasing at the same time higher standards for the protection of fundamental rights.

Such a discipline, however, despite many clarifications on the ECD's scope offered over time by the EU Court of Justice,[15] presents multiple divergences between the different EU jurisdictions, which often gave rise to conflicting interpretations among various EU member states. Therefore, further sector specific EU laws have been adopted in the last twenty years, with the aim of regulating certain profiles of the information society services, serving as exemptions to the general regime established by the e-Commerce directive, but without ever undermining the fundamental logic and principles established therein. On the contrary, these innovations in the ECD's regime have complemented over the years each of its four pillars, going on to target specific information society services in some cases, and more generical providers of all types of services in other cases.

Among these provisions, the Directive 2010/13/EC,[16] as amended by Directive (EU) 2018/1808 on video-sharing platform providers ("AVMSD"), defines the European approach in the regulation of audiovisual contents and commercial communications. [17]
The 2018 directive addresses all the platforms hosting illegal contents, for which they are not considered responsible, in the fields of child pornography, terrorism, racism, xenophobia and hate speech, imposing on them new obligations to take preventive actions on a better content organization, without influencing directly the contents their selves.[18] Any restriction imposed by the member states that would bring to ex-ante control measures or upload-filtering of contents would represent in fact a clear infringement of the general monitoring prohibition set out in the ECD.[19]

[15] Joined Cases C-509/09 and C-161/10 *eDate Advertising* and *Martinez v. MGN* EU:C:2011:685;.
[16] 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), (2010), OJ L.95, p. 1-24;
[17] Directive 2018/1808/EU of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, (2018), OJ L.303, p. 69-92;
[18] Directive 2018/1808/EU , AVMSD, recital 48;
[19] Directive, 2000/31/EC, e-Commerce Directive, art. 14;

Art.17 of the Directive on Copyright in the Digital Single Market (CDSM Directive) similarly stands as an exemption to the general regime set by the e-Commerce Directive, introducing a new liability regime for the online content-sharing service providers (OCSSPs) and imposing new obligations on the online platforms, regarding the methods which they should follow in order to manage illegal information and, particularly, the illegal copyright infringements therein committed.[20]

In addition to the mentioned directives, other recent norms might be mentioned as well in the framework of the current EU digital single market's legislation, as part of the substantive background which has created the perfect context for the DSA proposal.

Among them we might recall the "platform to business" regulation, which aimed to ensure higher fairness and transparency standards for business users of online intermediation services,[21] as well as the 2019/2161 Directive (EU), which, amending the previous consumer protection's legislations, has revised both in order to adapt the consumer protection's strategy at the digital age.[22]

Equally relevant is also the "General Data Protection" Regulation,[23] which not only reproposes the same data subject's rights already previously introduced in the so called "Privacy Directive",[24] but also introduces new safeguards, with aim of strengthening the right to be delisted, the data mobility and the explainability of automated decisions.

Finally, among the other acts which ultimately contributed to the formation of such a digital regulatory environment, the European Commission encouraged both a self- and a co-regulation of the various digital service providers, in certain very delicate sectors such as

[20] Directive 2019/790/EU of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, art. 17, (2019), OJ L. 130, p. 92-125;

[21] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, (2019), OJ L. 186, p. 57–79;

[22] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules;

[23] Regulation (EU) 2016/679;

[24] 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), (2002), OJ L. 201, p. 37–47;

counterfeit goods,[25] child sexual abuses, terrorist content,[26] hate speech[27] and fake news/online disinformation.[28]

### 3. The Digital Services Package

In the second pillar of the EU digital strategy,[29] namely "a fair and competitive economy", the EU Commission has laid out all the premises for a comprehensive set of new rules, which, in the intentions of the Commission, should have brought to a unique "Digital Services Act" package, intended for all the digital services, with a particular focus on certain online platforms of very big dimensions.

Taking note that, due to the significant scale that some platforms have acquired, they have become effectively capable to act as "private gatekeepers to markets, customers and information", the Commission's "*Shaping Europe's Digital Future"* Communication explicitly underlines the necessity to safeguard the fairness and the openness of our markets, by making sure that rules are also applied online.[30]

With this approach, the EC has set down some key actions which it aimed to carry out within the following five years, among which we might mention the purpose to strengthen the responsibility of online platforms, the intention to make sure that EU rules are fit for a digital economy and the goal of ensuring a fair competition for all companies in Europe.

On December 15th, 2020 the European Commission finally presented an ambitious reform of all the digital space, a first comprehensive rulebook for the online platforms that we all depend on in our daily lives, including social media, online marketplaces and other online

[25] European Commission, *Memorandum of Understanding,* Ref Ares(2016)3934515, July 26, 2016;
[26] European Commission, *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online,* IP/15/6243, December 3, 2015;
[27] EUROPEAN COMMISSION, *Code of conduct on countering illegal hate speech online,* June 30, 2016, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en*;*
[28] EU Code of Practice on Disinformation, 28 June 2018;
[29] European Commission, COM(2020) 67 final, 7;
[30] European Commission, COM(2020) 67 final*,* 10;

platforms operating within the EU: [31] the Digital Services Package, composed of the "Digital Services Act" [32] and the "Digital Market Act".[33]

Both the proposals are structured on the basis of the European core principles and values.[34] The new regulations aim to result in a fairer and more accessible digital space for everyone, as well as in an improved online protection for consumers and their fundamental rights.

A modern set of regulations for the EU's single market should promote competition, growth and innovation, while giving citizens access to new, trustworthy and improved online services.

Furthermore, in the intentions of the lawmaker, the package will facilitate the growth of smaller platforms, small and medium enterprises (SME's) and start-ups, by cutting compliance costs and giving them simple access to customers throughout the entire single market.[35]

Lastly, the new regulations will also forbid unfair terms imposed by digital platforms that have already become or are expected to become single market gatekeepers, in order to increase the protection standards of businesses and citizens across all the EU territory.[36]

The two proposals are posed at the heart of the Commission's ambition to build this "Europe's Digital Decade", a document published in 2021 setting out the EC digital ambitions for 2030 and establishing a monitoring system in addition to outlining key milestones and the means of achieving these ambitions.[37]

[31] European Commission, *Europe fit for the Digital Age: Commission proposes new rules for digital platforms,* Press release*,* IP/20/2347, Brussels, December 15, 2020; European Commission, *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment*, IP/22/2545, Press release, Brussels, April 23, 2022;

[32] European Commission, COM/2020/825;

[33] European Commission, COM/2020/842;

[34] Consolidated Version of the Treaty on European Union (TEU), OJ C326/13, October 26, 2012, art.2; Charter of Fundamental Rights of the European Union, OJ C364/1, December 18, 2000;

[35] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending directive 2000/31/EC (Digital Services Act), (2022), OJ 277, 1-102, recital 49; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending directives (EU) 2019/1937 and (EU) 2020/1828 (digital markets act), (2022), OJ 265, 1-266, recital 24;

[36] European Commission, IP/20/2347;

[37] European Commission, *2030 Digital Compass: the European way for the Digital Decade*, COM(2021)118 final, Brussels, March 9, 2021;

Following the presentation of the two proposals on December 15th, 2020 from the Commission, the European Parliament and the Council reached a provisional agreement on March 24th, 2022 for the DMA[38] and on April 23rd, 2022 for the DSA.[39]

The EU Parliament later adopted on July 5th, 2022 both the regulations of the DSA and of the DMA,[40] while the Council gave its final approval to the DMA on July 18th, 2022 [41] and to the DSA on October 4th, 2022.[42]

Both the proposals have ultimately been signed by the Parliament and the Council and later published in the *Official Journal of the European Union* correspondingly on October 12th, 2022 [43] and on October 27th, 2022.[44]

## 4. General Provisions

### *4.1 The Scope of Applicability*

The Digital Services Act leaves intact the current applicable legislation, composed by the e-Commerce Directive and the other sector specific laws,[45] complementing it with further provisions on transparency, disclosure and accountability, which do not overlap with the existing framework, but only integrate it in order to respond with more efficiency to the modern challenges, which could not have been foreseen twenty years ago, at the time of the e-Commerce Directive' s introduction.[46]

---

[38] Council of the European Union, *Proposition de Règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (legislation sur les marches numériques),* 2020/0374(COD), Brussels, May 11, 2022;

[39] Council of the European Union, *Proposition de règlement du Parlement Européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les service numériques) et modifiant la directive 2000/31/CE*, 2020/0361(COD), Brussels, June 15, 2022;

[40] European Parliament, *position of the European Parliament adopted at first reading on 5 July 2022 with a view to the adoption of Regulation (EU) 2022/... of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, EP-PE_TC1-COD(2020)0374 - EP-PE_TC1-COD(2020)0361, July 5, 2022;

[41] Council of the European Union, *Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, PE-CONS 17/22, Brussels, July 11, 2022;

[42] Council of the European Union, *DSA: Council gives final approval to the protection of users' rights online*, Press release, 808/22, October 4, 2022;

[43] Regulation (EU) 2022/1925 (DMA);

[44] Regulation (EU) 2022/2065 (DSA);

[45] Regulation (EU) 2022/2065, Digital Services Act, art.2 (3-4);

[46] EUROPEAN COMMISSION, *Public consultation on the regulatory environment for platforms, online intermediaries and the collaborative economy,* 9, January 26, 2016, https://digital-strategy.ec.europa.eu/en/library/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud;

The DSA Regulation applies to every online intermediary which provides services to businesses and consumers in the EU, on the basis of a substantial connection, regardless of the place of establishment, whether it is within or outside the European Union.[47]

Such a substantial connection to the Union should be assumed to be existing every time that a service provider is established within the Union or, in absence of such requirement, when the number of service recipients in one or more Member States is relevant compared to the population of that country, or even just when activities are targeted towards one or more Member States. Such targeting activities may be established on the basis of all relevant circumstances and may also result from the availability of an application in the appropriate national application store.
Moreover, when a service provider directs its operations to one or more Member States, as defined by Article 17(1), point (c), of Regulation (EU) No 1215/2012 of the European Parliament and of the Council, a significant relationship shall also be presumed to exist, while, on the contrary, a website's simple technical accessibility from the Union cannot be taken into account as establishing a meaningful relationship to the Union.[48]

Relying on the principle of proportionality, the Regulation establishes a "scalar" discipline[49] and distinguishes the obligations of its recipients based on a distinction among different types of services and seizes characterizing the ISPs, that is that the more some categories of intermediaries are going to be specialized in providing certain services or the bigger their dimensions are going to be, the stricter are also going to be the obligations to respect, in order to be qualified as compliant to the applicable legislation.[50]

The first category of recipients is represented by the providers of certain types of information society services (ISS), that are the "intermediary services providers",[51] where with information society services we mean, in accordance with the Directive (EU) 2015/1535,

[47] Regulation (EU) 2022/2065*,* Digital Services Act, art. 2 (1);
[48] Regulation (EU) 2022/2065*,* Digital Services Act recital 8;
[49] FERRARIS, *Digital Service Act approvato dal Parlamento europeo: le novità sugli intermediari online*, in *Il Quotidiano Giuridico,* July, 13, 2022, https://www.altalex.com/documents/2022/07/13/digital-service-act-approvato-parlamento-europeo-novita-intermediari-online;
[50] CONDEMI, *Digital Services Act: cos'è e cosa prevede la legge europea sui servizi digitali*, in *Agenda Digitale,* (2022 FERRARIS, *Digital Service Act approvato dal Parlamento europeo: le novità sugli intermediari online*, in *Il Quotidiano Giuridico,* July, 13, 2022, https://www.altalex.com/documents/2022/07/13/digital-service-act-approvato-parlamento-europeo-novita-intermediari-online;);
[51] Regulation (EU) 2022/2065 (digital services act), art.3(g);

"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[52]
Recalling the legislation already set down with the e-Commerce Directive more than twenty years ago,[53] the intermediary services providers are divided in three categories, namely providers of mere conduit (transport of information), caching (temporary storage) and hosting (storage on request) services.

The "mere conduit" service definition inherited by the ECD refers to such activity as an information society service consisting "of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network".[54]
In this case the intermediary service provider is not aware of the nature of the information passing through its computers or its cables and limits itself just to transport, in a mechanical and passive way, the data transmitted by third parties, without knowing the content therein. In other words, the mere conduit behaves in the same way as a carrier behaves in the transport of sealed containers, since the information is transmitted using communication protocols, which can be compared to ancient codes used for reading secret encrypted messages in times of war.[55]

On the other hand, the "caching" services are defined as information society services 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, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request".[56]
Such storage takes place to allow the user who surfs on the internet to access more quickly the information he wants, because instead of queuing in front of the website he is looking for, due to the presence of other visitors after the same, once he has had access to the intermediary's computer memory hosting the searched website, he can make a copy of the web page and download it into the memory of its intermediary's computer, in order to have

[52] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), *OJ* L. 241/2015, 1-14, art.1(b);
[53] Directive 2000/31/EC, section 4;
[54] Regulation (EU) 2022/2065 (digital services act), art.3, letr.g (i);
[55] BOCCHINI, *La Responsabilità Civile degli Intermediari,* 32;
[56] Regulation (EU) 2022/2065 (digital services act), art.3, letr. g (ii);

access to the pages of the website without going through the computer of the intermediary hosting that particular page.[57]

Lastly, the so called "hosting" services are considered by the Regulation as information society services consisting of "the storage of information provided by, and at the request of, a recipient of the service".[58]
With such services the intermediary provides a web space on the internet (free of charge or in exchange for a fee) and the information is stored permanently on its computer,[59] making it possible for the intermediary to easily know the content of such information.

In addition to the canonic distinction between mere conduit, caching and hosting services depicted by the ECD, the DSA typifies another two figures of recipients addressed by the Regulation, that are the so called "online platforms" and the "online search engines".

As for the "online platforms", they can be considered a particular type of hosting platforms[60] which, "at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".[61] In short, the storing activity with the dissemination of information to the public must represent the primary activity of the provider, while providers disseminating information to the public as a secondary and ancillary service feature, like for example a comment section of an online newspaper, will be excluded from this category.

[57] BOCCHINI, *La Responsabilità Civile degli Intermediari,* 33;
[58] Regulation (EU) 2022/2065 (digital services act), art.2, letr.g (iii);
[59] TOMMASI, *Protocolli TCP/IP e Problematiche Contrattuali di Accesso alla Rete Internet,* in SIROTTI GAUDENZI (EDT.), *Trattato Breve,*145;
[60] On the difference between online platforms and hosting providers see PINSENT MASONS, *A guide for online intermediaries on the scope of the EU Digital Services Act,* October 28, 2022, https://www.pinsentmasons.com/out-law/guides/guide-digital-services-act-for-online-intermediaries#:~:text=Online%20platforms%20are%20considered%20a,information%2C%20they%20disseminate%20it%20too;
[61] Regulation (EU) 2022/2065 (digital services act), art.3(i);

In this regard social networks, app stores and marketplaces might be considered to fall within this category of intermediaries, whereas emails and private messages generally fall outside the scope, until they do not reach an open number of persons.[62]
Moreover, when referring to "dissemination to the public" as used in this Regulation, such an expression should be interpreted as making information easily accessible to any service recipient, generally without further action to be taken and regardless of whether that person actually accesses the information in question. Therefore, where access to information requires registration or admission to a group of service recipients, only the cases in which service recipients are automatically registered or admitted, without a human decision or selection, should be regarded as public dissemination.[63]

On the other hand, the other type of online intermediaries, i.e. online search engines, which were originally absent in the initial proposal and have just ultimately been introduced by the final draft of the Regulation,[64] is referred from the DSA as "an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found".[65]

For what it regards the scalar distinction between recipients based on a dimensional criteria, it is only when reaching significant sizes that the online platforms as well as the online search engines may also be designated as "very large online platforms" (VLOPs) and "very large online search engines" (VLOSEs), which are identified at art. 33 of the Regulation as "online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million".[66]
This further classification of online intermediaries represents, more than any other provision, the category by far most impacting on the digital economy, as it puts very strict limits on the

[62] ORRICK (APOSTLE, HAGEDORN, SCHRODER, YAVORSKY, EGAN SUSSMAN, KAWKABANI), *The European Commission's Digital Services Act (DSA) is Approved: What You Need to Know,* October 28, 2022, https://www.orrick.com/en/Insights/2022/10/The-European-Commissions-Digital-Services-Act-is-Approved-What-You-Need-to-Know;
[63] Regulation (EU) 2022/2065 (digital services act), recital 14;
[64] VAN HOBOKEN, *Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU*, in 13 *Int. J. Com. L. Pol.,* 1-21, 7, (2009); RICCIO, *Profili di responsabilità civile dell'Internet Provider*, in STANZIONE, *Quaderni del Dipartimento,* Dipartimento di diritto dei rapporti civili ed economici nei sistemi giuridici contemporanei, Salerno, 2000, 98;
[65] Regulation (EU) 2022/2065 (digital services act)*,* art.3(j);
[66] Regulation (EU) 2022/2065 (DSA), art.33 (1);

major players of the market sector, the so called "big techs", ranging from Google to Meta, via Amazon, Twitter and others.[67]

Due to their limitless extension through the entire globe, such platforms have acquired a crucial role in modern societies, not only promoting a public debate on topical issues affecting the life of billions of citizens from all over the world, but also pushing the economy to grow in new and unexplored markets, having therefore an impact on the fundamental tenets of contemporary democracies.[68]

Accordingly, they are called by the Regulation to grant the integrity of their services as well as the adequacy of their risk management systems, with even a greater attention than that which could be required from all the other types of online intermediaries.[69]

Lastly, micro and small companies in the EU, with less than 45 million monthly active users, are excluded from some of the new provisions of the DSA, in order to protect the growth of start-ups and small businesses in the internal market.[70]

Once established the set of recipients addressed by the Regulation, some clarifications are however necessary to better understand the regulatory scope of the online search engines. The classification of such new figures, in fact, becomes more problematic considering the particular attention which has been paid to it by the European lawmaker. Added just at a later stage than the original proposal,[71] the online search engine's definition has been in fact reserved an autonomous space within the DSA Regulation.[72]

Unlike what was done in the United States' DMCA[73] and despite being referred as an "intermediary service", therefore deserving the same rank of mere conduit, caching and hosting services, such figure has not been included among the different typologies of

---

[67] LINKLATERS, *European Commission proposes impactful reform of rules for digital platforms,* *https://www.linklaters.com/en/insights/publications/2020/december/european-commission-proposes-impactful-reform-of-rules-for-digital-platforms;*

[68] STARK, STEGMANN, JÜRGENS & MAGIN, *Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse*, 52, May 26, 2020, https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf; SCHANZER, *Can Lawmakers Save Democracy from Big Tech?,* in *Georgetown Journal of International Affairs,* September 7, 2021, https://gjia.georgetown.edu/2021/09/07/can-lawmakers-save-democracy-from-big-tech/;

[69] Regulation (EU) 2022/2065 (DSA), art. 40, para. 4;

[70] Regulation (EU) 2022/2065 (DSA), artt. 29, 19, 15 (§2), recitals 49, 57

[71] PALUMBO, *Il Digital Services Act diventa legge,* in *Deberti Jacchia Franchini Forlani*, 2, November 8, 2022, https://www.dejalex.com/2022/11/il-digital-services-act-diventa-legge/?lang=it;

[72] Regulation (EU) 2022/2065 (DSA), art. 3, letr. j;

[73] Digital Millennium Copyright Act (17 U.S.C., adopted 28 October 1998), sec. 512 (D);

"intermediary services", which in the DSA are listed in art. 3(g),[74] making it consequently uncertain whether the lawmaker actually intended to identify a new type of intermediary service provider, parallel and alternative to the others despite being located in another article, or if it rather intended to define separately this figure, in the absence of real autonomy with respect to one of the already existing figures of intermediaries, as recital 28 would also suggest.[75] In this case, however, the legislator would have omitted to indicate precisely which of the already existing categories of intermediaries this figure belongs to.
Such doubt arises even more so in light of the fact that, where the legislator intended to specify a new category of intermediary service falling within one of the existing types of intermediaries listed by Article 3 (g), as in the case of online platforms,[76] it clearly stated that such a figure represented a specific typology of "hosting service", equipped with particular characteristics indicated in the Regulation. Conversely, with regard to the providers of search engines, despite their exclusion from the list of intermediary services, nothing is specified regarding their relationship with any of the other categories mentioned in Article 3g, giving almost the idea that search engines are distinguished and autonomous entirely compared to them.

Furthermore, based on a reading of the Regulation's text and despite a long-running debate going on this topic, [77] some may also think that this category of intermediary services actually represents a particular type of online platform, or at least hosting provider, considering that Article 24 of the DSA, entitled "Transparency reporting obligations for providers of online platforms",[78] provides for some transparency obligations that, in addition to apply to online platforms, also explicitly refer just to online search engines. This is also supported by the fact that once online search engines reach certain sizes, they will acquire a whole series of new additional responsibilities, on a par only with those that online platforms will also assume once they have reached a certain dimension.[79]

---

[74] Regulation (EU) 2022/2065 (DSA)„ art. 3, letr. g;
[75] Regulation (EU) 2022/2065 (DSA), recital 28;
[76] Regulation (EU) 2022/2065 (DSA), art. 3, letr. i;
[77] GOZZO, *Responsabilità del motore di ricerca nel caso di "caching",* October 25, 2012, https://francescogozzo.com/motore-di-ricerca-responsablita/; ROSATI, *Italian Supreme Court considers search engines hosting providers and finds them potentially eligible for the application of the hosting safe harbour,* July 3, 2022, https://ipkitten.blogspot.com/2022/07/italian-supreme-court-considers-search.html; PORTOLANO CAVALLO, *Direttiva eCommerce e responsabilità dei motori di ricerca: recenti orientamenti giurisprudenziali,* in *Portolano Cavallo INFORM@,* July 18, https://www.key4biz.it/News-2012-07-18-Policy-google-eCommerce-Portolano-Cavallo-Studio-legale-motori-di-ricerca-211812/23856/;
[78] Regulation (EU) 2022/2065 (DSA), art.24;
[79] Regulation (EU) 2022/2065 (DSA), Chapter 3, Section V;

In this case they would not only fully fall within the category of already existing intermediaries, but also they would be further burdened by the charges and responsibilities that have been foreseen in addition for hosting providers, and even more so for online platforms. In fact, as the DSA is structured on the model of a Russian doll,[80] the increasingly burdensome and stringent obligations that apply to the different types of information society services also contain all the other less stringent obligations of the other types of intermediary service providers that entail lesser risks for society.[81] This means that defining search engines as hosting providers, or even as online platforms, for example, would entail the burden for such service providers to comply with additional and more onerous compliance obligations compared to those provided for other mere intermediary service providers. This would be even more relevant considering that, once a certain threshold of size is exceeded, such providers will be subject, like the "very large online platforms", to the most stringent and burdensome obligations provided for by this Regulation, causing a sudden or gradual transition from a lax regime to a much more stringent one, depending on whether such figure falls within one of the other intermediate figures interposed between simple "intermediary service providers" and the most impactful "very large online search engines".

Nevertheless, it should be noted that, apart from the mention in Article 24, section II, chapter 3, which establishes "additional provisions applicable to providers of online platforms", almost always mentions exclusively the category of the "online platforms", and practically never the category of the "online search engines". Therefore, the possibility remains that the obligations shared by the two categories are only limited to Article 24, maintaining the online search engines autonomy with respect to online platforms and more generally with respect to hosting providers. It remains so still unclear, as it was already within the e-Commerce Directive, the real nature which must be attributed to the figure of the online search engines.

[80] BUITEN, *The Digital Services Act From Intermediary Liability to Platform Regulation,* in 12 *JIPITEC*, 361-380, 367, (2021);
[81] SAVOVA, MIKES, CANNON, *The Proposal for an EU Digital Services Act: A closer look from a European and three national perspectives: France, UK and Germany,* in 22(2) *Comp. L. Rev. Int.*, 38-45, 38,40, (2021); CARVALHO, ARGA E LIMA, FARINHA, *Introduction to the Digital Services Act, Content Moderation and Consumer Protection*, in 3(1) *Rev. Dir. Tec.,* 71-104, 76, (2021); WILMAN, *Het voorstel voor de Digital Services Act: Op zoek naar nieuw evenwicht in regulering van onlinediensten met betrekking tot informatie van gebruikers,* in *Ned. Tijds. V. Eur. Rec,* 27-36, 28, (2021);

*4.2 The Structure and the Objectives*

During the Impact Assessment carried out in June 2020,[82] three different policy options have been explored by the European Commission to respond promptly to the next "Europe's Digital Future" challenge, [83] already launched by the Commission in February of the same year.

For that occasion, diverse citizens and stakeholders were invited to participate and to provide feedback on the intended initiative, with the aim of providing a modern legal framework for the Digital Single Market, where digital services providers are called to more responsibility and respect of EU values, and where a new governance online is set down with the purpose of defining clearer roles, procedures and responsibilities for all the digital market's players.

One of these alternatives, in substance, intended to codify the 2018 Recommendation on Illegal Content,[84] with the objective of changing the existing system of intermediary liability and with the intention of making it more complicated, adding ultimately fresh concepts for gatekeeping platforms. Such a change could have also impacted on the scope and on the extent of the state of origin's principle, as well as of the disclosure obligation and of the modalities of cooperation.[85]

In addition to what already established with the first alternative, a second option would have also increased transparency standards and promoted a voluntary monitoring, whereas a third alternative, built on the previous two, would have provided ex ante restrictions on gatekeeping platforms, subjecting intermediaries with a considerable market power to an identification system and to specific requirements to comply with.

This last option might have been advantageous for the flexibility which enables different platforms to be treated in different ways, but could have been risky for its innovativeness within the field of the digital platforms, whereas in the telecoms sector a long-term experience has already been gained over the decades, reaching a high level of specialization.[86] Such a discipline, in fact, being a derivation of the competition law, is already applied within the EU in the sector of the Telecommunications (TMT), where

[82] European Commission, *Impact Assessment, Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services*, Ref. Ares(2020)2877686, July 4, 2020;
[83] European Commission, COM(2020) 67 final
[84] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ L. 63, *p. 50–61;*
[85] SAVIN, *The EU Digital Services Act*, 6;
[86] SAVIN, *The EU Digital Services Act*, 7;

determined enterprises with a significant market power are required to comply with specific obligations.

As a result of this comparison, the solution chosen by the lawmaker turned out to be a combination of all the three alternatives, leaving intact both the 2001 e-Commerce Directive and the sector specific laws derived from it,[87] and creating, within the DMA proposal, a separate ex-ante regime for the gatekeeping platforms.[88]
Accordingly, the structure of such a solution has therefore been divided into four chapters: the first chapter outlines general provisions, indicating the recipients, the objectives and the scope, together with the definitions of important terms used in the Regulation, whereas a second chapter sets down a new liability regime, which provides a set of exemptions to the previous ECD regime, and which recalls the prohibition for Member States to require intermediaries a general monitoring on their platforms. The third chapter, for its part, defines several due diligence obligations, aimed at guaranteeing a safe and transparent online environment and divided in five main sections addressing all the providers (Sect. 1), the providers of hosting services (Sect. 2), the online platforms (Sect. 3), and the very large online platforms (Sect. 4), and defining rules on due diligence, as well as standards and codes of conduct (Sect. 5). Lastly, the fourth chapter establishes a comprehensive discipline on the enforcement of this Regulation, attributing the corresponding responsibilities to each national authority.

Such an approach, based on Article 114 of the Treaty on Functioning of the European Union,[89] which promotes the correct functioning of the internal market, aims to create the best conditions for the growth of new digital services in the internal market, by fostering a stronger online protection of the fundamental rights, and by strengthening the level as well the number of corporate responsibilities in the digital sector, within the context of a harmonized and horizontal legal framework.

Only by acting at a Union level it is in fact possible to grant the consistency of the actions against illegal contents, as well as to increase predictability and legal certainty, while

[87] POLLICINO, G. DE GREGORIO, *L'Alba di Nuove Responsabilità sulle Piattaforme Digitali: il Digital Services Act,* in *Agenda Digitale,* December 15, 2020, https://www.agendadigitale.eu/sicurezza/privacy/lalba-di-nuove-responsabilita-sulle-piattaforme-digitali-il-digital-services-act/;
[88] European Commission, COM(2020) 842 final:
[89] TFEU, art.114;

lowering compliance expenses for all Member States. The transnational nature of the internet indeed does not permit legislative initiatives carried out on a national level to guarantee a satisfactory level of protection for the citizens and the businesses.
Moreover, just by granting such a context of clarity and legal certainty, the DSA might facilitate the digital internal market to grow in a fair and competitive way, giving the possibility to small but innovative businesses to start-up and scale-up, defending themselves from the influence of both larger companies and public authorities.

### *4.3 The Subject Matter*

In accordance with these objectives, the DSA establishes a safer online environment and ensures a higher consumer protection level, placing on digital services providers, and particularly on "online platforms" such as social media and marketplaces, a new accountability regime and a clear set of due-diligence obligations, which, in the intentions of the lawmaker, will increase both the transparency and the liability standards of these platforms.

The last one of these two innovations, namely a new set of due diligence obligations, is supposed to prevent the abusive use of the platforms' services, as well as to promote the adoption of responsible practices, by requiring digital services providers to respect a certain number of guarantees for the protection of fundamental rights, such as rigid notice and action procedures, new techniques of content moderation, and the possibility to challenge the platform's decisions.
Among those obligations, due to their specific characteristics, some online platforms are additionally required to ensure even higher standards of transparency and safety in the online environment, by enhancing activities of the type of receiving, storing, partially verifying and publishing information on the traders which are getting advantaged of their services.

As for the accountability regime, the DSA keeps in place the e-Commerce Directive's provisions, [90] which, given also the several interpretations offered by the European Court of Justice, have long been recognized as an authentic cornerstone of the digital economy as well as an essential tool for the online protection of basic rights.[91]

[90] Directive 2000/31/EC, artt.12-15;
[91] DE STREEL, HUSOVEC, *The e-commerce Directive,* 8;

Those provisions, however, considering the necessity of a full harmonization throughout the Union and the lack of clarity in some parts of the e-Commerce Directive,[92] have been integrated within the DSA Regulation, with the intention to reduce at the minimum the Member States' capacity to modify them, and with the purpose of providing legal certainty for businesses and consumers alike.
Just by resorting to a Regulation, in fact, it is possible to ensure a constant standard of protection across the Union, which prevents different legislations from limiting the freedom to provide services, by granting uniform rights and obligations for everybody.

Finally, in order to enforce a strict control and an effective application of this law, the present Regulation sets a new reinforced cooperation between Member States of the Union, in the perspective of an open and free market, where citizens and businesses can easily take action to guarantee the safeguard of their rights.
Member States are therefore required to supervise the compliance of the digital platforms with the DSA Regulation, providing simple and clear procedures, which are expected to enhance the trust in the institutions and the dialogue between the private and the public forces. Only where national authorities fail to guarantee a satisfactory level of homogeneity and where systemic risks might occur across several states of the Union, national authorities are required to step aside, in order to appoint the Union as the competent authority for the enforcement and the supervision of the Regulation.

[92] BASSINI, *Mambo Italiano: The Perilous Italian way to ISP Liability,* in *Fund. R. Prot. On.,* 84-114, 100, (2020);

# Chapter 3

# THE LIABILITY REGIME

The current digital landscape has undergone in the last decades a significant transformation, with the proliferation of digital services having a far-reaching impact on society. New business models including digital platforms have contributed to bring new growth opportunities for the single market and for the exercise of fundamental rights and freedoms, in particular freedom of expression.

The users benefiting from such services have become capable to perform an incredible number of activities through the internet, without even spending any money and with just a basic knowledge of the functioning of the web. Any person has become capable to transfer, reproduce or spread enormous amounts of contents of any type and any tool, which has been made readily accessible by modern technological facilities, may now be used to post texts, photographs, music and movies on a website.

At the same time, however, the development of the information society has amplified the risks for users, increasingly subject to the services provided by digital platforms, giving rise to a lot of problems which concern the liability of such platforms.

The damages that may occur within the information society's services are characterized by both their rapidity and their geographical extent. The disseminative capabilities of the Internet and the ease of accessing the network have exacerbated even more the potential for harm and facilitated the production of significant, swift, and repeated injuries to protected situations.

Additionally, the difficulties inherent in the international and decentralized nature of the internet pose a challenge in holding individuals accountable for violations committed. The decentralized nature of the Internet, in fact, can allow individuals to evade responsibility by

choosing to locate their server or to publish illegal content in a jurisdiction where the responsible party cannot be pursued, even if they have been accurately identified.[1]

Cyber offenses are also distinct from other offenses due to their subject matter, which is digital information and its inherent intangible nature, that impacts the unlawful act, rendering it without physicality and consisting of the unauthorized automatic processing of information in the form of bits. This characteristic cannot but affect the nature and structure of the offenses, which are also necessarily intangible, and give rise to a new type of offenses, characterized as informational, due to their association with the processing and circulation of illegal information, such as false, misleading, counterfeiting, defamatory or slanderous information.
Moreover, the common informational content distinguishes cyber offenses also by the potential duration of the violations committed,[2] perpetuated through a permanent means of information like the internet, and by their exceptional capacity for harm, resulting from the network's dissemination capabilities.

That being the case, some categories of legal violations, which are committed online thanks to the services provided by online intermediaries, might be distinguished on the basis of the particular material which is displayed therein. Among these materials, the most common illegalities committed on the web generally regard: a) the copyrighted materials, which, considering how simple it is to distribute creative material on the internet, are one of the legal areas most impacted by these violations; b) illegal and harmful contents, including elements such as pornographic, racist or terrorist contents, hate speech;[3] c) private and defamatory material, that regards contents such as intimate pictures, family information, financial or tax records or other types of private or disparaging information, which violate numerous privacy rights like those outlined in the EU data protection and antidefamation legislation; d) misrepresentative contents, recurring when fake news,[4] wrong news or deep fake contents,[5]

[1] Court of Lecce, February 24, 2001, in 124(6) *Foro it.,* I, 2001, 2031; 1; Court of Rome, March 22, 1999, in *Dir. Inf.,* 2000, 66; Court of Verona, December 18, 2000, in 124(6) *Foro it.,* II, 2001, 2032; Court of Rome, March 9, 2000, in *Interlex Diritto e Tecnologia,* http://www.interlex.it/testi/rm000309.htm;
[2] CASSANO, BUFFA, *Responsabilità del Content e dell'Host Provider,* in *Corr. Giur.,* 2003, 81; BOCCHINI, *La Responsabilità Civile,* 203;
[3] MACAVANEY ET AL., *Hate Speech Detection: Challenges and Solution*, in 14(8) *Pl. O.*, 1-16, 5, (2019);
[4] GUERINI, *Fake New e Diritto Penale: la Manipolazione Digitale del Consenso nelle Democrazie Liberali,* Giapichelli, Torino, 2020, 143;
[5] SUGANTHI, ET AL., *Deep learning model for deep fake face recognition and detection,* in 8 *P. Comp. Sci.*, 1-20, 2, (2022);

published and disseminated thanks to the use of these online platforms, provoke damages to third parties; e) other types of contents, whose illegal use could be made in violation of trademarks, patents, as well as unfair trade practices.

For all these reasons, it is clear the centrality assumed by the services provided by digital intermediaries and by the relationship running between such intermediaries and the recipients of their services. It is in fact precisely in this relationship that an illicit act of the recipient himself may be inserted, determining the onset of a compensation obligation between the internet services provider and the damaged user of the network.
Already since the rise of the web, internet services providers (ISP) have been put at the center of a heated doctrinal and jurisprudential debate on the matter of their responsibility, depending on the different roles played by them in different situations.[6]

The Digital Services Act's discipline on the liability of online intermediaries lays in particular on the principles already established in the e-Commerce Directive, leaving the core of its most important provisions substantially unaffected.[7] From art. 4 to 6 the DSA recalls almost the identical essence of the provisions already set down from art. 12 to 15 of the Directive on the Electronic Commerce.[8]

However, in line with the DSA's intention to create a new horizontal legal framework, which goes to harmonize the existing legislation on the online intermediaries, the European Commission ultimately opted for a legislative act with the legal rank of Regulation, in order to make its provisions directly applicable in all Member States, and without needing an internal reception from national legislations, as it still happens with the e-Commerce Directive.[9]

Moreover, in addition to what is already established within the ECD, the DSA Regulation also sets a new range of provisions aimed to counter the spread of illegal contents, that are

[6] SICA, ZENO-ZENCOVICH, *Manuale di Diritto dell'Informazione,* 375;
[7] European Audiovisual Observatory, *Unravelling the Digital Services Act Package,* 11, October 21, 2021, https://www.obs.coe.int/en/web/observatoire/press-releases-2021/-/asset_publisher/alYLDl7HvAtD/content/unraveling-the-digital-services-act-package;
[8] Directive 2000/31/EC;
[9] Directive 2000/31/EC; art.22;

likely going to increase the online intermediaries' liability, to the extent that they will have to comply with further measures to not be considered responsible for their users' actions.
Such new rules, due to their generality on some points, are likely going to further increase the uncertainty of the legal framework, raising the number and the complexity of interpretation issues, which will ultimately be addressed by the European Court of Justice.

## 1. The Debate on the Internet Services Providers (ISP) Liability

For a long time, due to multiple reasons such as the inertia, the delay or at least the inadequacy of the lawmaker's intervention, the internet has been considered a space out of the law, similar to other contexts in which is not present a national sovereignty, such as Antarctica, the open sea or the cosmic space.
Thereafter, more than twenty years ago, the cyber-activist John Perry Barlow released in Davos a rhetoric and imaginative "Declaration of the Independence of Cyberspace", in which a now famous call was launched by the author to safeguard the independence, the liberty and the sovereignty of the internet from the national governments.[10]

As a consequence of this void in the legislation, internet service providers have long been exposed to compensation actions for the illegal contents of third parties, especially considering that, in light of the ISP's characteristics, their identification represents the easiest solution as well as the only one actually possible in the most part of the cases.[11] Therefore, it's very common that, instead of turning to an anonymous subject or, even if identifiable, a subject who is not reliable from a financial point of view, the damaged user prefers to address his compensation claims directly to the provider of the internet service.[12]

In such a context, given the problem of the extent to which intermediaries should be held responsible for illegal acts committed by third parties, the question we will consequently have to ask ourselves will be: should internet intermediaries be found guilty of the harmful actions of internet users ?

[10] BARLOW, *A Declaration of Independence;*
[11] RICCIO, *La Responsabilità Civile*, 134; PANKOKE, *Von der Presse-zur,* C.H. Beck, Munchen, 2000, 76;
[12] SICA, ZENO-ZENCOVICH, *Manuale di Diritto dell'Informazione,* 375*;*

Already since its very beginning, the debate on the ISP's liability has appeared to be divided into two main and opposite positions, whereas if the first sustained the irresponsibility of the ISP, on the other hand the second one pushed for an increase of the ISP's accountability.
At the core of this debate, there's the difficult balance among opposite interests in the digital economy, considering that, if it is necessary to ensure the online protection of fundamental rights for both the internet users and the competing businesses, it is also true that it is a national interest to grant the actors of such economy the possibility to grow as much as possible, leaving them free to design their own business strategies and avoiding excessive burdens to be carried out.

From this perspective, considering the ISP free from any possible illegality committed by third parties on their platforms has been seen as a renunciation to the only available tool capable to control the network, to the extent that internet service providers are the only subjects in condition to intercept and discover the illegal contents on the web, as well as to punish and sanction in the shortest period the abuses committed therein.[13]

On the other hand, considering ISPs in any case responsible for the actions committed by their users would undoubtedly mean to attribute them a strict liability, imposing on them a general obligation to monitor everything that is put online and requiring them to always guarantee the compliance with the applicable law also by the third parties that are benefiting from their platforms.[14]
In this case, however, an ISP could always be held accountable regardless of whether it has knowledge of or control over the contents distributed through its services.
A burden of this type would ultimately discourage anybody from undertaking this kind of activity, therefore inducing services providers to interrupt the provision of internet connectivity, as well as pushing the businesses operating in the digital economy to settle just in the countries where it is ensured the most favorable legislation with their regards.[15]

[13] PASCUZZI, *Il Diritto*, 167;
[14] SCUDERI, *La responsabilità dell'Internet Service Provider alla Luce della Giurisprudenza della Corte di Giustizia Europea, causa c-610/15, 14 giugno 2018,* in *Dir. Mer. Tec.,* 2018*,* 1-16, *ivi* 5;
[15] PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service provider,* in 7(1) *Dan. Resp.*, 2002, 5-10, *ivi,* 5; JULIA-BARCELO, *Liability for Online Intennediaries: A European Perspective*, in 12 *E.I.P.R.*, 1-9, 6, (1998); BOCCHINI, *La Responsabilità Civile*, 26;

Within the European case law, the French judges were the first to face questions regarding extra-contractual liability from the Internet.

In the early stages, the legal debate centered on whether French press law and publishing law could be equally applied in the context of the internet, as in the very first judicial rulings the courts held that the offenses committed online should have been treated similarly to those defined in the press law.[16]

Following that, however, the French jurisprudence shifted from analogically applying press and publishing regulations to establishing the responsibility of the intermediary provider who offers hosting on its site to anonymous third parties without access restrictions.

After an initial lenient approach that excluded the intermediary's responsibility due to their ignorance of the illegal information transmitted, the jurisprudence issued some more stringent decisions, including the landmark case that changed the trend, the *Halliday* case,[17] decided by the Paris First Instance Court on June 9, 1998. In this case, the Court of Paris issued an injunction requiring the intermediary service provider to employ appropriate means to prevent the continued dissemination of certain photographs featuring a well-known model in a state of nudity. The court held the service provider accountable for its omission in informing the recipient of the service of its obligation to respect the rights of third parties, as well as its failure to supervise the content hosted on its website, which was generated by the recipient of the service.

The Paris Court of Appeal, upon being called to rule in second instance, determined that the intermediary provider, offering anonymous hospitality with no restrictions on access and enabling the dissemination of signs, writings, images, sounds and messages extraneous to private correspondence, exceeded its technical role as a mere information transmitter and is directly liable towards third parties for the commission of illegal acts carried out by the recipients of its service on the sites it manages. This liability was founded, not on the principle that the provider was obliged to monitor the content hosted on its site, but on the distinct principle that the provider, in exchange for compensation, facilitated the possibility for third parties to introduce information anonymously into its memory, effectively guaranteeing impunity. In this case, according to the Court, the intermediary service provider accepts

[16] Court of Strasbourg, February 3, 1998, in 22 *Colum-VLA J. L. & Arts,* 161, (1998); Court of Paris, April 14, 1999, in *Legalis*, https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-1ere-chambre-1ere-section-jugement-du-14-avril-1999/; Court of Lyon, July 21, 1999, in *Legalis,* https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-lyon-10eme-chambre-jugement-du-21-juillet-1999/;

[17] Court of Appeal of Paris, *Lacambre c. Hallyday,* February 10, 1999, in *Dir. Inf.,* 1999, 926-941, with note of RICCIO;

responsibility for the content posted online and is therefore liable in case of illegality towards third parties.

On the same understanding, the Court of Nanterre, in a ruling dated December 8th, 1999,[18] affirmed the civil liability of the hosting provider, recognizing that, unlike the access provider, the former provides a lasting service of information storage. The Court affirmed that the hosting provider has a general obligation of prudence and diligence that translates into monitoring the disseminated data, through the use of search engines functioning by keywords. Furthermore, the intermediary service provider and access provider cannot limit itself to requesting an email address from service users, but must actually verify their real identity. Its liability must, therefore, be evaluated in relation to the general law provisions of the civil code on the liability for third parties' actions.

Nevertheless, the rigorous stance was not unchallenged in France, as it was counterbalanced by more lenient dispositions towards intermediaries, as expressed in other branches of case law and doctrine. In the Altavista case, for instance, it was decided by judgment in 2001 that search engines are not automatically liable for the content of indexed websites. The President of the Court of Paris denied the injunction because the Altavista company, owner of the well-known search engine, was not deemed responsible for including a website among the indexed sites that infringed on the dignity and honor of a user. Indeed, according to this judgment, it is not possible to attribute objective and presumptive liability to a search engine for the content of indexed sites.

Just as in the jurisprudence the Altavista case reveals the variety of the courts' decisions, being such a case clearly inspired by a less strict criterion than the Hallyday case, similarly, in doctrine it is possible to find, just before the e-Commerce Directive was issued, very balanced opinions. Indeed, a careful examination of the studies conducted in France in the years preceding the issuance of the Directive shows that some authors had already outlined trends that would later be adopted by the Directive.[19]

With regard to the Italian legal system, the early case law has essentially maintained an ambivalent attitude, as in some decisions the responsibility of the intermediary was affirmed

[18] Court of Nanterre, December 8, 1999, in *la Semainè Juridique Edition Générale,* 2000, 577;
[19] TRUDEL, *Les Responsibilités dans Cyberspace,* in UNESCO, ECONOMICA, *Les Dimensions Internationales,* 244; BENSOUSSAN, *Internet,* 62;

on the assumption of an equivalence between the intermediary and the publisher,[20] while in others a more liberal approach has prevailed, equating the intermediary's function to that of the distributor.[21]

Following the trend already previously established by the Court of Paris in the Halliday case, in a number of decisions the provider has been attributed culpa in vigilando, given that the owner of a communication channel intended for the public of readers has the obligation to monitor the commission of acts of unfair competition that may be perpetrated through the publication of advertising messages, of which the owner must verify the obvious, truthful and correct nature. In case of default, the owner shall be held liable for the tort committed by the principal author.

Other decisions have followed the same trend, affirming the responsibility of the provider who had not exercised due vigilance,[22] while another jurisprudential approach has considered that a periodical made by using online telematic techniques may only be registered if also printed on paper, and therefore, at most, the press law may be extended analogously.[23]

Moreover, it should be noted that over time the jurisprudence has settled on the principle that there is no obligation of vigilance on the part of the provider, with respect to the contents conveyed through sites that it manages. Consequently, the provider cannot be held liable for illicit content that it has only technically allowed to transit on the network, provided that, according to some jurisprudence, the provider is not aware of the presence of illicit information on its site and takes all necessary measures to remove it.

For all these reasons, the majority doctrine found the basis of the online intermediaries' liability in the concept of the civil negligence, meaning that an ISP is deemed accountable only if it knowingly or culpably allows the infringement of other people's rights.[24]

Actual knowledge and constructive knowledge are the two separate degrees of involvement to take into account in such an evaluation of the provider's accountability.

---

[20] Court of Naples, March 18, 1997, in *Foro it.,* 1997, I, 2307; Court of Naples August 8, 1997, in *Diritto Informaz. Informat.*1997, 970;

[21] Court of Cuneo, June 23, 1997, in *Giurisp. Piem* 1997, 493; Court of Oristano, May 25, 2000, in 123(11) *Il Foro it.,*2000, 663;

[22] Court of Teramo, December 11, 1997, in *Apogeo,* https://www.apogeonline.com/articoli/abuso-del-diritto-di-cronaca-e-diffamazione-online-annarita-gili/; Court of Cuneo, June 23, 1997, in *Giurisp. Piem.,* 1997, 493; Court of Macerata, ord. December 2, 1998, in *Dir. Ind.,* 1999, 35;

[23] PALAZZOLO, *Il "Domain Name",* in 2 *N. Giur. Civ. Com.,* II, 2000, 168 ss., *ivi* 178; BUGIOLACCHI, *Principi e Questioni Aperte In Materia di Responsabilità Extracontrattuale dell'Internet Provider. Una Sintesi di Diritto Comparato,* in *Dir. Inf.,* 2000, 856 ss., *ivi* 860;

[24] BOCCHINI, *La responsabilità extracontrattuale del provider*, in VALENTINO (EDT.), *Manuale di diritto dell'informatica*, 542;

In case of actual knowledge, if an illegal content is published online on the platform of a certain ISP, then the ISP will be held accountable only when being fully aware that the illegal activity harms other people's rights, without taking any consequent action to restore a safe environment online. If instead the law opts for a so-called constructive knowledge liability, the ISP might be considered accountable not only when fully informed of the illegal activity carried on its platform, but even just in presence of a mere general knowledge of such activity, which itself could be considered sufficient to hold the ISP responsible of any tort committed on its platform.[25]

## 2. The Origins of ISP's Liability: The US D.M.C.A and C.D.A

On the eve of Directive 2000/31/EC, US jurisprudence had already begun to utilize three different models to identify civil liability in cases where multiple subjects appear to be involved in causing the damage: the so-called direct liability model, the model of contributory liability, and the model of so-called vicarious liability.

The direct liability model consists of attributing direct responsibility to the subject who directly and physically engaged in the illicit conduct.

On the other hand, the contributory liability model attributes civil liability to a different subject who is not the material author of the wrongdoing but is in a particular relationship (such as a work or family relationship, etc.) with the author of the illicit act. This model is distinguished into two further sub-models, depending on whether the subject called upon to respond in addition to the main author of the wrongdoing contributes to the violation by virtue of having actual knowledge of the illegality and not having done anything to prevent it (actual knowledge), or by virtue of having a duty to know, by reason of their position or profession, of the third party's illegality (reasoned knowledge), and having engaged in inert conduct.

Finally, the model of so-called vicarious liability arises when a subject, having a duty to do so, fails to control the activity of the third party who directly commits the norm violation, or even benefits from the agent's activity. Hence, vicarious liability exists alongside the direct liability of the material author of the wrongdoing.

[25] BAISTROCCHI, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in 19(1) *S. Cl. H. Tech. L. J.*, 111-130, 114, (2003); COLANGELO, MAGGIOLINO, *ISPs' copyright liability in the EU digital single market strategy,* in 26(2) *Int. J. L. Inf. Tech.*, 142-159, 155, (2018);

By virtue of this tripartition, a significant jurisprudence developed on the topic of the liability of internet service providers in the decade prior to Directive 2000/31/EC.[26] This jurisprudence represented the basis on which two important legislative interventions in the United States were developed, one of which was occasioned by the ratification of international treaties on intellectual property. These are the laws respectively of 1996 and 1998.

In 1996, the Communication Decency Act was enacted and its Section 230 (C) (1) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information content provider". The precept is clear: the service provider cannot be equated, for the purposes of civil liability for transmitted information, with the content provider or publisher. Service providers are mere distributors of information, unless it is provided that they are aware of the transmitted illicit information.
Moreover, the CDA, in its section 230 (C) (2) protects interactive computer service providers or users from civil liability, whenever they implement voluntary screening or blocking measures to limit access to offensive content, lately proven to be imperfect.
Such fundamental clause (Good Samaritan clause), which represents the keystone of the entire dialogue on the role of online platforms,[27] specifically states that: "No provider or user of an interactive computer service shall be held liable on account of (a) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (b) any action taken to enable or make available to information content providers or others the technical means to restrict access" to such material.[28]
In brief, the online intermediaries who host or republish contents of various kinds are protected by the application of a series of rules which would otherwise make them responsible for what others, the users, have said or done in their virtual spaces.

---

[26] TOSI, *Le Resposnsabilità Civili,* in TOSI, (EDT.), *I Problemi Giuridici di Internet. Dall'E-Commerce all' e-business,* Giuffrè Francis Lefebvre, Milano, 2003, 301; *Cubby v. Compuserve,* 776 F. Supp. 135 (140 S.D. NY 1991); *Playboy Enterprise, Inc. v. Frena,* 839 F. Supp. 1552 (M.D. Flo. 1993); *Sega Entertainment, Ltd. V. Maphia,* 857 F. Supp. 679 (N.D. Cal. 1994); *Religious Technology Center v. Netcom On-Line Communication Services,* No. C-95-20091 RMW (N.D. Cal. 21 *november*1995);
[27] PAOLUCCI, *Il blocco dei social di Trump e la libertà di espressione online,* February 15, https://www.iusinitinere.it/il-blocco-dei-social-di-trump-e-la-liberta-di-espressione-online-35567;
KUCZERAWY, *The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?,* April 24, 2018, https://www.law.kuleuven.be/citip/blog/the-eu- commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/. ;
[28] Communication Decency Act, 47 U.S.C, §230 c (2);

US courts have utilized such a clause to provide broad protection to ISPs, in line with the intended purpose of the legislation.[29] This protection has been applied even in situations where the ISP was aware of illegal content being hosted on its platform, received notice from a third party about such content, or paid for the data. [30]

In 1998, the Digital Millennium Copyright Act (DMCA) was enacted to implement the two WIPO treaties of 1996. Included within the DMCA is Section 512 (Limitations on liability relating to material online), which came into force on November 17, 1998.
Section 512 contains several provisions that limit the liability of internet service providers. Although primarily concerned with copyright infringement, the principles contained therein may also be applied to analogous situations involving the violation of other exclusive rights over intangible assets beyond the realm of copyright law.

After the came into force of both the Communication Decency Act of 1986 and the DMCA of 1998, case law has correctly applied the new legislation.
In the Gucci case,[31] a provider was sued before the New York Court in order to have its responsibility declared due to fault, since although it had been repeatedly warned about hosting on its server the illicit activity of a user connected to the sale of counterfeit Gucci items, it had not disabled the indicated sites. In turn, the provider invoked the applicability of Article 230 of the Communications Decency Act, which provides that no provider or interactive system can be held liable, like a publisher, for informational content written by third parties. The Court held that it could not apply it because the same law excludes the applicability of the legislation to the discipline of intellectual property rights. On the contrary, it recognized the liability of the provider for negligent participation since, although it did not directly commit the offense, having knowledge of it, it did not prevent the continuation of the violation.
Thus, US case law, even when affirming liability, never justifies it with a general obligation of surveillance by the provider on the transmitted or stored information. On the contrary, in US case law, such an obligation is almost always denied.

[29] FRYDMAN, RORIVE, *Regulating Internet Content Through Intermediaries in Europe and the USA*, in 23(1) *Z. f. Recht.*, 41-60, 45, (2002);
[30] HOLZNAGEL, *Responsibility for Harmful and Illegal Content as Well as Free Speech on the Internet in the United States of America and Germany,* in ENGEL, KELLER (EDS), *Governance of Global Networks,* 45;
[31] *Gucci America, Inc. v. Hall Associates*, 135 F. Supp. 2d 409 (S.D.N.Y. 2001);

In conclusion, leaving aside the problem of combating anonymity, which in the United States clashes with the First Amendment of the Constitution, the fundamental principles of civil liability of the provider in the US legal system are substantiated in affirming that it is not legally possible to assert the existence of an extra-contractual civil liability without fault, subject to the obligation to use techniques and filters for the discovery of any illicit information.

### 3. The Directive 2000/31/EC (e-Commerce Directive) Discipline

Adopted in 2000, the e-Commerce Directive contains the fundamental tenets of the EU liability framework for the online intermediaries, and therefore of the Digital Services Act Regulation.
The directive's objective, as for the liability of intermediary services providers, is to address the contradictions in national legislations and court's judgements, which led ISPs operating in the EU to compete in a context of legal ambiguity and created the conditions for new barriers to block the growth of the internal market.[32] Just by establishing a unified legislative framework, in fact, it is possible to guarantee the free circulation of information society services among Member States, as well as to ensure both consumer trust in online commerce and the legal certainty.

With the directive 2000/31/ EC the European legislator embraced the liability of the information society services provider (ISSP) from a horizontal point of view, consequently adopting a unique regime for all the different types of legislations, which, differing from the US discipline, covers from copyright law to criminal law, up to civil law and so on.
Not only, in fact, the lawmaker sought to prohibit the unlawful treatment of information on the internet, but also intended to ensure a fair balance between the different fundamental rights of several stakeholders (e.g. freedom of expression, privacy, freedom to conduct business and property rights, included the intellectual property rights).

[32] VAN EECKE, TRUYENS, *EU study on the legal analysis of a single market for the information society: New rules for a new age?*, 2009, 29, https://op.europa.eu/it/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722;

Furthermore, the ECD has configured a typology of liability based on the negligence of the provider, which is subsidiary to the one of the offender.[33] That means that the fact that some illicit contents have circulated through the network, thanks to the intervention of a certain intermediary service provider, it does not imply that the latter should necessarily be held accountable for them. The directive in fact, excluding a general liability regime for online intermediaries,[34] establishes that, in presence of certain determined requirements and conditions set down by the law, the service provider may be exceptionally exempted from the ordinary national liability regime, creating a basic framework which harmonizes the threshold beyond which the ISP cannot be considered accountable for information provided by third parties (so called "safe harbor" regime).[35]

For this reason, the ISP is not contested for the material fact committed by the user, but for the failure to prevent or adopt repressive measures despite being aware of the illegal nature of those contents.

Therefore, the responsibility for the online illegal contents is not just upon the service provider but is shared among several stakeholders. [36]

It emerges, at this regard, a clear favor legis for the economic rights of ISPs, which are not forced to grant an unrealistic and far-fetched general monitoring on what happens on their platforms, as it has been suggested in past European case law, but are only called to restore legality and consumer protection online, once they have acquired the "actual knowledge" of an effective illegality present on their services.

In case a general monitoring would have been imposed, in fact, such a burden would have required them to *ex ante* filter all the contents uploaded therein, which everyday transport millions, if not even billions, of information uploaded by their users.

As a consequence, at the time of the ECD publication, such regime appeared to be responding adequately to the demands on liability for network offenses, under the penalty of a forced renunciation to the process of markets globalization.[37]

---

[33] ASTONE, *La responsabilità del prestatore di servizi della società di informazione nella direttiva 2000/31/CE*, in 2 *Eur. Dir. Priv.*, 2003, 431ss., *ivi* 436;

[34] Directive 2000/31/EC, art.15;

[35] PEGUERA, *Mensajes y mensajeros en internet: la responsabilidad civil de los proveedores de servicios intermediarios,* in *UOC*, 2001, 3, https://www.uoc.edu/web/esp/art/uoc/0103008/peguera.html;

[36] *TOSI, Responsabilità civile per fatto illecito degli Internet Service Provider tra tipizzazione normativa ed evoluzione tecnologica, in AA. VV., Digesto Discipline Privatistiche, 688 ss.;*

[37] MAIETTA, *Il sistema delle responsabilità nelle comunicazioni via internet,* in CASSANO, CIMINO (EDT.), *Diritto dell'Internet,* 511;

Such a discipline on the ISP's liability, however, does not advantage any intermediary providing internet services, but is rather addressed just to certain subjects providing specific types of online services. More precisely, the directive introduced a classification of the ISPs based on the activity which they perform, with the consequence that, depending on the type of service offered by a certain intermediary, its degree of involvement in the offense may be established with more accuracy and the conditions for benefitting from a safe harbor may be tightened with more proportionality.[38]
Unlike the US counterpart, the ECD does not typify the two categories of the search engines and hyperlink services and distinguishes the activities which may enjoy exemptions from liability just among a) mere conduit (activity of mere transport), b) caching (activity of temporary storage) and c) hosting (activity of information storage) services.[39]

Despite the safe harbors, providers of such services may be, in any case, required from a public authority, whether it is a judicial authority or an administrative authority, to terminate or to prevent a determined infringement realized on such platforms, by removing, for example, illegal information or disabling access to it.[40]
Within the limits of the general monitoring prohibition, the national legislation must provide the legal basis for these corrective or preventative actions, even though, in certain areas like intellectual property law, EU legislation is entitled to provide itself for such a legal justification across the EU.

Passing through the analysis of the specific safe harbors established by the directive, the first category of services benefitting from an exemption from liability under the e-Commerce Directive, namely the mere conduit services, is subjected to a particular regime, under which it might be provided with a total exclusion of accountability at the occurrence of certain determined circumstances. Art. 12 of the ECD establishes in fact, in paragraph 1, that "Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission".[41]

[38] GAMBINI, *Le Responsabilità Civili dell'Internet Service Provider,* 271;
[39] TERESZKIEWICZ, *Digital Platforms: Regulation and Liability in the EU Law*, in 6 *Eur. Rev. Priv. L.,* 903-920, 906, (2018);
[40] Directive 2000/31/EC, recital 45, 48, art. 12 (3), art.13 (2), art.14 (3);
[41] Directive 2000/31/EC, art.12 (1);

The same article, in paragraph 2, specifies that the provider is not responsible for the intermediate and transient storage of the information transmitted, on condition that such activity serves only for the transmission on the communication network and that its duration does not exceed the time reasonably necessary for this purpose. In this regard, both the neutrality and the non-interference of the provider in the traffic of information are stressed by the Directive.[42]
Finally, in paragraph 3, the article establishes that the judicial or administrative authority to which supervision is entrusted may demand, even as a matter of urgency, that the service provider puts an end to the illicit activity.[43]

As for the exemption from liability in the caching services, the ECD requires from the provider not only passive behavior, but also conformative. Indeed, the provider must not only abstain from making any change to the information, but also comply with the conditions of access to information and with the rules for updating the information, which have to be indicated in a way that is widely recognized and used by businesses in the industry, without even interfering with the lawful use of technology, that also has to be widely recognized and used in the industry to obtain data on the use of information.
Furthermore, in this type of activity the service provider will have to act promptly, in order to remove the information stored on its facilities or to disable access, as soon as it actually becomes aware of the fact that the information has been removed from the place on the network where they initially were, or that access to information has been disabled or that a court or authority administration has ordered its removal or disabling.[44]
Art. 13, paragraph 2, further specifies that the judicial authority, or the administrative authorities with supervisory functions, may require that the service provider, in carrying out the activities referred to in paragraph 1, prevents or puts an end to the violations committed. The service provider neither implements nor interferes with the content of the information but is solicited to intervene only if there is any concrete indication of its abusive use, and is required, if agreed in judgment, to demonstrate the promptness of its behavior, thereby compliant with the professional diligence.

[42] Directive 2000/31/EC, art.12 (2);
[43] Directive 2000/31/EC, art.12 (3);
[44] Directive 2000/31/EC, art.13;

Lastly, to providers who ensure their users a durable storage of the information put in their network, namely hosting services providers, it is required, based on the following art.14 ECD, a heavier standard of exemption, given the greater risk of danger associated with the much more relevant duration of permanence of information on the network.

Thus, the provider will not be criminally liable only if it "does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[45]

In brief, the exemptions from liability set forth in this article only apply in situations where the activity of a provider of information society services is limited to the technical process of operating and granting access to a communication network, over which information made available by third parties is transmitted or temporarily stored for the sole purpose of increasing the efficiency of the transmission. This activity is purely technical, automatic, and passive, which implies that the provider of information society services is not responsible for any damages that result from the transmission of the information, to the extent that it doesn't have any knowledge or control over the information.[46] A hosting service can consequently benefit from the exemptions provided for mere transport and temporary storage services only if it is not involved in any way in the transmission of the information.[47]

For this purpose, any modification of the transmitted information by the service provider is not permitted, excepted for manipulations of a technical nature carried out in course of transmission, provided that they do not alter the integrity of the information.

Furthermore, the service provider is totally denied from deliberately cooperating with a recipient of the service for the purpose of committing unlawful acts, in order to not respond directly for the committed action.[48]

However, as stated in paragraph 2 of the same art.14, such principles do not apply in the eventuality that the recipient of the service acts under the authority or the control of the service provider,[49] based on the occurrence of a form of vicarious liability.

In addition to this, paragraph 3 of art. 14 once again reaffirms the power of intervention of the judicial or administrative authority, which may also require, even urgently, that the service

[45] Directive 2000/31/EC, art.14 (1);
[46] Directive 2000/31/EC, recital 42;
[47] Directive 2000/31/EC, recital 43;
[48] Directive 2000/31/EC, recital 44;
[49] Directive 2000/31/EC, art.14 (2);

provider, in the exercise of the activities referred to in paragraph 1, prevents or puts an end to the violations committed.[50]

The assumption of the intermediary's liability, based on the actual knowledge of the existence of an illegal activity, undoubtedly refers to the concept of actual knowledge previously adopted in the United States by the DMCA.
In such a case, however, the transposition has not been properly carried out. If on the one hand, in fact, US legislation has provided for a precise and detailed notification procedure to identify cases of actual knowledge by the intermediary followed by inaction in removing the site, on the other hand nothing of this sort exists in the European legislation, where the provider's knowledge and the accompanying circumstances (so-called "detailed knowledge") are subject to interpretation, both exegetical and systematic, with results that have not always turned out to be certain.

Finally, with art. 15 the e-Commerce Directive closes the ISP's liability discipline, establishing the absence of a general monitoring obligation for the provider and stating that Member States should not require providers of the services covered by articles 12, 13 and 14 to generally monitor the information they transmit or store or to actively search for facts or circumstances that could suggest an illegal activity therein.[51]
Moreover, without prejudice to the provisions of articles 12, 13 and 14, the service provider is in any case required to inform, without delay, the judicial authority or the administrative one with supervisory functions, when being aware of any alleged illegal activity and to provide without delay, at the request of the competent authorities, the information in its possession that permits the identification of the recipient of its services with whom it has a data storage agreement, in order to detect and prevent illicit activities.[52]

### 4. Critical Issues and Case Law of the e-Commerce Directive

During the last twenty years, large variances have emerged in the way the e-Commerce Directive has been implemented throughout the EU, while several interpretations by national courts have spread between Member States in a very heterogeneous way.

[50] Directive 2000/31/EC, art.14 (3);
[51] Directive 2000/31/EC, art.15 (1);
[52] Directive 2000/31/EC, art.15 (2);

The European Union Court of Justice case law, in fact, has not provided, from this perspective, sufficient guidance, giving consequently rise to a highly fragmented jurisprudence across the whole European continent.[53]

In this regard, several gaps have been found within the ECD discipline, starting with the problem of which online services fall within the definition of information society services, which represents the *sine qua non* condition to benefit from one of the ECD exemptions.
At the time of the publication, in fact, it was still unclear whether the recently developed online services, such as the so called "social networks", were falling within the scope of the directive and were therefore immune from any responsibility or should have rather been subjected to the ordinary liability regime, which varies from country to country.

Secondly, the safe harbor's conditions, as well as the so called "notice-and-take down" obligations (obligation to remove illegal content upon their knowledge) turned out to lack clarity, to the extent that the key concepts serving as the basis for the liability exemptions, namely the distinction between "active" and "passive" roles and the definition of "illegal activities", were not adequately defined for the purposes of an effective discipline's application.

Lastly, since automatic filtering technologies have started to be employed more often to find illicit information, another problem left unsolved by the directive has also been the distinction between the forbidden "general" content monitoring and the permitted "particular" content monitoring.

### *4.1 The Definition of Information Society Services*

As for the first of the mentioned issues in the e-Commerce Directive, several problems have emerged with regard to the scope of application of the liability exemptions provided by the e-Commerce Directive. A clear identification of the exact recipients represents in fact the first step to follow in order to grant a homogeneous and shared discipline through the whole European Union.

[53] MADIEGA, *Reform of the EU Liability Regime for Online Intermediaries,* May 1, 2020, 1, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf;

First, even though the ECD states that the liability exemption applies to services "normally provided for remuneration", [54] the text of the Directive leaves unclear whether this includes also activities promoted by advertisements, totally free models such as Wikipedia, or "freemium models" (i.e. when users make free use of a service and only some of them pay some kind of remuneration).
In this regard, the CJEU established in 2013 that online news publishers may be held accountable for defamatory and unlawful materials posted on their website by third parties, regardless of whether the users paid for the content or not.[55]
Furthermore, confirming the orientation set by the European Court, also the Paris Court of Appeal, in a later decision of 2016, endorsed the position of the Wikimedia Foundation, a nonprofit charitable organization which provides services free of charge, in granting it the claimed hosting provider status, which, in accordance with the e-Commerce Directive, exempted it from liability for third parties' contents.[56]

In addition to this, although some countries inside and outside of Europe contain specific safe harbors for activities such as those of search engines and hyperlinks,[57] the ECD does not, and their liability regimes are subjected to very inconsistent national laws and case law.
Already within the recital 21 ECD, in fact, the lawmaker took note of this lack of regulation, looking forward for future interventions to fill such void, with the aim of clarifying better the role played by other online intermediaries, which were not yet sufficiently developed at the time of the e-Commerce Directive publication, and could have not therefore been explicitly included within the scope of the legislation.[58]

In the absence of such classification, the CJEU and national courts have mostly addressed activities such as search engine and hyperlink operations in the framework of the hosting safe harbor, even though in some Member States' national legislation, such services have been classified only as "mere conduits".[59] While, in fact, a German court viewed, for example,

[54] Directive 2000/31/EC, recital 17;
[55] CJEU, Case C 291/13, *Papasavvas,* §45, in *IP Curia.EU,* https://ipcuria.eu/about.php;
[56] Appeal Court of Paris, June 14, 2016, n. 15/20204; PAULSON, ROGERS, *Victory in France: Court rules in favor of the Wikimedia Foundation,* 20 June 2016, https://diff.wikimedia.org/2016/06/20/france-legal-victory/;
[57] Spain, Ley 34/2002, de 11 de julio, sobre servicios de la sociedad de la información y comercio electrónico (LSSICE); US, Digital Millennium Copyright Act (17 U.S.C., adopted 28 October 1998), sec. 512(d); Canada, Copyright Act (R.S.C., 1985 c. C-42), Secs. 2.4(1b), 31.1(1-2,4), and 41.27(1);
[58] Directive 2000/31/EC, recital 21;
[59] HOBOKEN, *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines*, in 27 *Inf. L. Ser.*, (2012);

hyperlinking as a type of hosting service falling under art. 14 ECD, and, similarly, Spain and Portugal considered both search engines and hyperlink operations as particular types of hosting services, a UK court saw it instead as only a mere conduit activity, in accordance with art. 12 ECD.

In addition to this, since their recent appearance, the liability exemptions for blockchain players have also been put up for debate, whereas the cloud computing service providers (including Google Drive, Apple iCloud, and Dropbox) have strongly been criticized for being occasionally regarded as hosting providers.[60]

Nevertheless, among the services providers which have been discussed most in the recent case law of the European Union, academic studies have revealed strong uncertainties concerning the application of the e-Commerce Directive, especially with regards to the so-called "social media companies" and the "collaborative companies".[61]

In some recent decisions, in fact, the CJEU has ruled in very different ways on whether services offered by subjects like Google or Airbnb may be qualified as "information society services". If on the one hand, for example, the CJEU established in its 2017 *Uber* case that Uber should have just been classified as a "service in the field of transport" rather than an "information society service" benefitting from liability exemptions,[62] on the other hand the Court held in its *Airbnb Ireland* case that the company's services (matching up, via online platform, potential guests with hosts) actually fitted the definition of "information society service".[63] In accordance with the Court's ruling, in fact, the designation of a service as an "information society service" depends on the level of control the platform had over the provided service, in the meaning that the less control there is over the process, the more the service is likely to be designated as an information society service.

---

[60] WEBER, STAIGER, *Cloud Computing: A cluster of complex liability issues,* in 20(1) *Eur. J. Cur. Leg. Is.*, 2014;
[61] Directorate-General for Internal Policies, *Providers Liability: from the e-Commerce Directive to the Future,* 2017, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf; UK Committee on Standards in Public Life, *Intimidation in Public,* December 13 2017, https://www.gov.uk/government/publications/intimidation-in-public-life-a-review-by-the-committee-on-standards-in-public-life; ANDREWS, *We Need European Regulations for Facebook and Google,* in *London School of Economics blog*, December 13, 2016, https://blogs.lse.ac.uk/medialse/2016/12/13/we-need-european-regulation-of-facebook-and-google/;
[62] CJEU, Case C-434/15, *Associaciòn Profesional Elite Taxi v Uber Systems Spain SL,* par. 33- 40, in *InfoCuria Giurisprudenza,* https://curia.europa.eu/juris/liste.jsf?num=C-434/15; CJEU, Case C-320/16, *Uber France*, para. 48, in *InfoCuria Giurisprudenza,* https://curia.europa.eu/juris/liste.jsf?num=C-320/16;
[63] CJEU, Case C-390/18, *Airbnb Ireland,* https://curia.europa.eu/jcms/jcms/p1_2695382/en/;

Despite such clarifications from the CJEU, however, the e-Commerce Directive still leaves the problem of the incomplete harmonization, to the extent that definition of which subjects might be included within the scope of its provisions is still left to the freedom of singular Member States, which independently decide how to legislate in this regard.[64]
Furthermore, due to its complexity and case-specificity, national courts might interpret the CJEU jurisprudence in various and different ways, which could ultimately lead to a legal fragmentation on the interpretations given within the EU.

### *4.2 The Distinction between "Passive" and "Active" Intermediaries*

Proceeding through the analysis of the main critical issues which affect the proper and effective functioning of the e-Commerce Directive, considerable attention has to be reserved to the problematic distinction between passive and active services providers, which has emerged in the European and national case law of the last two decades, due to the importance that such distinction has acquired in the definition of the liability regime's scope.
The classification of an intermediary service provider as "passive" or "neutral" on the one hand, and as "active" on the other, determines in fact whether that provider may effectively take advantage of a safe harbor for its actions or should rather be subjected to the ordinary liability regime.

In the triple conflict of interest considered by the legislator (right of expression, right to conduct a business of the provider, right to honor/ IP right/ right of publicity of anyone who can be harmed by the online activity of others[65]), the liability exemption for this industry is considered to take on meaning only when the providers do not influence the contents published on their platforms and only provide a mere technical service.[66]
Such clarification is often used, especially in theme of copyright infringements, with the intention to exclude the safe harbor from those hosting providers which carry out activities considered to exceed an automatic and passive role, particularly when indexing, organizing

[64] VAN HOBOKEN ET AL., *Hosting intermediary services and illegal content online*, 30-31, 2019, https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en; HOFFMANN, GASPAROTTI, *Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act",* CEP study, March 2020, https://www.readkong.com/page/liability-for-illegal-content-online-weaknesses-of-the-eu-8865627;
[65] CARR., *Social Media and the Internet Drive the Need for a Federal Statute to Protect the Commercial Value of Identity*, in 22 *Tul. J. Tech. Int. Prop.*, 31, (2020);
[66] Directive 2000/31/EC, recital 42;

and promoting the materials uploaded by their users, by offering them to other users of their services,[67] with the purpose of making profit.[68]

However, reading carefully the recital 42 of the e-Commerce Directive, the plausibility of such reasoning appears considerably uncertain.
As already previously explained, the recital establishes that, in order for an ISS activity to obtain advantage from one of the safe harbors provided by the directive, that activity must: a) "cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient", b) be of "a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored."[69]

From the language used in the first condition, it emerges clearly enough that, in the intentions of the lawmaker, the provision was not meant to address providers falling under the hosting safe harbor, but rather just to consider the mere conduit and caching services, which are explicitly mentioned in the following recital 43, as also confirmed by Advocate General Jääskinen in his opinion in the *l'Oreal* case.[70]
Not only, in fact, the kind of activity depicted in such condition seems to be hardly referable to the long-lasting storage activity, which is typical of the hosting services providers, but also the first period of recital 42 ECD expressly states that is "only" in such cases that an ISS provider might benefit from one of the Directive's safe harbors, thus making the hosting services providers literally excluded from its scope of application, while including therein just the mere conduit and caching services.[71]

---

[67] Italian Supreme Court of Cassation, Sez. I, 19 March 2019, n. 7708, case RTI v. Yahoo, § 4, in *Corr. giur.*, 2020,177 ss. ;
[68] KOTLER, HOLLENSEN, OPRENSIK, *Social media marketing. Marketer nella rivoluzione digitale*, Hoepli, Milano, 2019, 85-87;
[69] Directive 2000/31/EC, recital 42;
[70] Opinion Jääskinen, Case C-324/09, L'Oréal paras 138-141, maxime 141, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62009CC0324;
[71] Appeal Court of Milan, January 07, 2015, n. 29, *Yahoo v. RTI*, RG 3821/2011, § 27, in *Diritto d'autore.it,* https://banchedati.dirittodautore.it/giurisprudenza/corte-di-appello-di-milano-sentenza-7-gennaio-2015-n-29; Opinion Jääskinen, Case C-324/09, *L'Oréal*, § 141-142, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62009CC0324; BUGIOLACCHI *L., Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti dell'attuale approccio case by case, (Commento a Trib. Milano 25 Maggio 2013 ord.)*, in 78(6) *Resp. civ. prev.*, 2013, 1997, *ivi* 2007; COLARUOTOLO, *Facebook e hyperlinking illecito degli utenti. L'inerzia ingiustificata del prestatore di servizi è fonte di responsabilità*

However, in addition to the "mere conduit" and "caching" services, the section 4 of the ECD's second chapter, namely the section on the "liability of intermediary services providers", textually envisages the figure of the "hosting provider" as well, giving almost the idea that such a category was added only at a later stage, without updating the text of the recital 42,[72] considering also that, in an original draft, such providers were not included within the text of the Directive.

Starting from the assumption, so, that the literal reading of the recital 42 ECD does not refer to the hosting providers, it is therefore necessary to better understand the scope of such provision.
While it may be possible to adopt a more expansive interpretation of recital 42 to include also hosting providers, on the other hand it is even possible that hosting providers may be subject solely to the conditions outlined in art. 14 of the ECD. In such case, if a hosting provider meets all the requirements of art. 14, it would be exempt from liability without having to satisfy any additional rules or requirements that are comparable to those specified in recital 42.[73]
However, in case we would like to share the first interpretation, a more in-depth evaluation would be required.

The activity of a hosting service, in theory, might even just be restricted to nothing more than hosting contents from third parties or providing results for queries made using search engines. In this case, however, the payment of a fee for the service would become necessary, taking into consideration the lack of an alternative source of income.

In practice, however, the solution that has actually been enforced has ultimately been to offer such services apparently free of charge to the general public (for this reason called siren servers)[74] and to reserve instead a compensation request only to those benefitting from

*civile e risarcitoria, nota a Trib. Roma 15.02.2019, RTI v. Facebook-Ponzone,* in *Riv. dir. ind*., 2019, 328; BRIDY, *The Price of Closing the "Value Gap": How the Music Industry Hacked EU Copyright Reform*, in 22(2) *Vand. j. ent. & tech. l.*, 323-358, 337, (2020); RIORDAN, *The Liability of Internet Intermediaries*, 402;
[72] PETRUSO, *La responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a confronto*, Giappichelli, Torino, 2019, 140;
[73] CJEU, *L'Oreal v. eBay*, C-324/09, § 141-142; Appeal Court of Milan, January 7, 2015, *Yahoo v. RTI*, § 26-27;
[74] POSNER, WEY., *Radical markets,* 220;

additional services, such as the advertisers: "Google subsidize users by providing a large portfolio of free services (search, email, ...) and resell their attention to advertisers with a payment per result (pay-per-click)".[75]
Such modus operandi has been observed to be the result of a change in the business model, whereas, if initially Google intended to offer paid services without advertising, and consequently actually chose the opposite solution.[76]

This allows the so called "profiling" activity, which is "a partially automated processing technique of personal and/or non-personal data, aimed at creating predictive knowledge by discovering correlations among data and by building profiles, which can then be used to assume decisions."[77]
Such data might be collected in any way, both on their own and by acquiring them from third parties,[78] to the point that some authors have written about "data colonialism" in this regard, making a parallel with the colonial exploitation of the resources of non-European countries.[79]

Taking into account such a socio-economic context, the answer to the question of whether the figure of hosting providers, as regulated by art.14 ECD, should equally fall under the scope of recital 42 ECD, therefore becomes pretty much more difficult, considering also that, in the second period of the same recital, it is clearly stated that, in order to get advantaged by the safe harbors set by the Directive, the ISS providers must provide services of "a mere technical, automatic and passive nature".

Precisely in this regard, the CJEU created a conceptual distinction between the "passive" and "active" roles of online intermediaries, reserving it a particular attention specifically in the context of the *Google France* and *l'Oreal* cases.[80]

---

[75] SAVIOZZI, *Imprenditorialità*, Egea-Pixel, 2017, 77; PERLINGIERI, *Profili civilistici dei social networks*, Edizioni scientifiche italiane, Napoli, 2014, 88; RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in 3 *Riv. dir. civ*., 2020, 652-653, *ivi* 642; SCHNEIDER, <<*Verificabilità*>> *del trattamento automatizzato dei dati personali e tutela del segreto commerciale nel quadro europeo,* in 2 *Merc. concorr. regole,* 2019, 327-356; ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete,* in *Riv. Trim. Dir. Proc. Civ.*, 2018, 411-440, *ivi* 416;
[76] POSNER, WEY, *Radical Markets*, 224;
[77] BOSCO, CREEMERS, ET AL., *Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities*, in GUTWIRTH, LEENES, DE HERT (EDT.), *Reforming European Data*, 8;
[78] PASQUALE, *The black box society,*30-34;
[79] COULDRY, MEJIAS., *The Costs Of Connection*, 67;
[80] CJEU, *Google France*, case C-236/08, in 124(2) *Harv. L. Rev.* 648, (2010); CJEU, *L'Oréal*, case C-324/09;

In the first case, namely in *Google France v. Vuitton and others*, the problem of defining the active or passive role of the provider arose in particular with reference to the AdWords "positioning" advertising service offered by Google, in which, on the basis of the amount paid, the advertiser places himself at the top or at the bottom of the search results.
In its final decision, the CJEU embraced the interpretation according to which the hosting providers should operate in a merely technical, passive and automatic way (so called neutrality condition), in order to comply with the provision set in the second period of recital 42.[81]
Here the Court limited itself to say just that, in order to assess the ISP's liability, it is relevant not the positioning service itself, but "the role played by Google in drafting the commercial message that accompanies the advertising link or in determining or selecting these keywords",[82] whereas the condition of passivity is met only when "[an] operator has not played an active role allowing it to have knowledge or control of the data stored".[83] It will be then up to national courts to assess the influence of such activities for the qualification of such platform as active or passive providers.
To this extent, the Court found Google liable for the activities carried out in the concrete case and ruled out that the role played by the company had ultimately been active.[84]

More significant is the dictum in the case of *L'Oréal and others v. eBay and others* where the Court, even recognizing the exemption from liability under art.14 ECD in the cases in which "the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers", [85] yet retained that optimizing the presentation of offers for sale and their promotions, as in that particular case, made the provider of such services lose its passive role and prevented the safe harbor from being invoked.

In addition to the above-mentioned cases, also in the 2014, with the case Papasavvas v. Fileleftheros,[86] the Court of Justice remained in line with its previous jurisprudence on the liability of the ISP, in cases of infringement of intellectual property rights, whereas in the

[81] CJEU, *Google France and Google v Louis Vuitton*, Cases C-236/08 to C-238/08, §114, 120;
[82] CJEU, *Google France and Google v Louis Vuitton*, Cases C-236/08 to C-238/08, §118-119;
[83] CJEU, *Google France and Google v Louis Vuitton*, Cases C-236/08 to C-238/08, §114, 120;
[84] CJEU, *Google France and Google v Louis Vuitton*, Cases C-236/08 to C-238/08, §120;
[85] CJEU, *l'Oreàl,* case C-324/09, §115-116;
[86] CJEU, *Papasavvas*, case C-291/13;

specific case, the issue concerned the civil liability of a content provider (a newspaper publisher) for defamation.
In this case, however, the defamation did not derive from user-generated contents, but from journalistic articles written by professional journalists and published in the newspaper.
The Court, recalling its previous case law, reiterated that the exemptions from liability provided by Directive 2000/31/EC only concern cases in which the activity of an information society service provider is purely technical, automatic and passive, and that, in order to benefit from those exemptions, the provider cannot know or control the information transmitted or stored on its platform.
Accordingly, it is not important that access to the online newspaper website is free or paid, nor the fact that the publisher is paid with the proceeds of commercial advertising, whereas the only thing that really matters is just to ascertain whether in the concrete case the service provider has been aware or not of the information published and has exercised control over it.

Despite the fact that the peculiar concept of "active hosting" cannot be found in any regulatory source, being just attributable to a recent consolidated practice of CJEU's case law, this notion has finally become an achievement acquired in the context of the whole European Union.
For this reason, during the last years, the passivity criterion has become one of the most controversial issue across several European jurisdictions, leading to diverging outcomes at a national level and consequently allowing national courts to easily side-step the ECD.
Even, in fact, some large-scale online media sharing platforms, like YouTube or Vimeo, having been qualified for years as hosting providers by national courts,[87] due to the passive/neutral nature of their activities, yet such qualification has been frequently contested over the time, on the ground that they detain enough knowledge of or control over the information they store to determine the legality of those contents.
Moreover, a growing body of case law before the European Court of Human Rights further indicates that many national courts have likely misapplied the ECD in a variety of ways.[88]

[87] France: Tribunal de grande instance de Paris, TF1 et autres v. YouTube, 29 May 2012, in *Med. L.,* (2012); Germany: OLG Hamburg, 5 U 87/12, 1 July 2015; OLG München, 29 U 3496/11, 17 November 2011; Spain: Court of Madrid, case 289/2010, 20 September 2010, Telecinco v. Youtube; partially confirmed by AP Madrid (sec.28) January 14, 2014 Westlaw.ES JUR\2014\36900;
[88] ECHR, Delfi AS v. Estonia [GC] (App no 64569/09), 16 June 2015; Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v. Hungary (App no 22947/13) 02 February 2016;

In particular in Italy, the distinctive criterion between passive and active hosting providers, more generally ISPs, has given rise to a heated jurisprudential debate,[89] which has recently culminated in the fundamental sentence of the Supreme Court of Cassation 7708/2019, already set down as a leading case in the field of ISP's liability.

Until that moment, never before had the highest Italian Court expressed itself with a final decision on such debate.[90] For at least a decade, in fact, lower courts have been divided in different lines of thinking as to the relevance to attribute to the distinction between active and passive internet services providers.

If on the one hand the Court of Rome has repeatedly denied the safe harbor protection to all the hosting providers making profit from the contents uploaded on their services, regardless of whether they were published by third parties or not,[91] on the other the Milan Court of Appeals and the Court of Turin[92] have focused their attention on the particular activity carried on by the hosting provider, which would become "active" only if it conducted any operation on the specific hosted content, since, in this way, it could not then be judged unaware, therefore eliminating de facto any distinction between active and passive providers.

---

[89] Court of Catania, case 2286/2004, in *Dir. Inf.,* 2004, 466; Italian Supreme Court of Cassation, case 49437/2009, *The Pirate Bay,* in *Altalex,* February 11, 2010; Court of Rome, judge Marvasi's order, *RTI (Reti televisive italiane) v. YouTube Llc and others*, December 16, 2009, in 133(4), *Foro it.*, 2010, 1348-1353, 1348; Court of Milan, case 1972/2010, Google v. Vividown, in *Riv. Dir. Ind.*, 2010, 347; Court of Milan, case 7680/2011, *RTI v. Italia On Line (IOL)*, in *Dir. Inf.* , 2011, 660; Court of Milan, case 10893/2011, *RTI v. Yahoo! Italy*, in *Riv. Ind.,* 2012, 364; Court of Rome's order, March 20, 2011, *PFA Films S.r.l. v. Yahoo!,* in *Riv. Ind.,* 2012, with note of TOSI, *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca a margine dei recenti casi "Google Suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale,* in *Riv. Ind.,* 2012, 44; Court of Appeals of Milan, case 8611/12, *Google v. Vividown*, in *Dir. Pen. Cont.,* 2013, https://archiviodpc.dirittopenaleuomo.org/d/2115-la-corte-d-appello-assolve-i-manager-di-google-anche-dall-accusa-di-illecito-trattamento-dei-dati-p; Italian Supreme Court of Cassation, case 5107/13, *Google v. Vividown*, in *Dir. Pen. Cont.,* 2014, https://archiviodpc.dirittopenaleuomo.org/d/2817-la-sentenza-della-cassazione-sul-caso-google; Court of Appeals of Milan, case 29/2015, RTI v. Yahoo! Italy; Court of Rome, case 8437/2016, *RTI v. Break Media,* in *Aida*, 2018; Court of Rome, case 9026/2016, *Kit Digital France-Kewego*; Court of Rome, case 14279/2016, *Megavideo*; Court of Appeals of Rome, case 2883/2017, *RTI v. Break Media*; Court of Turin, case 1928/2017, *Delta Tv v. YouTube,* in *Med. L.,* https://www.medialaws.eu/il-tribunale-di-torino-interviene-sulla-responsabilita-degli-internet-service-provider/; Court of Turin, case 342/2018, *Delta Tv v. Dailymotion*; Italian Supreme Court of Cassation, case 7708/2019, *RTI v. Yahoo! Italy*; Court of Rome, case 18727/2019, *RTI v. Bit Kitchen*; Court of Rome, case 693/2019, *RTI v. Vimeo LLC*; Court of Rome, case 14757/2019, *RTI v. Dailymotion SA;*

[90] APA, FRIGERIO, MONTINARI, *The Court of Cassation rules on the active and passive hosting providers debate in the RTI v. Yahoo! Case,* in *Portolano Cavallo inform@,* 5 April 2019, https://portolano.it/en/newsletter/litigation-arbitration/the-court-of-cassation-rules-on-the-active-and-passive-hosting-providers-debate-in-the-rti-v-yahoo-case;

[91] Court of Rome, case 8437/2016, RTI v. Break Media; Court of Appeals of Rome, case 2883/2017, RTI v. Break Media; Court of Rome, case 9026/2016, Kit Digital France-Kewego; Court of Rome, case 14279/2016, Megavideo; Court of Rome, case 693/2019, RTI v. Vimeo LLC;

[92] Court of Turin, case 1928/2017, Delta Tv v. YouTube; Court of Appeals of Milan, case 29/2015, RTI v. Yahoo! Italy; ; Court of Turin, case 342/2018, Delta Tv v. Dailymotion;

Before reaching the Supreme Court of Cassation, the specific case arose already in 2009 with RTI (*Reti Televisive Italiane)* filing a lawsuit against *Yahoo! Italy S.r.l.* and *Yahoo! Inc.* (collectively, "Yahoo!"), as operators of the *Yahoo! Video* service established in Italy, asking the Court of Milan to find Yahoo! liable for copyright infringement, having it hosted several of RTI's videos uploaded by its users, without any authorization.

Despite the fact that the judge in the first instance originally accepted RTI's claims, holding Yahoo! accountable for copyright infringement,[93] in 2015 the decision was overturned with the Judgment n. 29/2015 of the Milan Court of Appeal, declaring that Yahoo! was just an intermediary and, as such, could consequently benefit from the safe harbor protection. Accordingly, the Court of Appeal specifically rejected any distinction between active and passive hosting providers, finding that it was meaningless under EU law.[94]

In reaching such a conclusion, the Court stated that "copyright protection must be granted in such a way as to guarantee a fair balance between other fundamental rights possibly in contrast, such as the freedom of enterprise and the freedom of information and expression of Internet users, protected and guaranteed by articles 16 and 11 of the EU Charter of Fundamental Rights".

Therefore, the provider is considered "advanced", by the judging Court, to the extent that it is "the most suitable subject to put an end to such violations", and not on the basis of a concept, rooted until then, that the provider represents a participant in the offense together with the subject who publishes potentially contra legem contents.

As already mentioned, the Court of Cassation overturned the judgment on ISP liability and returned the case to the Milan Court of Appeals for further considerations on whether the URL of the content is necessary within the ex parte communication, in order to properly put the provider "on notice".[95]

In light of the CJEU's prevailing interpretation and recent legislative changes at the EU level, in particular the new directive on copyrights,[96] the Court of Cassation acknowledged a well-established distinction between active and passive hosting providers, ruling that an active

[93] Court of Milan, case 10893/2011, RTI v. Yahoo! Italy;
[94] Court of Appeals of Milan, case 29/2015, RTI v. Yahoo! Italy; BUGIOLACCHI, *Ascesa e declino della figura del "provider attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in 4 *Resp. Civ. Prev.*, 2015, 1261-1270;
[95] Italian Supreme Court of Cassation, case 7708/2019, *RTI v. Yahoo! Italy*;
[96] Directive (EU) 2019/790, *92–125;*

hosting provider is a provider who offers information society services beyond simple technical, automated, and passive services, engaging actively and helping thereby others to carry out illegal activities.
As a result, standing with the Court's reading, the active hosting provider is not qualified to benefit from the safe harbor liability regime outlined in article 16 of the Decree (art.14 of the e-Commerce Directive), and its accountability must therefore be determined in accordance with the general liability regime.
To this extent, the Court listed a few indicators, not all of which must be present, that point to the hosting provider having an active role, if made as part of a service management strategy that is business oriented. Such indicators are in particular: a) filtering, b) selection, c) indexing, d) organization, e) cataloging, f) aggregation, g) evaluation, h) use, i) modification, l) extraction, m) promotion of content. User profiling methods may also be relevant in this regard, when used to build user loyalty, with the aim of completing and enhancing, in a non-passive way, the fruition of material by indeterminate users.

By virtue of what has been established, the applicable legal regime seems to be of particular interest, considering that it depends on whether an ISP may be considered active or passive and given that the Court, in the event of an offense committed by an active provider, refers to the category of the omission offense in the specific form of unlawful commission.
In its interpretation, the Supreme Court suggested that lower courts' judges, when determining an active hosting provider's liability, should enforce the theory of tort law, in order to comply with the ordinary liability regime. The Italian Civil Code's article 2043, in fact, defines an illicit conduct as any act or omission resulting in a harm to another party.
If all the legal conditions are satisfied in such a situation, the active hosting provider may be held accountable for its involvement in the third party's illegal activity.
The provider of the active hosting, in turn, is not necessarily responsible for the content hosted. The court must establish in fact whether or not the general elements required by tort law were actually met, and whether the "active" hosting provider knew or not about the illegal content.

Given that the Court of Cassation's statements do not bind lower courts to follow its rulings, it is likely that the juridical dispute will continue to go on.

In the view of some authors,[97] the position shared by the majority doctrine of several national courts, like the Italian ones, and the European Jurisdiction, like in the *Google France* and in the *L'Oreal* cases, appears to be unmotivated in the method, given that the optimizing activity does not constitute knowledge or control of the contents, and is non-shareable in the outcome. The reading given by the European Court, in fact, has not taken into account that, having any hosting intermediary a minimal degree of control over the data stored in its system, even just owning the hosting infrastructure or being subjected to its terms of service may give it the power to exercise control, which would ultimately exclude it from the safe harbor's scope established in art. 14 ECD.

Moreover, even admitting that the provider indexes and proposes the files uploaded by users, it does so in a massive and automatic way, based on the one hand on the types of content present in such files, which are detected by metadata and not by fact checking,[98] and on the other on the preferences detected by data tracking, which consists of an analysis made by ideal types, i.e. by segmenting and categorizing users present on the platform.[99]

In other words, operating a matching between the preferences of the users and the commercial offers from the advertisers, namely the two sides of the market, it is true that such data processing can be said to do so on the basis of contents, which also conserve traces left by users within them, but such elements precisely consist in mere traces of personal data combined with keywords, abstracts or other synthetic parameters, that are pre-set for each product/file viewed.[100]

Not far from this position is that of those who argue that the ratio of the passivity requirement lies in drawing a dividing line between one's own materials, or one's own "adopted content" as for editorial responsibility, and third-party information, instead of restricting the safe harbor.[101]

---

[97] ALBERTINI, *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, in 4 *L. Med. Work. Pap. Ser.*, 62, (2020); KUCZERAWY, *Active vs. passive hosting in the EU intermediary liability regime: time for a change ?*, in *KU Leven CiTiP Center for IT & IP law*, 07 August 2018, https://www.law.kuleuven.be/citip/blog/active-vs-passive-hosting-in-the-eu-intermediary-liability-regime-time-for-a-change/;

[98] BORGOMANERI, SIGNORELLI, *Il recepimento della direttiva Copyright in Italia: ora è tempo di responsabilizzare,* in *Agenda Digitale,* 03 August 2021, https://www.agendadigitale.eu/cultura-digitale/il-recepimento-della-direttiva-copyright-in-italia/;

[99] DELMASTRO, NICITA, *Big data. Come stanno cambiando il nostro mondo,* Bologna, Mulino, 2019, 37;

[100] RIORDAN, *The liability of internet intermediaries,* 401;

[101] HUSOVEC, *Injunctions aganist intermediaries,* 55-57;

In offering such services, the ISP does not distinguish between files with lawful content and files with illegal content,[102] especially where the judgment depends on the particular context.[103] For this reason, on the contrary of what often declared by national and European judges, these activities should therefore be considered eligible to fall within the concept of safe harbor, as it emerges from the text of recital 42.

A final clarification from the Court of Justice, in this regard, is not only expected, but it cannot be deferred any longer, considering the divergent opinions spreading in the jurisprudence and the need to defend both the positions of the ISP and of the user.

### *4.3 The "Good Samaritan" Paradox*

Related to the problematic distinction between "active" providers and "passive" providers is also the further issue of whether the e-Commerce Directive disincentives in practice online intermediaries from proactively monitoring the lawfulness of their hosted contents, due to the risk of losing the benefit of liability exemptions, in case they would do so.[104]
If on the one hand, a platform that enforces ex ante moderating practices may be deemed to be playing an active role and consequently be excluded from the liability exemption, on the other, relatedly, the deployment of voluntary monitoring and content-filtering procedures, as well as the possibility of "specific" monitoring obligations, is permitted under art. 15 ECD. This is also known as the "Good Samaritan" paradox.

This juridical risk has been presented in particular by the online intermediaries which have taken part in the public consultations carried out by the European Commission on the ECD.[105] However, according to the European Commission's communication from September 2017 on countering the online illegal content, voluntary proactive measures "do not in and of

[102] GEDDES, *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, in 43(4) *Col. Journ. L. A.*, 469, 476, (2020);
[103] BLOCH-WEHBA, *Automation in Moderation*, in 53 *Corn. Int. L. Journ.* 41-96*,* 55, (2020);
[104] NORDEMANN, *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, 2018,10,https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf; ANGELOPOULOS, *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market*, in *SSRN,* 1-47, 29, (2017);
[105] European Commission, *Commission Staff Working Document - Online services, including e-Commerce, in the Single Market*, SEC(2011) 1641 final, 35; European Commission (2016), *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe*, COM(2016) 288, 9; European Commission, *Commission Staff Working Document on the Mid-Term Review on the implementation of the Digital Single Market Strategy*, SWD(2017) 155 final, 28;

themselves lead to a loss of the liability exemption, in particular, the taking of such measures need not imply that the online platform concerned plays an active role which would no longer allow it to benefit from that exemption".[106]

The key reason in favor of this standpoint is that, even if such actions lead to knowledge or awareness of any illegality, the hosting platform still has "the possibility to act expeditiously to remove or to disable access to the information in question upon obtaining such knowledge or awareness."[107] Accordingly, if it will do so, the hosting provider will not lose the protection of the safe harbor.

This position has also been confirmed by specific case law.

For instance, in Germany, the platform has not been recognized as having an active role, despite YouTube's usage of Content ID, which is a model "Good Samaritan" filtering system.[108]

Similarly, in a Spanish case, the national court came to the conclusion that YouTube's editorial tasks or activities did not imply that it actually had active knowledge of the illegal contents uploaded by its users or a proactive control over the same.[109]

Likewise, Good Samaritan clause examples may be found also in codes of conduct, such as the UK's *IPO Code of Practice on Search and Copyright*,[110] or France's *Charter for the Fight against the Sale of Counterfeit Goods on the Internet*.[111]

However, the more a platform searches for an illicit content, the more likely that platform is going to discover it. Therefore, due to the acquired active role, the provider will no longer enjoy the safe harbor protection and the probabilities that it might be found accountable for having not acted promptly to remove the illegal contents are likely going to increase.[112]

---

[106] European Commission, *Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms*, COM (2017) 555, 13;

[107] European Commission, *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*, COM(2017) 555 final, Brussels, 28 September 2017;

[108] NORDEMANN, *Liability of Online Service Providers*, 10-11, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf; OLG Hamburg, July 1 2015, case 5 U 87/12, §198;

[109] AP Madrid (sec.28), January 14, 2014, Telecinco v. Youtube, Westlaw.ES JUR\2014\36900;

[110] IPO Code of of Practice on Search and Copyright (UK), Art. 22, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609478/code-of-practice-on-search-and-copyright.pdf;

[111] French Charter for the Fight against the Sale of Counterfeit Goods on the Internet, Par. 6 Preamble and Art. 3;

[112] KUCZERAWY, *The EU Commission on voluntary monitoring;*

If indeed a concrete disincentive were demonstrated in practice, such a situation would obviously be very counterproductive, especially considering that the ECD essentially seeks to encourage providers to take more preventive measures to fight the spread of illegal content online.
As a consequence, within the EU, there has been disagreement among academics, as to whether the ECD legal framework should have been amended, in order to provide an explicit recognition to a Good Samaritan clause.
For instance, such a protection is found in Section 230(c)(2) of the US Communications Decency Act,[113] which shields platforms searching for illegal content online from liability, when they act, in the limits of their possibilities, to moderate the contents present therein, even if they fail in doing so and therefore do not take any action in response to such content.[114]

In absence of a CJEU's ruling or of a clarification of the legal system, uncertainties in this regard still persist within the context of the e-Commerce Directive.

### *4.4 The Hard Distinction Between Duty of Care and General Monitoring*

According to art. 15 of the e-Commerce Directive, Member States are not permitted to impose on internet services providers a general obligation to monitor the information passing through or saved on their systems.
Such prohibition, however, only applies on a monitoring request of a general type, whereas it doesn't affect the possibility of Member States to require duties of care and monitoring obligations in specific cases, as specified in recital 48 of the e-Commerce Directive.
In accordance with national law, in fact, in order to stop specific violations (e.g. to enable plaintiffs to enforce their copyright),[115] national courts may issue injunctions against online intermediaries, which could also require them to accomplish a certain level of supervision.

However, as the directive does not define whether such obligations involve identifying and preventing illicit acts, the distinction between duties of care and general monitoring still

[113] USA, Communications Decency Act, 47 U.S.C., §230(c)(2);
[114] KUCZERAWY, *The EU Commission on voluntary monitoring*;
[115] VAN EECKE, TRUYENS, *EU study on the legal analysis,* 34;

remains unclear, making it difficult to differentiate a "general" monitoring from "specific" monitoring obligations.[116]

Furthermore, due to the widespread use of automatic filtering systems on major online platforms, even less legal certainty may be granted with regards to the monitoring of online contents.

If on the one hand, such measures have been put in place on the basis of Recital 40 of the e-Commerce Directive, which says that the liability rules established within the Directive do not limit the development and the use of technical systems of protection and identification, as well as of technical surveillance instruments, on the other hand it has been debated whether requiring ISPs to take such proactive steps may lead to a general monitoring activity, in which case such requests by national courts would become against the Directive itself.

Such considerations acquire even more relevance taking into consideration that these measures may even come with serious disadvantages for both the provider and the users, such as a lack of transparency as for how these technologies operate, a lack of proper safeguards, and the possibility of an over-enforcement, with online providers risking to become more likely to use an algorithm which removes far too much content rather than too little.[117] Opponents of such systems have emphasized that human review remains in any case necessary, in order to prevent discrimination and basic rights breaches, since filtering algorithms frequently make mistakes (i.e. false positives) being unable to comprehend the context, the political activism, or the humor of a specific situation.[118]

In the cases *Scarlet v. SABAM* of 2011[119] and *SABAM v. Netlog* of 2012,[120] the CJEU has better clarified such concepts, analyzing in particular the question of the admissibility of

[116] KUCZERAWY, *To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive*, in *KU Leuven CiTiP*, 2019, https://www.law.kuleuven.be/citip/blog/to-monitor-or-not-to-monitor-the-uncertain-future-of-article-15-of-the-e-commerce-directive/; ANGELOPOULOS, *CJEU in UPC Telekabel Wien: A totally legal court order...to do the impossible*, in *Kluwer Copyright Blog*, 2014, https://copyrightblog.kluweriplaw.com/2014/04/03/upc-telekabel-wien/;

[117] RIIS, SCHWEMER, *Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation*, in 22(7) *Journ. Int. L.*, 1-21, 4, (2019);

[118] SPOERRI, *On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market*, in 10(2) *J. Int. Prop. Inf. Tech. E-Com. L.*, 173-186, 179, (2019); EUROPEAN DIGITAL RIGHTS (EDRI), *More responsibility to online platforms – but at what cost?,* July 19, 2019, https://edri.org/our-work/more-responsibility-to-online-platforms-but-at-what-cost/;

[119] CJEU, case C-70/10, *Scarlet*; SIANO, *La sentenza Scarlet della Corte di Giustizia: punti fermi e problemi aperti*, in PIZZETTI, *I diritti nella "rete" della rete.*, 81-96;

[120] CJEU, C-360/10, *Sabam c. Netlog NV*;

preventive surveillance obligations, which are imposed on digital intermediaries by national authorities.

In such cases, the Court of Justice established the incompatibility between the art. 15 of the e-Commerce Directive and the obligation imposed on an internet service provider like Scarlet, or on an online social network like Netlog, to conduct a general monitoring and to put up filtering mechanisms on peer-to-peer communications, in order to stop copyright violations.

The court highlighted that such an obligation of preventive surveillance, entailing very high costs for the service provider, does not guarantee a fair balance between the need to protect intellectual property rights and the intermediary's freedom of enterprise, in addition to lead to violations of users' freedom of information and protection of personal data.

However, in the *UPC Telekabel Wien* case of 2014,[121] the Court has also interpreted EU law as not precluding a court from issuing such injunctions, as far as, in doing so, it does not unduly restrict internet users access to information and the measure prevents illegal access to protected content.

In the Court's findings, in fact, such a request does not appear to violate the very essence of the freedom to conduct a business, since, firstly, the ISP is free to choose the measures that are best suited to the resources and capabilities at its disposal, and secondly, the order's addressee is given the possibility to avoid liability, merely by proving that he has taken "all reasonable measures."[122] The Court has claimed in this regard that the possibility of exoneration does not imply that the addressee of the injunction will have to make "unbearable sacrifices", considering also that the ISP is not directly accountable for the violation.

Furthermore, in its approach to filtering systems, the *UPC Telekabel* case diverges, at least in part, from the precedents set by *Scarlet* and *Netlog*, considering that it amply demonstrates how the role played by ISPs is under serious threat, and demonstrates how the overall framework of Directive 2000/31 may be (and is) compromised by the implementation of other applicable directives.[123]

---

[121] CJEU, Case C-314/12, UPC Telekabel Wien;
[122] CJEU, Case C-314/12, UPC Telekabel Wien, §52-53;
[123] CJEU, Case 131/12 Google Spain v AEPD; GIOVANNELLA, *Online Service Providers' Liability, Copyright Infringement, and Freedom of Expression: Could Europe Learn from Canada?,* in FLORIDI, TADDEO, *The Responsabilities,* 228;

According to CJEU case law, a balance must be made between the preventative measures imposed on technical intermediaries and the applicable fundamental rights that might be impacted by such measures.[124]

Therefore, before issuing any monitoring, filtering, or blocking order, national courts must carefully assess both the proportionality and the basic rights, whereas the freedom of information, the users' right to privacy, and the companies' freedom to conduct business must all be protected.

Lastly, the European Court of Justice was recently requested to define the scope of the responsibilities that might be placed on a hosting provider under the e-Commerce Directive in the *Eva Glawischnig-Piesczek v. Facebook Ireland* case of 2019.[125]

In line with the Court's decision, a social network platform operator, such as Facebook, may be required to track down and remove comments which are identical to comments already previously declared illegal, as well as equivalent comments coming from the same user, which, however, cannot lead to an excessive obligation on the providers. The elements of the injunction, such as the name of the person concerned, the circumstances and the equivalent content, must therefore be duly specified.

These considerations concerned in the specific context a case of defamation, but are similarly applicable well beyond such scope, as they are also valid for the protection of digital content in cases of infringement of online intellectual and industrial property, which require ex post monitoring by ISPs, following a previous judiciary assessment of the digital content's unlawfulness.[126]

In the view of some analysts, however, this decision has made it possible to require platforms to actively monitor online contents,[127] since it would be difficult to put such strategy into effect, without simultaneously imposing a broad monitoring duty on the internet intermediary.[128]

---

[124] LAURENT ET AL., *SABAM v. Netlog (CJEU C 360/10) ... as expected!*, in *Kluwer Copyright Blog,* February 20, 2012, https://copyrightblog.kluweriplaw.com/2012/02/20/sabam-v-netlog-cjeu-c-36010-as-expected/;

[125] CJEU, case C-18/18, *Eva Glawischnig-Piesczek v. Facebook Ireland;*

[126] TOSI, *Responsabilità civile degli hosting provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilita' ex post***,** in 1 *Il Dir. Af.,* 2020, 1-24, *ivi* 16;

[127] CHELIOUDAKIS, *The Glawischnig-Piesczek v Facebook case: Knock, knock. Who's there? Automated filters online*, in *KU Leuven CiTiP*, 2019, https://www.law.kuleuven.be/citip/blog/the-glawischnig-piesczek-v-facebook-case-knock-knock-whos-there-automated-filters-online/;

[128] ROSATI, *Material, personal and geographic scope of online intermediaries' removal obligations beyond Glawischnig-Piesczek (C-18/18) and defamation*, in 41(11) *Eur. Int. Prop. Rev.*, 672-682, 677, (2019);

In continuity with the European case law, the aforementioned Italian Court of Cassation' decision in the 7708/2019 case, has also admitted the *pro future* injunction, in relation to specific contents published in violation of copyright, embracing the motivation for the appeal of the erroneous Milan's Court of Appeal decision of 7 January 2015, which instead denied such possibility to the holder of intellectual and industrial property rights.

### *4.5 The Problematic Definition of "Actual Knowledge"*

The liability of hosting providers is bound by Article 14(1) ECD to two knowledge standards of an illegal content. These are actual knowledge and awareness of circumstances surrounding the illegal status of hosted content, also known as constructive knowledge.
If a platform gains knowledge or awareness of illegal content, it must act quickly to remove it to benefit from the safe harbor. Recital 46 ECD reiterates this point, stating that the removal or disabling of access to illegal content should be done while observing freedom of expression principles and national procedures. This recital assumes that hosting providers who benefit from the safe harbor act in good faith.[129]

The definition of "actual knowledge" remains undefined in the case law of the Court.
It is clear, however, that the notion excludes constructive knowledge, knowledge presumptions or fictions, while it is uncertain whether the provision refers to "general" or "specific" knowledge of illegal activity or information stored at the request of a recipient of the service. In this context, "general" knowledge would refer to knowledge about the use of the service to host illegal content, whereas "specific" knowledge would relate to knowledge of the illegality of a particular hosted content.
European courts have traditionally interpreted "actual" knowledge as meaning "specific" knowledge, even though some scholars have suggested a shift towards a more "general" knowledge-based approach.[130] An example of the courts approach is provided in the case of *l' Oreal,* where the Court of Justice of the European Union (CJEU) stated that a notification regarding hosted illegal content must be "sufficiently precise and adequately substantiated" in order to result in actual knowledge of the infringement for the hosting provider.[131]

[129] NORDEMANN, *Liability of Online Service Providers,* 11;
[130] ANGELOPOULOS, *European Intermediary Liability in Copyright. A Tort-Based Analysis*, in 39 *Inf. L. Ser.*, 274, (2016);
[131] C-324/09 - L'Oréal, § 122;

The CJEU has provided some guidance in *l'Oréal* on what constitutes "awareness" within the meaning of art. 14 ECD.[132] A platform has awareness "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realized" that the content was unlawful and did not act expeditiously to take it down. The awareness standard should be interpreted in light of the model of good faith hosting provider endorsed in Recital 46 ECD, allowing courts to refuse safe harbor protection to hosting providers in bad faith or that are not sufficiently collaborative, i.e those intermediaries whose business model relies on fostering infringement by their users.

There exist two approaches to acquiring knowledge and awareness. The first is proactive, resulting from "investigations undertaken on the intermediary's own initiative".[133] The second is reactive, arising from "information supplied by an injured party or otherwise".[134]
From a purely legal perspective on intermediary liability, the incentives for intermediaries to engage in proactive efforts to acquire knowledge of infringement are limited. Such proactive measures may lead the intermediary to depart from the passive and neutral model preferred by the ECD and expose it to the risk of losing safe harbor protection (Good Samaritan paradox). Moreover, some measures aimed at proactively seeking knowledge of infringements within the platform may contravene art. 15 ECD, which prohibits the imposition of general monitoring obligations and cannot be imposed by Member States on platforms.
Consequently, it seems that knowledge or awareness will most commonly be acquired through reactive methods such as notifications by third parties. This incentivizes the adoption of Notice-and-Take-Down (NTD) procedures whereby hosting providers are obligated to remove infringing content they host if notified, or else lose the benefit of safe harbour protection.

Although art. 21(2) ECD requires more detailed harmonized rules on NTD procedures, the existing framework falls short of providing such procedures, as some countries within and outside Europe have already adopted them.[135]

---

[132] C-324/09 - L'Oréal, § 106;
[133] C-324/09 - L'Oréal, § 122;
[134] C-236/08 - Google France, § 109;
[135] In Europe, see e.g.: in Hungary art. 13, Act CVIII, 2001; in Finland, arts. 20-25, Act 458/2002; in the USA, secs 512(c)(1)(C) and 512(c)(3) of the Digital Millennium Copyright Act (17 U.S.C., 28 October 1998);

By solely requiring a service provider who "is actually aware of the facts" to take immediate action to remove or disable access to the illicit information, without any express reference to the necessity of the provider's actions to be subject to an order from a competent national authority, the European legislator appears to suggest that actual knowledge of illicit activities may, in principle, automatically give rise to an obligation on the part of the provider to act, even if the request to act comes simply from a private individual.[136]

However, not every notification of illegal content received by the platform automatically leads to a loss of safe harbor protection, if not accompanied by the removal of the content at issue. In other words, the action taken by the hosting provider following a notice does not necessarily have to entail taking down the content.

In the l'Oréal case, as previously mentioned, the judges underscore that a notification "may turn out to be insufficiently precise or inadequately sustained" to lead to actual knowledge or awareness on the side of the platform, and that it is for national courts to decide whether or not a platform can still rely on art. 14 ECD.[137] In this vein, National Courts and legislators, as well as stakeholders through Codes of Conduct, have established minimum requirements on occasion for notifications to lead to actual knowledge by the platform.

Nevertheless, even if notifications of illegal acts are characterized by sufficient precision and are brought to the knowledge of the service provider with sufficiently supported evidence, forcing service providers to automatically remove content, based on their discretionary assessment, without a response from a state authority and without clear and precise indications as to which specific content should be removed, could still entail serious risks that intermediaries may not always be able to evaluate with the same objectivity and professionalism as would be required of a public authority.

Considering effective, for the purpose of acquiring knowledge by the ISP, the notification from a party, even in the absence of an order from a judicial or administrative authority, may, indeed, potentially expose the ISP to charges of liability, in the event that the ISP acts upon a warning that is subsequently found to be groundless.[138]

---

[136] SICA, *Giurisprudenza nazionale ed europea e frammentazione legislativa della responsabilità civile del provider*, in MANCALEONI, POILLOT (EDT.), *National Judges and the Case Law*, 212;

[137] C-324/09 - L'Oréal, § 122;

[138] TOSI, *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca. a margine dei recenti casi "Google Suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale*, in 61(1) *Riv. Dir. Ind.*, 2012, 44-55, *ivi* 53; GAMBINI, *Gli hosting providers tra doveri di diligenza professio- nale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in 2 *Cost. it.*, 2011, 12;

Furthermore, unlike an administration or a judicial authority, web intermediaries are bearers of private interests and as such inevitably lean towards a greater or lesser control of their own content, based on the greater economic conveniences that they can derive from one behaviour or the other. If on the one hand, for example, a social network like Facebook may consider it more economically convenient to guarantee less control over its platform compared to the amount of the sanctions imposed on it by States authorities or the European Union, on the other hand, excessively high sanctions, both quantitatively and qualitatively, could instead lead it to adopt a more defensive approach in managing its content, sometimes ending with paradoxical and aberrant results, such as removing content that would not have been removed if placed under the control of a public authority, in order to prevent the risk of being fined.

For these reasons, a greater clarity regarding the exact notice and takedown procedures has become of fundamental importance, and different parts of doctrine have moved in this direction, with the purpose of developing possible solutions.

For example, in order to enhance the efficiency of the rules, it has been proposed that the Electronic Commerce Directive include a complete framework for a Notice-and-Takedown process that contains detailed provisions on notification exchange and evaluation. This framework should take into account that the majority of notifications are currently sent by automated means, rather than by humans, and offer incentives for minimizing mistakes in notifications and processing, such as fines, suspension of submission, or fees for alternative dispute resolution (ADR).[139]

Moreover, in an effort to protect fundamental rights, safeguards against over-removal of legitimate content should also be introduced, such as transparent rules on content removals, personalized explanations for affected users, audits for authorities or researchers,[140] and external Alternative Dispute Resolution (ADR) bodies, which could resolve complaints of affected users at the expense of providers if they make a mistake.

A legal immunity could therefore be granted to providers who adhere to Alternative Dispute Resolution (ADR) decisions, which would not only provide users with a credible remedy but also improve complaint rates.

Furthermore, such a system would also incentivize providers to improve the quality of their internal complaint mechanisms, as they would seek to avoid ADR-related costs.

---

[139] DE STREEL, HUSOVEC, *The e-Commerce Directive*, 47;

[140] European Parliament Resolution, P9_TA(2020)0032, 12 February, 2020, *Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services*;

However, for effective ADR and any other dispute resolution to take place, providers must be able to differentiate between violations of law and violations of the Terms of Service.
In this perspective, an essential requirement for the implementation of such a system would be that providers are bound by ADR decisions for at least a certain limited time, since otherwise providers could circumvent ADR decisions by simply changing their terms of service, thereby undermining the integrity of the ADR system.
Considering that the value of user-generated content decreases with time, introducing a delay to such decisions should be sufficient for users to protect their speech interests, while still ensuring that providers retain control over their "house rules". If external ADR functions well, it can incentivize providers to invest in good quality internal control mechanisms such as internal ADR, human review, etc., over the long term.

As for the Italian legal system, the legislator has differently declined the obligation of removal or disabling of access to illicit information or activities imposed on hosting providers, making it subject to the receipt of a communication from a national competent authority or, in any case, to the knowledge of facts that make the illegality apparent.[141]
In doing so, the Italian system has the undeniable merit of linking the immediate intervention of removal or obscuring of stored material to an investigation carried out by competent national authorities, which ensures that it is not the hosting provider, exercising partly investigative, partly adjudicatory, and partly censorial powers, who investigates and decides whether a user is committing an offense or disseminating illicit information, as well as who unilaterally classifies certain information or activities as illegal, regardless of the purposes pursued by the person making it available, and who intervenes, if necessary, to suppress established illegality.
It is easy in fact to predict the reactions that the possible censorial interventions of telematic operators - removal or, perhaps, even before that, the choice of materials to be disseminated on the network - could trigger in content authors, who might feel their constitutional right to freedom of expression has been violated,[142] in addition to possible contractual liabilities that service recipients could invoke for damages suffered as a result of abusive removals or disabling of access.

[141] Italy, Legislative Decree 70/2003, art.16, par.1, letr. b);
[142] RODOTÀ, *Libertà, Opportunità, Democrazia e Informazione,* in *Convegno Internet e Privacy – Quali Regole?,*1998, https://www.privacy.it/archivio/garanterelrod.html; DI CIOMMO, *Internet, Diritti della Persona e Responsabilità Aquiliana del Provider,* in *Dan. Resp.*, 1999, 754-767, *ivi* 756;

In this perspective, therefore, the provision represents an evident attempt to reconcile the opposing needs for protection of injured situations and guarantee of freedom of expression.

On the other hand, as for all the other cases where the intermediary, through any other means, is aware of the illicit or harmful nature of the content of a service to which it provides access, the legislator has not provided for the stricter obligation of removal or disabling of access to the service, but simply the more permissive obligation to inform the competent authorities.[143] The reason for this lesser rigor can be found in the fact that, while in cases where the obligation of the removal or disabling of access occurs the intermediary is bound to act by the authority of a judicial or administrative order or, in any case, by the objectivity of manifestly illicit facts (e.g. paedophilia, hardcore pornography, etc.), in all other cases the legislator has hypothesized cases of third parties' civil rights violations (e.g. unfair competition, counterfeiting of trademarks and domain names, etc.) of which the intermediary has only knowledge through the third party, but without the issuance of orders by the judicial or administrative authority brought to its knowledge or the manifest illegality of the fact itself emerging from the context or the situation .[144]

It follows that the legislator, once again, does not want to make the intermediary a judge of the case, with the almost inevitable burden of responsibility either towards the victim or towards the alleged perpetrator of the offense, in the event that the intermediary adopts an omissive or repressive conduct, later contradicted by decisions of the judicial or administrative authority.

The clear wording of the legislative decree leaves no doubts that the certainty of illegality cannot derive from the mere knowledge of a site that, in abstract, could violate the rights of third parties, since the intermediary is not called upon to be a judge of an offense reported by third parties. It seems therefore reasonable to impose on the intermediary in these cases only an informational obligation.

This finding assumes all its relevance in particular in relation to errors of law, because if the intermediary host does not recognize, even negligently, that content known to him is illegal, in the absence of a decision by the judicial or administrative authority, and refrains from blocking it, when this is technically possible, he is not liable, because EU legislation protects the intermediary host for "negligent" ignorance of the content.

---

[143] Italy, Legislative Decree 70/2003*,* art.17, par.3;
[144] BOCCHINI, *La Responsabilità Civile degli Intermediari,* 156, 172;

Therefore, beyond the cases in which the intermediary fails to comply with the removal notices from the public authorities, the responsibility of the intermediary host for failure to remove content only arises in cases where the intermediary host has knowledge, by any means, of the manifest illegality of the activity or information, and not of the mere fact, and has not acted to remove such content. In all other cases, at the most, liability could arise for failure to communicate the alleged illegal acts to the competent authorities, but not for refusing to remove certain content from the service to which they give access.

Hence, considering the vital role played by national competent authorities in protecting the constitutionally guaranteed interests by communicating the content that must be removed, it is clear enough that the most significant critical issues arise regarding the determination of what constitutes manifestly unlawful activity or information, as it bounds the intermediary to immediately remove such content even without receiving any communication from the state authorities.

In this regard, it has been suggested that a possible solution could lie in the professional diligence that the intermediary must follow while carrying out its activities, as explicitly mentioned in recital 48 of Directive 2000/31/EC concerning the identification and prevention of illegality.[145]

The duty of diligence that a hosting provider must reasonably exercise, given its capacity as a professional operator with greater control and knowledge of the material hosted on its server, may lead to demands for knowledge of information not requirable from other intermediary service providers. Moreover, the regulatory provisions may include the cases where the provider knowingly ignored manifest illegality, thereby failing to exercise due diligence in identifying and interpreting the clear signs of such illegality.

For instance, a case of manifest illegality may be considered the illegal content of hosted sites that results evident from the choice of a domain name denoting the unequivocal danger or harmfulness of the content itself.

Furthermore, without prejudice to the prohibition on imposing on the intermediary service provider a constant obligation of surveillance and active research on the network of illegal activities, the duty of diligence may even involve a hypothetical control and evaluation by the operator on the hosted material, where the choice of an ambiguous domain name or the

[145] GAMBINI, *Le responsabilità civili dell'Internet service provider*, 293;.

use of unambiguously offensive expressions indicates the clear illegal nature of the content or activities stored, and the presence of sites manifestly suspected of illegality on its server.
In addition to this, the duty of diligence may ultimately be violated also in cases of failure to adopt filtering systems or other technical devices that could easily detect or prevent the presence of manifestly illegal information or activities on the web space made available to users, which should be evaluated in light of the organizational solutions adopted by an average provider engaged in storage activities, that is one that behaves according to the state of the art known in its professional field, in line with the Article 1176, paragraph 2, of the Italian Civil Code.

It is evident, therefore, that the apparent distinction between the European legal system, which refers in its case law to the criterion of the "diligent economic operator", and the Italian legal system, which distinguishes between obligations to remove content based on notification from competent authorities and cases of manifest illegality of the content, which can be communicated even by a private individual with an interest, ultimately fades away, since the determination of those contents characterized by manifest illegality also implies the same discretionary evaluation by the ISPs, in accordance with the criterion of the diligent operator, as to which contents should be considered manifestly illegal, in order to automatically censor them without the need for a state order, based on their subjective evaluation of the specific case.

Over time, Italian case law has indeed offered several examples of this legal uncertainty, which does not allow to determine with certainty and clarity the factors that trigger a duty on the part of internet service providers to remove content, which would avoid burdening the ISP with the discretionary evaluation, time and again, of when they should take action on the content reported by their users, in order to avoid being considered insufficiently diligent according to current best practices.
For example, in the well-known case of Tiziana Cantone,[146] the judge reiterated the absence of obligations of preventive surveillance or active search for illegal facts and circumstances on the part of providers but established that Facebook should have promptly removed the content reported by the claimant as seriously damaging to her reputation, thus trusting the

[146] Court of Naples, case n.9799, November 4, 2016; BOCCHINI, *La responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in 3 *Giur. it.*, 2017, 632-643, 637; ALLEGRI, *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti, in 26(1-2) Inf. Dir., 2017, 69-112, ivi 100;*

party's warning, without waiting for the judicial authority's order. This was because, in the case of a violation of personal rights, the claimant's inactivity would have irreparably prejudiced them and would no longer be susceptible to reinstatement.[147]

In addition to this, in the aforementioned sentence n. 7708 of March 19, 2019, the Court of Cassation sets out the further legal principle regarding the time and modus operandi of the ISP's civil liability, with great detail, establishing that the liability of the active hosting provider arises when: "a) the ISP has legal knowledge of the illegal act committed by the recipient of the service, having received notice from the holder of the injured right or aliunde, specifying the non-necessity of a judicial removal order, and, upon closer examination, expanding the hypothesis of knowledge of the illegality to any form of information retrieval of the commission of the illegality and not only, therefore, to communication by the injured party; b) the illegality of another's conduct is reasonably ascertainable, so that they are grossly negligent for not having positively verified it, in accordance with the degree of diligence that can reasonably be expected from a professional network operator at a given historical moment; thus taking a considerable step forward as the actual knowledge of illegality, initially only connected to a judicial removal order, then expanded to the mere communication of illegality by the injured party, becomes knowledgeable according to the technical diligence parameter linked to the evolution of the information society at a given historical moment; c) they have the possibility of usefully activating themselves, since they have been sufficiently specifically informed of the illicit contents to be removed".

In outlining the responsibility of the Internet Service Provider (ISP) resulting from the failure to remove the reported illicit content (more precisely, known or knowable illicit content), the Supreme Court highlights the need for the notice of the illegality to be sufficiently specific or suitable to enable the ISP to retrieve the illicit content complained of by the injured party.

## 5. The DSA: News and Changes in the e-Commerce Directive Discipline

The Digital Services Act maintains the fundamental principles of the e-commerce Directive, confirming the need for regulation of the liability of intermediary service providers while seeking to preserve the delicate balance between the various interests at stake, particularly the protection of citizens on the one hand, and the protection of the digital market, which also means protecting its users, on the other.

[147] Naples North Court, order of November 3, 2016;

As a result of the DSA, articles 12, 13, 14, and 15 of Directive 2000/31/EC are repealed and replaced, respectively, by Articles 4, 5, 6, and 8 of the new Regulation, following a substantial continuity with the e-commerce Directive, albeit not without some significant innovations.
If on the one hand, in fact, its main merit stands in that, as a Regulation, it renders such provisions directly enforceable within each Member State, without the need for national legislation,[148] on the other hand, the DSA also incorporates new legal and regulatory aspects that may result in more complex interpretation problems, which ultimately may need to be resolved by the Court in Luxembourg.

Providing for a system of general immunity for internet service providers, the DSA is also similar to Directive 2000/31/EC, given that the provider complies with certain regulatory requirements, that are distinguished based on the different activities performed by the provider itself, namely mere conduit, caching, or hosting.
In line with the current system, the DSA establishes, for each of the indicated categories, the conditions that exclude the provider's liability for the illegality of the information transmitted and/or stored.[149] In particular, the art. 6 of the DSA retains the core of the existing intermediary liability regime, which implies that online platforms are essentially not accountable for third-party content.
Among the reasons why the DSA maintained the liability regime of the e-Commerce Directive, within the DSA proposal it has been considered particularly the clarification and guidance provided by the European Court of Justice (ECJ) with its interpretations,[150] which have resulted in legal certainty, allowing ultimately new services to flourish within the internal market.[151]
The impact assessment suggested that altering the liability exemption, by increasing legal risks for intermediaries, would have negatively impacted citizens' freedom of expression online, in addition to be excessively expansive for new businesses.

[148] FACCI, *La Responsabilità dei providers*, in ROSSELLO, FINOCCHIARO, TOSI*, Commercio elettronico*, 234; BOCCHINI, *La responsabilità di Facebook*, 636;
[149] ARROYO AMAYUELAS, *¿La responsabilidad de los intermediarios en internet: puertos seguros a prueba de futuro?*, in 12(1) *Cuad. Der. Trans.*, 808-837, 823, (2020);. VAN HOBOKEN, *Legal Space for Innovative Ordering,* 15;
[150] European Commission, COM/2020/825, 3;
[151] Regulation (EU) 2022/2065 (DSA), recital 16;

Reducing the standard for hosting providers to qualify for liability exemptions would have ultimately harmed, as a consequence, the security and trust of the entire online environment.[152]

Apart from the immunity from liability, the other two pillars that are enshrined in the e-Commerce Directive, and which the DSA recalls, are the country-of-origin principle and the ban on general monitoring obligations.[153]
The country-of-origin principle, which stipulates that an online platform is only subject to the liability laws of the EU country in which it is located,[154] remains in effect under the DSA, but its significance has been reduced through harmonization at the EU level.[155]
As for the ban on general monitoring obligations, the DSA, acknowledging that there is a fine line between prohibited general monitoring measures and specific monitoring measures that are allowed,[156] especially in cases of suspected intellectual property rights infringement,[157] retains the ban on general monitoring obligations and clarifies that authorities and courts may issue orders to halt specific instances of illegal content.[158]

The impact assessment produced for the DSA highlighted three primary weaknesses in the current liability system,[159] which have therefore been addressed in the course of the Regulation's legislative proceeding: first, the e-commerce Directive does not specify when a platform is considered to have gained "actual knowledge" of an illegality that requires the removal of content; second, the definition of an "active" role is ambiguous; and third, the e-commerce Directive may discourage voluntary efforts to combat illegal online content.

As for the first of these critical issues, within the context of this Regulation, the lawmaker seems to have become aware of the fact that the e-commerce Directive does not provide a

[152] European Commission, *Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digi- tal Services Act) and amending Directive 2000/31/EC*, SWD (2020) 348 final, Part 2, 48;
[153] BUITEN, DE STREEL, PEITZ, *Rethinking Liability Rules for Online Hosting Platforms*, in 28(2) *Int. J. L. Inf. Tech.,* 139-166, 144,145, (2020);
[154] Directive 2000/31/EC, art. 3; HOLZNAGEL, *Platform Liability for Hate Speech & the Country of Origin Principle: Too Much Internal Market?*, in 21(4) *Comp. L. Rev. Int.,* 103-109, 103, (2020);
[155] WILMAN, *Het voorstel voor de Digital Services Act*, 28;
[156] Case C-360/10 *SABAM v Netlog* EU:C:2012:85;
[157] Case C-314/12 UPC Telekabel Wien v Constantin Film Verleih and others EU:C:2014:192;
[158] Regulation (EU) 2022/2065 (DSA), art 4(3), 5(2), 6(4), recital 31; BERBERICH, SEIP, *Der Entwurf des Digital Services Act,* in 1 *Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR- Prax)*, 4, (2021);
[159] EC *Impact Assessment*, part 2, 157;

clear guidance regarding the threshold at which a platform is considered to have gained "actual knowledge" of a violation, which would immediately require it to remove the interested content.

In order to fill this void, article 16 of the DSA, in coordination with article 6, has consequently outlined the requirements for a notice-and-action mechanism, which, by reaching a certain level of obviousness, is intended to trigger knowledge or awareness of such illicit on the part of the provider.

In this direction, paragraph 2 of the article 16 specifically requires notices of illegal content to be submitted in a "sufficiently precise and adequately substantiated" way, whereas paragraph 2, letter A further specifies that such notices must include "a sufficiently substantiated explanation of the reasons why the individual or entity alleges the information in question to be illegal content".

Nevertheless, it is crucial to note that a user's assertion that certain content is illegal does not necessarily constitute knowledge or awareness under Article 6, unless the notified content meets a specific threshold of obviousness of illegality. For this reason, upon obtaining such a precise and substantiated explanation, paragraph 3 of article 16, recognizing a well-tested orientation already established in the CJEU and in several other national supreme courts,[160] has made it clear that, in order to equip providers with such actual knowledge of illegality on their platforms, notices shall "allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination",[161] so as to permit it to analyze the notices and take the consequent decisions in a "timely, diligent, non- arbitrary and objective manner".[162]

In a similar sense recital 22 clarifies that notices need to be "sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content", [163] and states that the removal or disabling of access to content "must adhere to the principle of freedom of expression". This last overarching provision, in particular, is consistent with the EU legislation, which requires platforms and relevant authorities to consider the impact of their decisions on freedom of expression, alongside other factors such as their effectiveness and the effect on other rights.

[160] Italian Supreme Court of Cassation, case 7708/2019;
[161] Regulation (EU) 2022/2065 (DSA), art. 16, par.3;
[162] Regulation (EU) 2022/2065 (DSA), art. 16, par.6;
[163] Regulation (EU) 2022/2065 (DSA), recital 22, art. 16 (2,3);

In any case, however, these legal indications lack any specificity with regards to the criteria, parameters, and safeguards that platforms must incorporate when implementing these measures. Administrative and judicial authorities in charge of overseeing these aspects, in fact, are not provided with any specific mandate, procedural or substantive, for the proper consideration and protection of human rights, whereas public intervention, in this regard, is primarily aimed at ensuring that illegal content is addressed or eliminated.

It is also evident that the DSA, just as the E-Commerce Directive, lacks precise instructions on how to detect such obviousness of illegality or to determine if there has been a reasonable effort to identify this illegal content. It is not clear, in fact, what kind of specific information is necessary to activate such a level of awareness on the part of the provider, so as to be able to objectively and unanimously recognize the presence of illegality on its platform.
Although the notice-and-action mechanism depends on the existence of specific illegal content, in fact, the DSA intentionally refrains from providing a substantive definition of what constitutes illegal content in this context and throughout the whole Regulation. Instead, the DSA only refers to illegal content, in its article 3H), as any information that, either by itself or in connection with an activity such as the sale of products or provision of services, violates Union or Member State law that complies with Union law, regardless of the law's precise subject matter or nature. That is, in other words, that the Regulation relies only on current legal provisions from corresponding sector-specific legislation, at the national or EU level, to assess the legality of content circulating on online platforms.
That being the case, the new Regulation apparently continues to carry on the serious risk that, despite all the generical recommendations which the European legislation constantly recalls in its provisions, such ambiguity might still encourage an over-removal of content from the platforms, with significant implications for the exercise of fundamental rights such as, foremost, freedom of expression and information.

Furthermore, art. 16, par. 6, in requiring platforms to analyze any notice they receive and take the consequent decisions concerning the information related to those notices, establishes that such reaction by the provider should be enacted in a non well specified “timely” period, which leaves unexplained the effective and precise margin of time within which the provider must take notice of the reported illegality, in order to avoid liability.

In the absence of regulatory guidance, it is clear how also such imprecision will only be inevitably left to the discretion of individual national judicial bodies, which may ultimately change by court to court, generating further confusion.[164]

As to the problematic distinction between active and passive providers, the Impact Assessment acknowledges that there is still uncertainty regarding the definition of when an intermediary, particularly a hosting service provider, can be said to have knowledge or control over the data it hosts. The Impact Assessment clarifies that certain automatic activities such as tagging, indexing, providing search functions, or content selection are necessary for user-friendly services and, given their importance for navigating through a vast amount of content, should not be seen as evidence of an "active role".
Acknowledging this position, the DSA finally crystalizes the traditional interpretation of "actual" knowledge, as meaning "specific" knowledge, and establishes that "such actual knowledge or awareness cannot be considered to be obtained solely on the ground that the provider is aware, in a general sense, of the fact that its service is also used to store illegal content." The DSA explains in fact that "the fact that the provider automatically indexes information uploaded to its service, that it has a search function or that it recommends information on the basis of the profiles or preferences of the recipients of the service is not a sufficient ground for considering that provider to have 'specific' knowledge of illegal activities carried out on that platform or of illegal content stored on it".[165]
In doing so, the provider should no longer risk anymore being considered, in carrying out such activities indicated by the Regulation, as sufficiently aware of illicit content on its platform as it is required to be considered an "active" provider and should ultimately retain the benefit of the safe harbor, as long as it is going to continue to exercise an activity of a "mere technical, automatic and passive nature".

In order to qualify for liability exemptions, however, despite the strong misgivings of some authors,[166] service providers must still maintain a clear distinction between a passive, neutral role and an active one,[167] meaning that, as before, there must be no knowledge or control

[164] BARATA, *Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act*, https://cdt.org/insights/positive-intent-protections-incorporating-a-good-samaritan-principle-in-the-eu-digital-services-act/, 14;
[165] Regulation (EU) 2022/2065 (DSA), recital 22;
[166] BUITEN, *The Digital Services* Act, 371;
[167] Regulation (EU) 2022/2065 (DSA), recital 18; CAUFFMAN, GOANTA, *A New Or- der: The Digital Services Act and Consumer Protection*, in 12(4) *Eur. J. R. Reg.*, 758-774, 764, (2021);

over the information stored and that only technical and automatic functions must be performed.[168] From this point of view, the DSA does not significantly develop this concept,[169] but does provide some further clarifications, which may help in any case to provide a better distinction between the two categories.

Firstly, the DSA includes for the first time in a European legislation a "Good Samaritan" clause.[170]

Secondly, the DSA excludes intermediary service providers from liability exemptions if they knowingly cooperate with users to engage in illegal activities, since, in that case, the provider lacks the requirement of the neutrality.[171]

Lastly, with the aim of protecting the average consumer,[172] the last point to consider is that if a third-party presents offers that appear as if they are the online marketplace operator's own offers, the operator cannot claim exemption from liability.[173] In this scenario, in fact, it is not as important to determine who controlled the offer or stored the information, but rather whether the service provider gave the impression that the offer or information originated from them.

For instance, one scenario where this may occur is if an online platform delays providing the identity or contact information of a seller until after the consumer has completed the transaction, or if an online platform promotes a product or service under its own name, rather than under the name of the seller who will actually provide the product or service.[174]

This liability framework aims to distinguish the responsibilities of various e-commerce platforms based on their level of involvement in promoting and executing transactions, with some having a limited role and others playing a central role.

Lastly, based on the impact assessment, the interpretation of the e-commerce Directive by the ECJ has resulted in a contradictory set of incentives for service providers, which has led to serious doubts concerning the efficiency of the current legal system.

---

[168] Cases C-236/08 to C-238/08 *Google France and Google v Louis Vuitton*;
[169] BERBERICH, SEIP, *Der Entwurf des Digital Services Act,* 4;
[170] Regulation (EU) 2022/2065 (DSA), art. 7, recital 26;
[171] Regulation (EU) 2022/2065 (DSA), recital 20;
[172] Opinion of Advocate General Maciej Szpunar, 2 June 2022, Christian Louboutin v. Amazon, Joined Cases C-148/21 and C-184/21, ECLI:EU:C:2022:422, par. 65-72, https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220096en.pdf;
[173] Regulation (EU) 2022/2065 (DSA), art. 6 (3), recital 24; BUSCH, MAK, *Putting the Digital Services Act in Context: Bridging the Gap Between EU Consumer Law and Platform Regulation,* in 10 *J. Eur. Cons. Mar. L.*, 109-115, 110, (2021);
[174] Regulation (EU) 2022/2065 (DSA), recital 24;

As already seen before, in fact, when taking proactive measures to identify illegal activities, it has been argued that service providers play an "active" role, as services controlling the content uploaded by users, and therefore that they are not eligible for exemption from liability.
This has created a situation where the e-commerce Directive may paradoxically discourage service providers from taking voluntary measures to remove or detect unlawful content.
For this reason, another principle that with the DSA has finally been introduced, for the first time at a European regulatory level, is the protection of the so-called "Good Samaritan".[175]
In line with the objective of encouraging service providers to improve their platform monitoring practices without breaching the ban on general monitoring obligations, this regulation is likely the most noteworthy development in terms of liability.

Following the Anglo-Saxon system, and in particular the Section 230© of the Communication Decency Act, this principle aims to assert that intermediaries are not penalized and, above all, do not lose the benefit of the exemption from liability only because they have voluntarily implemented measures aimed at combating illegal content.
According to Article 7 of the DSA, intermediaries may not lose their liability protections "solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation".
Recital 26 reinforces and elaborates such principle, stating that the mere fact that providers undertake investigative activities "does not render unavailable the exemptions from liability set out in this Regulation, provided those activities are carried out in good faith and in a diligent manner", where specifically "the condition of acting in good faith and in a diligent manner should include acting in an objective, non-discriminatory and proportionate manner, with due regard to the rights and legitimate interests of all parties involved, and providing the necessary safeguards against unjustified removal of legal content, in accordance with the objective and requirements of this Regulation".

The choice to give regulatory status to such a criterion has the dual purpose of incentivizing voluntary proactive measures, by providers, in searching for and removing illegal content

[175] SAVIN, *The EU Digital Services Act*, 6; BARATA, *Positive Intent Protections*, 1;

without this, paradoxically, turning against them and causing a loss of the "safe harbor" protection recognized to them.[176]

This legislative novelty must be welcomed, considering that the prevention and monitoring of information traveling on the network plays a crucial role in enabling the rapid removal of any illegal content. This need is further amplified by the realization that the prompt intervention of intermediaries plays a primary role, given that the persistence of illegal content over time is capable of exponentially increasing the damage suffered by the injured party, both in terms of quantity and quality.[177]

Nonetheless, such innovation comes not without challenges in terms of legal interpretation. For instance, the explicit reference to the diligent operator criterion, in addition to that of good faith, both explicitly invoked by Article 7 to confer protection to the so-called "good Samaritan", distinguishes considerably the liability protection clause for intermediaries provided by the DSA compared to that introduced in the United States under Section 230 (c)(1) of the CDA, which, conversely, does not mention any diligence requirement, referring exclusively to the good faith prerequisite of the provider.

This difference, apparently superficial, risks, upon further analysis, entirely hampering the effectiveness of the norm itself, to the extent that an erroneous removal or failure to remove content by the provider, even if done in good faith, would still risk compromising the quality of diligent operator, ultimately leading to a loss of the safe harbor protection for the operator.[178]

For instance, Kuczerawy provides the example of a moderator who is trained to identify one type of illegal content but is unaware that a specific video may violate another rule.[179] If the moderator fails to remove the illegal content, despite reviewing it, the hosting provider could still be held liable because it either "knew" or "should have known" about the illegal activity. It is therefore of crucial importance that case law, over time, continues to specify further, in increasingly detailed and precise terms, in which cases an intermediary can benefit from the safe harbor provision, by operating diligently in accordance with this regulation.

---

[176] VAN HOBOKEN ET AL., *Hosting intermediary services and illegal content online.*, 40; RODRÍGUEZ DE LAS HERAS BALLELl*, Il paradigma della responsabilità degli intermediari digitali nel contesto di una economia di piattaforme (platform economy*), in 1 *Dir. Com. Sc. Int.*, 2018, 203ss., *ivi* 210;

[177] SCOLA, *Digital Services Act: occasioni mancate e prospettive future nella recente proposta di regolamento europeo per il mercato unico dei servizi digitali***,** in 1 *Contr. Imp. Eur.,* 2022, 156;

[178] KUCZERAWY, *The EU Commission on voluntary monitoring;*

[179] KUCZERAWY, *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*, in *Verfassungsblog,* 2021, https://verfassungsblog.de/good-samaritan-dsa/;

This is primarily to avoid situations where, despite the inclusion of the Good Samaritan clause, intermediaries may still be induced to remove an excess of content or, conversely, to not conduct enough searches for illicit elements on their platforms, in order to avoid as much as possible the risk of not being considered diligent when managing information on their platforms, and therefore not being able to enjoy liability protection in the exercise of their activities.

In the end, in addition to a revision of the most critical issues affecting the current ECD liability regime, another significant introduction, made by the DSA, is the prediction of new rules regarding the orders national judicial or administrative entities can issue to intermediaries, established in Articles 9 and 10 of the Regulation.
Such orders may require intermediaries to collaborate with the judicial or administrative authorities of member states in fighting specific instances of illicit content. The directives must contain a statement of reasons and information about the possibility of appealing, as well as indicating the legal basis of the order, the authorities involved, and the content in question.
Articles 9 and 10 do not confer new powers, but rather establish a harmonized framework for the exercise of existing powers in an efficient and effective manner.[180]

### 6. Coordination With the Copyright Directive and Other Sector Specific Laws

In the digital age, online platforms serve as the primary gateway to information and other content, whether accessed through search engines, social networks, micro-blogging sites, or video-sharing platforms.[181]
While these platforms offer many benefits, such as facilitating economic and social interactions, they have also facilitated the unprecedented dissemination of unlawful content, such as hate speech, incitement to terrorism, and copyright infringement.[182] This has happened particularly within the context of the so-called Big Tech platforms, such as Facebook and YouTube, which, in the last 15 years, have acquired significant control over online speech and commerce.[183]

[180] Regulation (EU) 2022/2065 (DSA), recital 31;
[181] European Commission, COM/2017/0555, 2;
[182] European Commission Recommendation of January 3, 2018 on measures to effectively tackle illegal content online, C/2018/1177;
[183] SUZOR, *Lawless,* 134;

In response to such challenges, the European Union and its Member States have proposed and enacted a growing number of laws and policies aimed at regulating online content, through a gradual transition from a regime of uniform and horizontal responsibility to a stratified and vertical system of liability, which takes into account the varying degrees of danger associated with the specific activities conducted by individual operators.

Regarding copyright-protected material, Article 17 of the Directive on Copyright in the Digital Single Market (CDSM Directive), which precedes the Digital Services Act (DSA), establishes a new liability regime for Online Content-Sharing Service Providers (OCSSPs), whose rules had to be adopted by EU Member States by June 7, 2021. [184]
The concept of OCSSPs is defined in art. 2(6) of the CDSM Directive, with further guidance in recitals 62 and 63, and it indicates providers of an information society service, whose primary objective is to collect and provide access to massive amounts of user-generated content, at the condition that the purpose for organizing and promoting such content is of an economical nature.

Article 17 CDSMD stipulates that the OCSSPs, allowing access to works or contents uploaded by their users, become directly liable for such uploads and, limited to copyright relevant acts, are therefore expressly excluded from the hosting safe harbor enshrined in art. 14(1) of the e-Commerce Directive, which, until that moment, used to be applied on the most part of such contents.
Assuming arguably the features of a lex specialis with respect to the liability regime set down in the Digital Service Act,[185] which recalls the e-Commerce discipline, this provision establishes later a complex set of regulations to govern OCSSPs, which include a liability exemption mechanism in paragraph 4, along with various mitigation measures and safeguards.
The liability exemption mechanism requires OCSSPs to comply with best-efforts obligations for preventive measures, which include filtering content ex-ante, notice and stay-down, and

[184] Directive (EU) 2019/790 (Copyright Directive), art. 17;
[185] PEGUERA, *The New Copyright Directive: Online Content-Sharing Service Providers Lose ECommerce Directive Immunity and Are Forced to Monitor Content Uploaded by Users (Article 17),* in *Kluwer Copyright Blog*, 2019, http://copyrightblog.kluweriplaw.com/2019/09/26/the-new-copyright-directive-online-content-sharing-service-providers-lose-ecommerce-directive-immunity-and-are-forced-to-monitor-content-uploaded-by-users-ar- ticle-17/;

notice and takedown mechanisms.[186] Article 17(4) establishes in particular three cumulative conditions for this liability exemption mechanism, consisting of i) a demonstration of a diligent request for an authorization;[187] ii) a demonstration of best efforts to ensure the unavailability of specific works indicated in details by the right holders; iii) expeditious take down measures, in addition to preventive actions, subsequent to notices from right holders.
Considering such provision, the second condition appears to impose an upload filtering obligation, as some critics have argued, while the third condition introduces a notice-and-takedown mechanism similar to that of article 14 of the e-Commerce Directive, along with a notice-and-stay-down obligation, or re-upload filtering.[188]

Article 17 of the CDSM Directive and multiple provisions of the DSA impose obligations on how online platforms should handle illegal information.
However, whereas Article 17 of the CDSM Directive targets content that infringes copyright, the DSA, by revamping the 21-year-old horizontal rules on intermediary liability in the e-Commerce Directive, focuses more on illegal content in general, including that which infringes copyright, thus creating the issue of how the two legislations will interact with each other once both have fully entered into force.
If at first glance, in fact, these regimes may possibly appear to not overlap, since article 17 of the CDSM Directive is lex specialis to the DSA, upon a closer examination a much more complex situation emerges, whereas the proposed DSA regulation is complementary to article 17 of the CDSM Directive and imposes several additional obligations on online platforms that qualify as "online content sharing service providers" (OCSSPs).
For this reason, given also the territorial nature of copyright law, which, consisting in varying national implementations of article 17 of the CDSM Directive, ultimately risks to further complicate matters, it is therefore necessary to analyze the extent to which the DSA provides a new regulatory approach to online platforms, through a new horizontal regime that extends to most corners of EU law.

[186] Directive (EU) 2019/790 (Copyright Directive), art. 17 (4) (b) (c);
[187] METZGER ET AL., *Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law – Comment of the European Copyright Society,* in *SSRN Elect. J.*, 1-21, 3,(2020);
[188] HUSOVEC, *How Europe Wants to Redefine Global Online Copyright Enforcement*, in 16 *TILEC Discus. Pap.,* (2019);

From this view point, a first issue, which is likely going to affect the concrete application of the two legislation, is whether the DSA is also going to be applied to the so called OCSSPs.
In this regard, it is important to notice that a potential conflict between the two legislations may only arise when dealing with copyright-related portions of an online platform that qualifies as an Online Content Sharing Service Provider (OCSSP). If on the one hand, in fact, article 17(3) of the Copyright Directive in the Digital Single Market (CDSM) Directive clearly states that the hosting safe harbor provision of the e-Commerce Directive, as well as that of Article 6 of the Digital Services Act, applies to OCSSPs "for purposes falling outside the scope of this Directive", on the other hand, art. 2 (3) of the DSA conversely establishes that the Regulation does not affect the copyright and related rights rules set out by Union law. For instance, in the case of YouTube, which qualifies as an OCSSP, if the information or content it hosts is related to copyright, the CDSM Directive's Article 17 is then going to be applied. If instead, on the other hand, the information or content pertains to hate speech, child sexual abuse material, or any other unlawful information or content, then the hosting liability exemption of the e-Commerce Directive, and correspondingly that of the DSA, is necessarily going to be taken into account. In other words, YouTube would be deemed an OCSSP for copyright purposes, while it would be considered a Very Large Online Platform (VLOP) for other types of information.

The Explanatory Memorandum, however, clarifies that, despite specific obligations set out in other Union legal acts will continue to apply, the DSA will still apply to providers wherever there are no more specific provisions, meaning that, even though the rules and procedures set out in art. 17 for OCSSPs under the CDSM Directive have to be considered more specific than the DSA's provisions, the DSA is still going to be applied to OCSSPs for any rule which regulates matters not covered by art. 17 and specific rules where art. 17 allows for Member State discretion.
This applies to other types of illegal content as well.

Given such overlap between OCSSPs and online platforms or VLOPs, the main legal question is therefore how the liability rules (Chapter II) and the asymmetric obligations (Chapter III) of the DSA are going to apply to these online platforms.
Although the analysis mainly refers to copyright, it can serve as well as a framework for examining how the DSA's liability and obligations would apply to other sector-specific legislations such as the AVMSD, which already imposes obligations on video-sharing

platform services to protect minors and EU citizens from certain types of harmful and illegal content, while also assigning "cooperative responsibility" to the platforms' organizational control.[189]

According to some authors' view,[190] OCSSPs are partly exempt from the liability rules in the DSA. The art. 6 hosting safe harbor, which replaces the e-Commerce Directive's article 14, is not applicable to OCSSPs, as expressly established by art. 17(3) CDSM Directive, given that the activities at issue fall within the scope of art. 17 CDSM Directive itself.
However, the general monitoring prohibition in art. 7 DSA, which replaces art. 15 ECD, does not appear to be affected by the CDSM Directive. While, in fact, art. 17(8) CDSM Directive states that the article's application shall not impose any general monitoring obligation, it does not set aside art. 15 of the e-Commerce Directive.
As for the "Good Samaritan" rule in article 6 of the DSA, regarding voluntary investigations and legal compliance, the provision is not clear in its application to OCSSPs. This is because, due to its express reference to the liability exemption set in the DSA, the norm seems to be directly linked to the specific hosting safe harbor, which does not apply to OCSSPs according to article 17(3) of the CDSM Directive.
Furthermore, such provision is intended to enable actions aimed at detecting, identifying, and removing illegal content or complying with EU law, including the DSA. However, art. 17(4)(b) and (c) of the CDSM Directive already establish a liability exemption mechanism for OCSSPs, requiring them to make their best efforts to prevent copyright infringement. These specific rules for OCSSPs would leave little room for voluntary investigations by online platforms and thus the application of art. 6 DSA may not be necessary, meaning that it may not be necessary to look for interpretations that would include voluntary activities by OCSSPs.

Nevertheless, it is still possible that some voluntary measures taken by OCSSPs could surpass the required "best efforts" without incurring liability, as long as they stay within the boundaries established by art. 17(7)-(9) of the CDSM Directive. This is especially true due to the dissimilar nature of the instruments in question, namely Regulation vs. Directive, and the potential for disparate national interpretations and implementations of the "best efforts"

[189] VAN DRUNEN, *The Post-Editorial Control Era: How EU Media Law Matches Platforms' Organisational Control with Cooperative Responsibility*, in 12(2) *J. Med. L.,* 166-190, 166, (2020);
[190] QUINTAIS, SCHWEMER, *The Interplay between the Digital Services Act and Sector Regulation: How Special is Copyright?,* in 13(2) *Eur. J. R. Reg.*, 191-217, 198, (2022);

principle in art. 17(4).[191] The issue of multi-layered, geographically dispersed enforcement is not necessarily resolved by the Commission's Guidance, either.

Despite the Commission's identification of scenarios, sectors, and players in relation to which OCSSPs must proactively seek or react to licenses in art. 17(4)(a), and despite copyright being a territorial right, it is still unclear to what extent a platform's obligation should extend. Furthermore, the Commission's guidance suggests that this obligation should be evaluated on a case-by-case basis,[192] which means that legal uncertainty may arise due to the different preventive measures implemented by platforms for copyright-infringing content in various countries, as opposed to the EU-wide obligations under the DSA. Because of the potential complexity of this legal issue, it is critical to clarify the relationship between the DSA and the CDSM Directive during the legislative process. This has practical implications for how platforms should design their content moderation systems while considering both regulations.

In conclusion, arts. 9 and 10 of the DSA, on the orders against illegal content and orders to provide information, outline a regime that may also apply to OCSSPs. While some may argue that art. 8(3) of the InfoSoc Directive already covers specific rules on injunctions, it only applies to intermediaries that are not directly liable for the content they host, which does not include OCSSPs due to their direct liability under art. 17(1) of the CDSM Directive. As a result, the applicability of art. 9 DSA to OCSSPs raises questions about how CJEU case law on fundamental rights, copyright enforcement, and the prohibition on general monitoring would apply to this new reality.[193]

---

[191] LARROYED, *When Translations Shape Legal Systems: How Misguided Translations Impact Users and Lead to Inaccurate Transposition – The Case of "Best Efforts" Under art. 17 DCDSM*, in *SSRN,* 1-32, 20, (2020);

[192] QUINTAIS, *Commission's Guidance on Art. 17 CDSM Directive: The Authorisation Dimension,* in Kluwer Copyright Blog, June 10, 2021, http://copyrightblog.kluweriplaw.com/2021/06/10/commissions-guidance-on-art-17-cdsm-directive-the-author- isation-dimension/;

[193] HUSOVEC, *Injunctions against Intermediaries,* 59; ANGELOPOULOS, *European Intermediary,* 89; ANGELOPOULOS, SENFTLEBEN, *An Endless Odyssey? Content Moderation Without General Content Monitoring Obligations,* in *SSRN,* (2021);

# Chapter 4

# DUE DILIGENCE OBLIGATIONS

## 1. Specific Rules for Each Digital Platform: The Russian Doll System

Through the implementation of the Digital Services Act, the Commission has enacted new horizontal rules to moderate illegal content online, resulting substantially in the end of the cyberspace independence.

While all providers of intermediary services are subject to the most basic rules, additional duties are imposed only on providers falling under different categories, divided according to the type of service offered and the number of users served (Russian dolls). For this purpose, intermediate service platforms are classified into four distinct categories within Section III, which include general intermediate services (Section 1), hosting services (Section 2), and online platforms (Section 3), along with specific rules applicable to very large online platforms (VLOPs) and very large online search engines (VLOSEs) (Section 4), which are subject to the most stringent restrictions within the Regulation.

These rules entail obligations related to transparency and due diligence in content moderation. Furthermore, they also establish harmonized notice-and-action mechanisms, that require the justification of removal decisions, and set forth regulations governing account suspension, while simultaneously granting users the right to challenge content moderation decisions.

### *1.1 Obligations Applicable to All Providers of Intermediary Services*

Considering the difficulty of identifying and establishing communication with certain service providers, it is required, first of all, that service providers designate a sole electronic point of contact for official communication with regulatory bodies within the European Union as well

as with their users. Non-EU-based services are also required to appoint a local legal representative to fulfil their obligations within the jurisdiction.[1]

All digital intermediaries falling within the scope of these regulations are obligated to explicitly disclose to users, through their terms and conditions, any limitations imposed on the utilization of their services.[2] This includes the clarification of their content moderation policies, with specific emphasis on algorithmic decision-making and human review processes. Accordingly, these service providers are also required to exercise diligence, objectivity, and proportionality in the implementation of any restrictions, while duly considering the rights and legitimate interests of all parties involved, including the relevant fundamental rights.

In addition to this, all intermediaries falling under the scope of these regulations (excluding micro-enterprises) are compelled to generate annual reports detailing their content moderation activities.[3] This includes disclosing the number of removal orders received from national authorities or notices received from users or flaggers, the speed of their response, and a comprehensive overview of their proactive content moderation actions (number and type of measures implemented) as well as their complaint-handling activities.

### *1.2 Additional Obligations Applicable to Providers of Hosting Services, Including Online Platforms*

Under Chapter III, Section 2 of the Digital Services Act (DSA), hosting services are subjected to supplementary obligations.
In relation to illegal content, the DSA provides clarification on the requirements for platforms to benefit from liability exemption, notably replacing the previous "notice and takedown" procedure with a "notice and action" mechanism, which hosting service providers are required to establish in order to enable individuals and entities to report instances of allegedly illegal content. This mechanism should be easily accessible, user-friendly, and exclusively permit the submission of notices through electronic means.[4]

[1] Regulation (EU) 2022/2065 (DSA), artt. 11, 12, 13;
[2] Regulation (EU) 2022/2065 (DSA), art.14;
[3] Regulation (EU) 2022/2065 (DSA), art.15;
[4] Regulation (EU) 2022/2065 (DSA), art.16 (1);

In order to trigger the obligations established by the DSA, the Regulation outlines the essential elements that must be included in such notices, eliminating the ambiguity surrounding the concept of "actual knowledge" by the service provider. It establishes that notifications must include not only the reason for the request, but also explicit details regarding the location of the information, specifically the exact URL address, in addition to the requesting party's name, the contact information and a statement indicating good faith.[5] These requirements reflect the established case law of the European Court of Justice (ECJ), which permits injunctions targeting specific content but prohibits general injunctions.
Once all the requirements are met, upon receipt of the notice, the provider is required to promptly send a confirmation of receipt to the sender (including information on any automated processing or decision-making employed) and inform it of its decision. This decision must be made in a timely, diligent, and objective manner, adhering to uniform, transparent, and unambiguous rules, which should encompass robust safeguards aimed at protecting the rights and legitimate interests of all data subjects,[6] and should also be accompanied by an information on all the available solutions for seeking redress.

Moreover, hosting service providers are also obliged to inform users without delay when they choose to remove or disable access to content, as well as when they restrict payments, suspend operations, or terminate either their own services or the user's account. The notification should be given at the latest when the removal takes place and should include a statement providing a detailed explanation for the decision, presented in a clear and comprehensible way. This statement must encompass relevant elements, such as the underlying facts that led to the decision, whether automated means were involved, and a reference to the legal basis or breached terms and conditions of the provider.[7]
Yet, an exception to this information duty exists for deceitful, widely-distributed commercial content, commonly referred to as spam. This exception recognizes the ongoing adversarial nature of spam prevention. In fact, requiring automatic notifications to be sent to spammers whose content has been identified and removed, would inadvertently assist them in enhancing their spambot's efficacy.[8]

[5] Regulation (EU) 2022/2065 (DSA), art.16 (2);
[6] Regulation (EU) 2022/2065 (DSA), recital 52;
[7] Regulation (EU) 2022/2065 (DSA), art.17;
[8] Regulation (EU) 2022/2065 (DSA), art.17 (2);

Lastly, in the event that intermediary service providers have reasonable grounds to believe that serious criminal offense have been committed, it is required for them to promptly notify the relevant national law enforcement or judicial authorities.[9]

### *1.3 Additional Obligations Applicable Only to Providers of Online Platforms*

Excluding micro or small enterprises,[10] the more important changes in the DSA apply to providers of "online platforms", namely hosting providers who, on behalf of a user, store and disseminate information to the public, unless this is a minor and purely ancillary feature, including social media services and online marketplaces.

The DSA seems to adopt a relatively non-interventionist approach. Apart from imposing stricter obligations on very large platforms, there are minimal requirements for content policing on the online platforms. Instead, the new regulations appear to prioritize content protection by granting users the right to file complaints regarding content removal and even to access extrajudicial appeal processes if dissatisfied with the platform's handling of such complaints. This represents a notable shift for many platforms, as they will now be obligated to enhance transparency regarding their moderation procedures and may require substantial additional resources to address subsequent user objections and appeals.

Users of online platforms are now granted additional rights, primarily the right to lodge complaints directly with the online platform and to pursue out-of-court settlements.
Referring to the first point, all online platforms must establish an internal system for handling complaints. This system should allow users, for a minimum of six months, to electronically and free of charge submit complaints against decisions made by the platform, regarding the illegality or violation of general terms and conditions of certain user information. Online platform providers are obligated to promptly notify complainants of their decisions on the disputed information, which are made under the supervision of appropriately qualified personnel, and not solely based on automated processes. This introduces a human oversight requirement that can eventually result in significant costs for platforms. Additionally, providers must also inform complainants about the option of resolving disputes through out-of-court settlements and other available means of redress as outlined in Article 20.

[9] Regulation (EU) 2022/2065 (DSA), art.18;
[10] Regulation (EU) 2022/2065 (DSA), art.19, 29;

In addition, article 21 governs the regulation of out-of-court dispute resolution. This process does not hinder the right of the service recipient to seek legal recourse before a court, as permitted by the applicable law. Service recipients have the freedom to choose an out-of-court dispute resolution body from those certified by the Digital Services Coordinator of their respective Member State, whereas the certification is granted to dispute settlement bodies that meet the requirements outlined in paragraph 3 of Article 21, including impartiality, expertise, independent remuneration, accessibility, effectiveness, and adherence to clear and fair procedural rules.

To enhance the efforts in addressing illicit content, platforms must also work together with designated "trusted flaggers", as recognized by the Digital Services Coordinators on the basis of certain pre-established conditions, who are designed entities which are granted priority in the handling of complaints of illegal content, where illegal content, as defined by the DSA, encompasses any information that, either on its own or in connection with an activity, violates the laws of the EU or its Member States.[11] The explanatory sections of the DSA provide some specific instances of illegal content, such as the sharing of images depicting child sexual abuse.

After determining the role and characteristics of these trusted flaggers, the DSA establishes also some guidelines for online platforms to combat misuse by users who frequently signal clearly illegal content or by individuals or entities (referred to as complainants) who frequently submit notices or complaints that are clearly baseless.[12] These guidelines encompass actions like issuing warnings and temporarily suspending service provision for a reasonable period.

Furthermore, apart from the overall transparency obligations applicable to all intermediary services, online platforms are obligated to meet additional transparency requirements, which include providing reports on the number of dispute resolutions and on the instances of service misuse, as well as providing disclosure on the number of monthly active users in the EU.[13] In light of this approach to transparency, they are prohibited from employing any deceptive techniques, commonly referred to as "dark patterns", which involve manipulating users into

[11] Regulation (EU) 2022/2065 (DSA), art.22;
[12] Regulation (EU) 2022/2065 (DSA), art.23;
[13] Regulation (EU) 2022/2065 (DSA), art.24;

unintended choices through interface design.[14] This prohibition comes as an additional restriction complementing those already previously set forth in the Unfair Commercial Practices Directive[15] and the GDPR,[16] serving the same purposes.

Another key aspect regarding the new due diligence obligations imposed on online platforms relates to advertising and its transparency. Notable restrictions on targeted advertising have been introduced, including prohibiting targeted advertising towards children, and targeting based on sensitive personal data such as ethnicity, political beliefs, sexual orientation, religion, or genetic/biometric data.[17] More in general, there are broader obligations concerning specifically advertising transparency. This includes the requirement to provide meaningful information about why a user is being targeted with a specific advertisement and disclosing the advertiser's identity or sponsorship. In cases where profiling is involved, platform providers must inform users of any available means to modify or adjust the profiling criteria.[18]
Likewise, intermediary service providers utilizing recommender systems must clearly outline in their terms and conditions the primary factors influencing the suggestions or prioritization of information for users, as well as providing options for users to modify or influence those factors.[19]

Importantly, besides the prohibition on targeted advertisements directed towards minors, online platforms must also ensure a strong level of privacy, safety, and security for minors utilizing their services, which entails the implementation of "appropriate and proportionate measures".[20]

Lastly, with regards to online platforms facilitating consumer transactions with traders (e.g., on online marketplaces), it is mandatory for them to ensure the traceability of these traders.

[14] Regulation (EU) 2022/2065 (DSA), art.25;
[15] 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 (Unfair Commercial Practices Directive).
[16] European Data Protection Board, Guidelines 3/2022 on Dark patterns in Social Media Platform Interfaces: How to Recognize and Avoid Them, 14 March 2022;
[17] Regulation (EU) 2022/2065 (DSA), art.26 (3), 28 (2);
[18] Regulation (EU) 2022/2065 (DSA), art.26;
[19] Regulation (EU) 2022/2065 (DSA), art.27;
[20] Regulation (EU) 2022/2065 (DSA), art.28;

This necessitates the collection and verification of their basic information prior to granting them access to the platform. The platform is required to make such information readily available to service recipients through its interface, in a clear, easily accessible, and understandable manner. In the event that the platform becomes aware of any illegal products or services offered by a contractor, it must promptly inform affected consumers.[21]
Similarly, for the purpose of safeguarding consumer interests, the platform is also obliged to structure its services in a manner that allows these traders to fulfil their legal obligations under EU law, which includes, for example, compliance with EU consumer protection rules concerning pre-contractual information.[22]

### *1.4 Additional Obligations for Providers of Very Large Online Platforms (VLOPs) and of Very Large Online Search Engines (VLOSEs)*

Finally, Chapter III, Section 4 of the DSA introduces the most stringent requirements for compliance, accountability, and risk management applicable to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). This is due to their inherent systemic impact in facilitating public debate, economic transactions, and the dissemination of information, opinions, and ideas.
As per Article 33, in order for its rules to be enforced, the concerned online platforms and search engines must possess an average monthly active user base in the European Union that equals or surpasses 45 million. Alternatively, if there is a population change of at least 5% compared to the 2020 population or the population after adjustment through a delegated act, the threshold will be adjusted to 10% of the EU population. The responsibility of designating platforms meeting these criteria lies with the EU Commission.[23] It is noteworthy that these platforms are thus determined quantitatively, distinguishing them from the DMA, which focuses on their gatekeeping function and impact on the internal market.

In addition to the aforementioned obligations, VLOPs and VLOSEs are required to carry out an annual risk assessment which prioritizes systemic risks, including but not limited to the distribution of illegal content, the protection of fundamental rights, civic discourse, electoral processes, and public security. Such assessment should consider deliberate manipulations

[21] Regulation (EU) 2022/2065 (DSA), art.30;
[22] Regulation (EU) 2022/2065 (DSA), art.31;
[23] Regulation (EU) 2022/2065 (DSA), art.33;

occurring within the services of these platforms and the potential adverse effects on minors, encompassing issues such as gender-based violence and harm to physical or mental health.[24] The DSA explicitly underscores that these risks must be mitigated through the adoption of reasonable, proportionate, and effective measures, in accordance with the requirements outlined in article 35.[25] Some examples of these measures may include adapting content moderation and recommendation systems, implementing targeted measures to safeguard the rights of children, enhancing collaboration with trusted flaggers, and establishing cooperation with other platforms through the adoption of codes of conduct and crisis protocols.
A crisis response mechanism is also incorporated within the DSA to address extraordinary circumstances that pose a serious threat to public security or public health within the Union or significant parts thereof.[26]

Among the other requirements, VLOPs and VLOSEs are asked to fulfil enhanced transparency obligations, at their own expense, such as providing more rigorous semi-annual transparency reports, which include also information on the amount of resource dedicated to content moderation.[27]
Pursuant to article 37, VLOPs and VLOSEs are obligated to undergo an annual independent audit, aimed at assessing their compliance with the due diligence obligations stipulated in Chapter III, as well as their adherence to the commitments set forth in codes of conduct.[28] Similarly, in relation to the use of recommendation systems, further transparency obligations ensure that users have access to recommender system options that do not rely solely on profiling,[29] while, as for the online advertising, the DSA imposes additional obligations to establish a repository where recipients have the ability to retrieve information about online advertisements displayed in the preceding year, including the content of the online advertisement, the entity responsible for it, the duration of its display, and the specific target groups it was intended for.[30]
In regard to this last point of view, the enforcement of these provisions may present a considerable obstacle in safeguarding the confidentiality and protection of trade secrets.[31]

[24] Regulation (EU) 2022/2065 (DSA), art.34;
[25] Regulation (EU) 2022/2065 (DSA), art.35;
[26] Regulation (EU) 2022/2065 (DSA), art.36;
[27] Regulation (EU) 2022/2065 (DSA), art.42;
[28] Regulation (EU) 2022/2065 (DSA), art.37;
[29] Regulation (EU) 2022/2065 (DSA), art.38;
[30] Regulation (EU) 2022/2065 (DSA), art.39;
[31] MATHESON, *EU Digital Services Act: What Does it Mean For Online Platforms?*, in *Lexology*, October 19, 2022, https://www.lexology.com/library/detail.aspx?g=740ef9f9-b28e-4597-add0-73c8cf764bab;

Moreover, VLOPs and VLOSEs are additionally compelled to provide regulatory authorities with unfettered access to any pertinent data deemed necessary for evaluating their compliance to the provisions set forth in the DSA.[32] Upon the request of the competent regulatory body, they must facilitate the provision of specific data to duly authorized researchers, for the purpose of identifying and assessing systemic risks associated with the dissemination of illicit or harmful content.

Likewise, both VLOPs and VLOSEs must establish an autonomous compliance function within their organizational structure, which operates independently and reports directly to the board.[33] This compliance function must consist of suitably qualified professionals who possess the necessary expertise and undergo appropriate training. This framework bears resemblance to the concept of a "Data Protection Officer", as stipulated within the purview of the General Data Protection Regulation (GDPR), and has a direct impact on the organizational framework of very large digital platforms, particularly in terms of corporate governance.

Lastly, VLOPs and VLOSEs are required to pay an annual supervisory fee to cover the costs incurred by the Commission in performing its supervisory duties, as mandated by the DSA.[34] The precise amount of this payment must be determined based on the Commission's estimated expenses for supervision. Nonetheless, the individual annual supervisory payment should not exceed 0.05% of the provider's annual worldwide net income.

## 2. Implementation and Enforcement

In Chapter IV, the DSA outlines a comprehensive framework for the implementation, cooperation, sanctions and enforcement of the new obligations set by the Regulation.

[32] Regulation (EU) 2022/2065 (DSA), art.40;
[33] Regulation (EU) 2022/2065 (DSA), art.41;
[34] Regulation (EU) 2022/2065 (DSA), art.43;

*2.1 Competent Authorities and National Digital Services Coordinators (DSCs)*

Taking a distinct approach from the e-Commerce Directive, the DSA first specifically addresses the national authorities responsible for the enforcement of the DSA itself, for the purpose of regulating their competences, coordination and functions. In this regard, the DSA follows the precedent already set by the General Data Protection Regulation (GDPR).[35]

To expedite enforcement by national authorities, each Member State is required to designate one or more competent authorities entrusted with the task of supervising intermediary service providers and enforcing the DSA, among which, one in particular must be appointed as a Digital Services Coordinator (DSC).[36] This is an independent authority with the responsibility of overseeing intermediary service providers within their respective Member State, in an impartial, transparent and timely manner,[37] and with the task of enforcing DSA rules against them. The basic idea behind such figure is to establish a primary point of contact in situations where Member States have multiple competent authorities, serving as a single reference for the Commission and actively participating in the EU cooperation mechanism.

Digital Service Coordinators are granted extensive powers under the Digital Services Act.[38] In terms of investigations, they have the authority to require cooperation from any party, not just intermediaries, possessing relevant information regarding infringements and are endowed with significant powers, such as conducting on-site inspections at premises utilized by intermediaries. During these inspections, they have the right to examine, seize, copy, or obtain information in any format, regardless of the storage medium, if it is linked to a suspected infringement. Furthermore, Digital Service Coordinators are empowered to conduct interviews with staff members of the provider and record their statements.
On the other hand, in terms of enforcement, they enjoy specific prerogatives that include the power to accept binding commitments, to order the cessation of infringements and impose remedies, to levy fines and/or periodic penalty payments, as well as to adopt interim measures. While the majority of these measures primarily target intermediaries, Digital Services Coordinators (DSCs) possess the authority to levy fines or penalty payments also

[35] SAVIN, *The EU Digital Services Act,* 22; SAVOVA, MIKES, CANNON, *The Proposal for an EU Digital Services Act*, 38;
[36] Regulation (EU) 2022/2065 (DSA), art.49;
[37] Regulation (EU) 2022/2065 (DSA), art.50;
[38] Regulation (EU) 2022/2065 (DSA), art.51;

on other entities or individuals who fail to comply, even if they are not intermediaries themselves (e.g., for non-compliance with information requests).
Additional powers are then granted to DSCs in cases where all other measures have proven ineffective, allowing them to compel management to directly intervene in rectifying the situation. In cases where this measure proves ineffective and there is a potential for serious harm or a serious criminal offense that poses a threat to life or safety, DSCs can also request judicial authorities to impose restrictions on access to the service or interface for relevant recipients. Member States are obligated to ensure that the enforcement measures adhere to the applicable constitutional and procedural provisions.

With regard to the penalty system,[39] each EU Member State retains the authority to establish its own rules concerning the penalties for infringements of the DSA within their respective jurisdictions. The aim is to ensure that these penalties are not only effective and proportionate in relation to the gravity and nature of the infringement but also serve as a dissuasive measure to ensure compliance with respect to the Regulation.
From this point of view, the DSA provides guidance by specifying the maximum fines that can be imposed by Member States. In cases of non-compliance with a DSA obligation, the maximum fine allowable is set at 6% of the offender's annual worldwide revenue from the preceding financial year. For scenarios involving the provision of incorrect, incomplete, or misleading information, as well as the failure to respond or rectify such information, and the refusal to undergo an inspection, the highest fine that can be imposed would equal 1% of the annual income or global turnover of the intermediary service provider or the person concerned, based on the financial data from the preceding year. Moreover, the maximum amount of a periodic penalty payment, is capped at 5% of the offender's average daily worldwide revenue.

Finally, Digital Services Coordinators must issue yearly reports regarding their actions[40] and are authorized to receive complaints from individuals against intermediaries,[41] for non-compliance with the obligations outlined in the DSA. Recipients also have the right to pursue compensation from intermediaries for any damage or loss incurred as a result of a violation of the obligations set forth in the DSA.[42]

[39] Regulation (EU) 2022/2065 (DSA), art.52;
[40] Regulation (EU) 2022/2065 (DSA), art.55;
[41] Regulation (EU) 2022/2065 (DSA), art.53;
[42] Regulation (EU) 2022/2065 (DSA), art.54

*2.2 Competences Allocation and Coordination within the European Board for Digital Services ("The Board")*

The Digital Services Coordinator in the Member State where an intermediary service provider's principal establishment is located will assume the role of competent authority to enforce the DSA's provisions on such provider. In the case of non-EU providers offering services within the EU, the place of enforcement is determined by the location of their legal representative. If not even a legal representative is designated, all Member States have the authority to enforce, but a system of notification prevents duplicative proceedings in multiple states.[43]

However, a subsequent amendment to the DSA's original proposal was introduced before the law being enacted, conferring to the European Commission direct and exclusive enforcement jurisdiction over the specific obligations pertaining to VLOPs and VLOSEs, as well as any systemic issues associated with them.[44] Consequently, the European Commission now holds alone the competence to enforce these specific obligations on VLOPs and VLOSEs. Moreover, the Commission is now vested with the power to impose fines reaching a maximum of 6% of the annual global turnover of VLOPs or VLOSEs.

These provisions are highly regarded as they serve to prevent forum shopping and precludes the potential for providers to evade enforcement by selecting jurisdictions with lenient oversight. Furthermore, they are expected to establish a greater degree of consistency in the enforcement of regulations and potentially address the insufficiency of resources or expertise within national supervisory bodies.[45]

In conclusion, the Digital Services Coordinators of various jurisdictions are expected to engage in collaboration with DSCs from other Member States, particularly working together as part of an autonomous advisory group known as the European Board for Digital Services (referred to as the "Board"),[46] whose role is to provide advice and guidance on matters related to the DSA, engage in joint investigations and supervise systemic platforms. The Board will

[43] Regulation (EU) 2022/2065 (DSA), art.56;
[44] Regulation (EU) 2022/2065 (DSA), Ch.4, Sect.4;
[45] AMNESTY INTERNATIONAL, *What the EU's Digital Services Act means for human rights and harmful Big Tech business models,* July 07, 2022, https://www.amnesty.org/en/wp-content/uploads/2022/07/POL3058302022ENGLISH.pdf;
[46] Regulation (EU) 2022/2065 (DSA), art.61;

also work in conjunction with the Commission and the DSCs to further foster effective cooperation and ensure a uniform application of the DSA throughout the European Union.[47]

### *2.3 General Provisions*

The final section of the Regulation's chapter on implementation and enforcement of new obligations lastly introduces some significant provisions applicable on all the providers, encompassing various key aspects.

Primarily, it sets out new rules regarding professional secrecy, aimed at safeguarding the confidentiality of specific information.[48] This provision ensures that sensitive data is protected and not disclosed inappropriately during the enforcement process.

Next, it establishes an information-sharing system, which serves as a crucial mechanism for facilitating effective communication among Digital Services Coordinators, the Commission, and the Board.[49] This system enables the seamless exchange of relevant information and enhances collaboration among these entities involved in the enforcement process.

As a last provision, recipients of intermediary services are granted the prerogative to designate a body, organization, or association to act on their behalf and exercise their rights, given that such entities meet certain requirements duly listed within article 86 of the Regulation.[50] This provision empowers individuals to entrust the representation of their interests to competent entities, ensuring that their rights are effectively protected and advocated for throughout the enforcement proceedings.

[47] Regulation (EU) 2022/2065 (DSA), art.63;
[48] Regulation (EU) 2022/2065 (DSA), art.84;
[49] Regulation (EU) 2022/2065 (DSA), art.85;
[50] Regulation (EU) 2022/2065 (DSA), art.86;

# CONCLUSION

Upon the enactment of the Digital Services Act on November 16th, 2022, online platforms and search engines were granted a period of 3 months to submit a report on the average of monthly active recipients accessing their websites (by February 17th, 2023) and were requested by the Commission to provide notification of the published numbers. Based on these statistics, the Commission, on April 25th, 2023, classified 19 providers as either Very Large Online Platforms (VLOP) or Very Large Online Search Engines (VLOSE).[1] Many of these services are utilized on a daily basis by the average European citizen, including Alphabet's Google Maps, Google Play, Google Shopping, and YouTube, Meta's Facebook and Instagram, Amazon's Marketplace, and Apple's App Store. Other prominent actors within the digital sphere were also included, such as Microsoft's LinkedIn, Booking.com, Pinterest, Snap Inc's Snapchat, TikTok, Twitter and Alibaba's AliExpress, whereas Bing and Google Search were designated as VLOSE.

Subsequent to the Commission's designation decision, such platforms have been granted a 4-month period to ensure compliance with the obligations prescribed by the DSA, which includes conducting and submitting the initial annual risk assessment exercise to the Commission. Accordingly, the designated providers are expected to fully comply with the comprehensive set of new obligations outlined in the DSA by August 25th, 2023, and, in parallel, EU Member States are mandated to grant their Digital Services Coordinators the necessary authority and jurisdiction by February 17th, 2024, the general date of entry into application of the DSA, when the DSA is universally going to become applicable to all entities falling within its scope.[2]

In light of its ambition to establish a primary form of regulation for online activities conducted by digital platforms, the DSA emerges as a true revolutionary act within the field

[1] FRESHELDS BRUCKHAUS DERINGER, *Very large online platforms' and 'very large online search engines' – how are they designated and what does it mean?*, in *The Digital Services Act - Change or Challenge? – Lexology*, May 10, 2023, https://www.lexology.com/library/detail.aspx?g=0fa9ebaf-86d1-433f-bc86-4cb4cd3f3e8b;

[2] Regulation (EU) 2022/2065 (DSA), art.93;

of digital and corporate law, carrying significant implications that have the potential to deeply impact all dynamics of the European digital market, and serving as a cornerstone upon which all subsequent specialized sector-specific laws will be built. It establishes an extensive and comprehensive framework of new rules for digital services within the European Union and, unlike the recently enacted Digital Markets Act, its scope is going to be extended beyond a select few "gatekeeper" companies and their "core platform services". Instead, it is going to encompass all businesses engaging with content published by third parties within the EU, irrespective of their size or location of establishment. Unless exempted as micro or small enterprises, every provider of digital services will consequently be required to adhere to the multiple obligations outlined in the Regulation, facing substantial organizational and operational challenges, in order to achieve compliance and mitigate the risk of potential regulatory penalties.

This law is part of a continuously evolving regulatory framework that originated in Europe with the introduction of the ground-breaking e-Commerce Directive and has developed consistently over the past years, giving rise to discussions about a true "digital constitutionalism".[3] At the legislative level in Europe, one can consider some measures stemming from the constitutional path of the Union, aimed at curbing the power of platforms, in line with the General Data Protection Regulation (GDPR), the Copyright Directive, and the Regulation (EU) 2019/1150 on platform-to-business relations, which aims to regulate the relationships between online platforms and defined "business users". Among these, in addition to the Digital Services Act under analysis, the Digital Markets Act assumes primary importance. It forms part of the same package of laws as the DSA, issued on December 15th, 2020, and its objective is to regulate competition and the market among the major digital giants. The Data Act and the Data Governance Act are also of significant importance as they aim to implement a new data governance framework, with the former seeking to strengthen the protection of personal data, promote transparency and access to data, and the latter pointing to facilitate secure data sharing among organizations, fostering trust in their use.
In addition to these, fundamental proposals for new legislations that will forever change the landscape of the European digital market include also the regulation on cryptocurrencies and decentralized finance, namely the MiCAR Regulation, and on the artificial intelligence, that is the Artificial Intelligence Act.

[3] DE GREGORIO, *The rise of digital constitutionalism in European Union',* in 19(1) *Int. J. Const. L.*, 41-70, 50, (2021);

Regarding the latter, a recent debate has emerged about the scope and extent of the definitions concerning the subjects that will be affected by the legislation, particularly due to recent technological developments that have taken place between late 2022 and early 2023, culminating in the release of the new Chat GPT artificial intelligence model,[4] at the moment considered to be the most powerful AI tool in circulation.

Within this context, the primary objective of the DSA is to enhance the level of accountability for online platforms and intermediaries, through the introduction of new regulations pertaining to transparency, diligent obligations, third-party content liability and an extensive scope of policy areas, including new requirements for online marketplaces and the safeguarding of minors. In this way, the DSA effectively transforms the status of platforms from de facto authorities to legal authorities, aiming to mitigate the potential for abusive exercise of their contractual power and to strengthen the obligations imposed upon them, while concurrently ensuring the safety of end users. Especially with regards to algorithmic transparency, the DSA requires platforms to disclose the functioning of their "recommendation system" and to provide the resultant outcomes, in order to enhance user information and decision-making capabilities.
In doing so, the DSA follows a consolidated jurisprudential trend that has developed in recent years, both within the EU and in national courts, which intends to increasingly highlight the role of digital platforms as responsible entities for all that occurs online. They are required to act as "diligent operators", setting a new level of compliance for the platforms themselves. This approach intends to depart from the primordial liberalism idealized and perpetuated throughout the early years of the new millennium, which allowed for a free and favourable approach to the development of the digital market, and to increasingly bind these platforms to a new form of negligent liability. They are expected to behave essentially as regulatory bodies with substantially public powers, balancing conflicting interests and rights within the digital sphere, in full compliance with the criteria and principles established by major Western constitutions, as well as the Charter of Fundamental Human Rights.

In consideration of this point of view, however, a major threat might be posed unconsciously to the fair and impartial balance of interests between users who perceive their fundamental

[4] METZ, *The New Chatbots Could Change the World. Can You Trust Them?,* in *The New York Times,* December 10, 2022, https://www.nytimes.com/2022/12/10/technology/ai-chat-bot-chatgpt.html;

rights to be infringed upon and the freedom of speech of publishers whose content is accused of being unlawful and infringing upon the rights of third parties.

A greater pressure for the platforms to apply more stringent obligations, in fact, as it may ensure higher standards of protection for online users and competing businesses, could also increase the risk of an excessive monitoring on what is published online, as well as of arbitrary and casual restrictions on the freedom of speech, encouraging the removal of contents, even when not strictly necessary, in order to avoid severe penalties or unfavourable legal regimes, in case of non-compliance with the applicable legislation.[5] As a consequence, the more rigorous a practice of content monitoring and removal by online intermediaries is, the greater the risk of a "private censorship" could be,[6] giving rise to a new form of private jurisdiction, put in place on the part of those platforms that increasingly seem to take on the role of real independent courthouses.[7]

It is therefore worth considering the convenience of perpetuating the same approach pursued by local and supranational courts in recent years, in the perspective of increasing private platforms accountability and reducing the responsibility of competent authorities. Even with the establishment of new dedicated authorities to oversee platforms compliance with all the new obligations set forth in this regulation, the underlying problem of discretionary decisions made by digital platforms would still in fact persist.[8] These private authorities, despite being tasked with balancing all relevant interests in full compliance with legal and constitutional constraints, would still be driven by purely private interests, therefore being inadequate in ensuring a fair and impartial balance of interests for all parties involved.

The decision-making freedom of individual market operators, burdened by the public responsibility to safeguard the interests of all involved parties, not only risks failing to achieve the intended goal of enhancing online platforms accountability, with the possibility of platforms leaning towards excessive content removal and restrictions on third-party activities to avoid the risk of new sanctions or civil liabilities, but also poses potential harm, as it places digital market operators in front of a dilemma: whether to comply with the new rules stipulated by the Regulation, incurring significant managerial and organizational costs

---

[5] BASSINI, *Fundamental rights*, 183;

[6] CORNILS, *Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries*, in *Governing Platforms*, 2020, https://algorithmwatch.org/de/wp-content/uploads/2020/05/Governing-Platforms-legal-study-Cornils-May-2020-AlgorithmWatch.pdf; MONTI, *Privatizzazione della censura e internet platforms: la libertà di espressione e i nuovi censori dell' agorà digitale*, in 1 *Riv. It. Inf. Dir.*, 2019, 35-51, *ivi* 44; BASSINI, *Fundamental Rights*, 188;

[7] BALKIN, *Free Speech,* 2295;

[8] FROSIO, GEIGER, *Taking Fundamental Rights Seriously in the Digital Service Act's Platform Liability Regime*, in *Eur. L. J.,* 1-44, 23, (2022);

to meet the legislative obligations, or to operate outside the law, disregarding the new provisions established by the DSA and risking being targeted by regulatory authorities, along with the resulting consequences of accountability and negative publicity. Although the legislative text refers several times to the principles of proportionality and reasonableness and excludes micro-enterprises that do not reach a certain user threshold from the restrictions, it is important to acknowledge that an increase in administrative and organizational costs due to new stricter obligations, within the corporate structure of individual companies, could still make certain commercial activities more burdensome. This could further complicate the expansion into the digital market for intermediaries that do not reach significant sizes and, paradoxically, it could even enhance the commercial power of a few very large digital platforms that, despite facing a stricter regime, may still have greater ease in bearing the costs associated with a full compliance under the new regulatory framework.

Moreover, the enforcement of new limitations established within the DSA, currently lacks clarity, leaving room for potential disputes and challenges regarding specific obligations such as, for example, determining whether a particular practice qualifies as a "Dark Pattern" and how such practice can be distinguished from an acceptable activity to promote businesses interests, or ensuring that machine learning algorithms remain actually within the boundaries set by the DSA, preventing inadvertent inferences with sensitive data, such as someone's political opinion or health status, when delivering targeted advertisements.
Additionally, there are some concerns also regarding the transparency of recommender systems, whereas malicious actors could eventually manipulate the systems by strategically using keywords that they know will be favoured by the algorithm, and regarding what information can be considered sufficient to identify a user as a child, thus triggering the prohibition of targeted advertising based on profiling.
All of this, without considering the arduous challenge posed by the complex coordination with respect to all other sector-specific laws, ranging from the GDPR to the emerging AI Act, which are inevitably going to raise questions about harmonization and consistency. It is therefore essential to establish how these laws will complement and coexist with each other, considering their shared objectives in safeguarding user rights, privacy, and online safety.

For these and many other questions, that are going to arise in the coming years, we can only await for future developments that will place at their core both the role of the new public authorities, established to exercise functions and powers that are entirely innovative

compared to the past, and of the digital service intermediaries themselves, which, in addition to being closely scrutinized by regulators, will need to demonstrate their ability to sufficiently ensure the respect and promotion of social interests, while conforming to the standards and parameters imposed by the legislator.

Should this approach prove ultimately successful, this will pave the way for a new era in the European digital market, wherein businesses will operate and thrive in an atmosphere of legal certainty, and citizens will be shielded from the risks and pitfalls that have proliferated since the beginning of this millennium, violating even the most basic rights that had been taken for granted in the majority of Western countries since the end of World War II.

# BIBLIOGRAPHY


- ADLER, *The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship,* in 20(1) *Journ. L. Pol.*, 231-265, (2011);
- ALBERTINI, *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, in 4 *L. Med. Work. Pap. Ser.*, (2020);
- ALLEGRI, *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti, in 26(1-2) Inf. Dir., 2017, 69;*
- AMMORI, *The "New" New York Times: Free Speech Lawyering in the Age of Google and Twitter*, in 127 *Harv. L. Rev.*, 2259-2295, (2014);
- ANGELOPOULOS, *European Intermediary Liability in Copyright. A Tort-Based Analysis*, in 39 *Inf. L. Ser.*, (2016);
- ANGELOPOULOS, *On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market*, in *SSRN,* 1-47, (2017);
- ANGELOPOULOS, SENFTLEBEN, *An Endless Odyssey? Content Moderation Without General Content Monitoring Obligations,* in *SSRN,* (2021);
- ARROYO AMAYUELAS, *¿La responsabilidad de los intermediarios en internet: puertos seguros a prueba de futuro?*, in 12(1) *Cuad. Der. Trans.*, 808-837, (2020);
- ASTONE, *La responsabilità del prestatore di servizi della società di informazione nella direttiva 2000/31/CE*, in 2 *Eur. Dir. Priv.*, 2003, 431ss.;
- BAISTROCCHI, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in 19(1) *S. Cl. H. Tech. L. J.*, 111-130, (2003);
- BALKIN, *Free Speech and Hostile Environments*, in 99(8) *Col. L. Rev.*, 2295-2320, (1999);
- BALKIN, *Old-School/New-School Speech Regulation*, in 128(8) *Harv. L. Rev.*, 2296-2342, (2014);
- BALKIN, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation,* in 51 *Univ. Calif. Dav. L. Rev.*, 1149-1210, (2018);
- BAROCAS, HOOD, ZIEWITZ, *Governing Algorithms: A Provocation Piece,* in *SSRN,* 1-12, (2013);

- BASSINI, *Fundamental rights and private enforcement in the digital age*, in 25 *Eur. L. Jour.*, 182-197, (2019);
- BASSINI, *Mambo Italiano: The Perilous Italian way to ISP Liability,* in *Fund. R. Prot. On.,* 84-114, 100, (2020);
- BELLI, FRANCISCO, ZINGALES, *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police*, in BELLI, ZINGALES (eds), *Platforms Regulation*, *How Platforms are regulated and how They regulate us,* FGV Direito Rio, Rio de Janeiro, 2017;
- BELLI, VENTURINI, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation,* in 5(4) *Int. Pol. Rev.,* 1-17, (2016);
- BENJAMIN, *Algorithms and Speech,* in 161(6) *Uni. Pen. L. Rev.*, 1445-1494, (2013);
- BENSOUSSAN, *Internet Aspect Juridique,* Hermes, Paris, 1998;
- BENTATA, *COVID 2019 pandemic: a true digital revolution and birth of a new educational era, or an ephemeral phenomenon?*, in 25(1) *Med. Educ. On.,* (2020);
- BERBERICH, SEIP, *Der Entwurf des Digital Services Act,* in 1 *Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR- Prax)*, (2021);
- BERMAN, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation,* in 71 *Un. Col. L. Rev.,*1263-1310, (2000);
- BETZU, *Libertà di espressione e poteri privati nel cyberspazio*, in 1 *Dir. Cost. – Riv. Quad.*, 2020, 117;
- BLACK, *Constitutionalising Self-Regulation,* in 59(1) *Mod. L. Rev.*, 24-55, (1996);
- BLOCH-WEHBA, *Automation in Moderation*, in 53 *Corn. Int. L. Journ.* 41-96*,* (2020);
- BOCCHINI, *La Responsabilità Civile degli Intermediari del Commercio Elettronico,* Edizioni Scientifiche Italiane, Napoli, 2003;
- BOCCHINI, *La Responsabilità extracontrattuale del provider*, in VALENTINO (EDT.), *Manuale di diritto dell'informatica*, Edizioni Scientifiche Italiane, Napoli, 2016, 540ss.;
- BOCCHINI, *La Responsabilità di Facebook per la mancata rimozione di contenuti illeciti*, in 3 *Giur. it.*, 2017, 632;
- BOSCO. CREEMERS. FERRARIS, GUAGNIN, KOOPS*, Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities*, in GUTWIRTH, LEENES, DE HERT (EDT.), *Reforming European data protection law*, Springer Science-Business Media B.V., Dordrecht, 2015;

- BRIDY, *The Price of Closing the "Value Gap": How the Music Industry Hacked EU Copyright Reform*, in 22(2) *Vand. j. ent. & tech. l.*, 323-358, (2020);
- BUGIOLACCHI, *Principi e Questioni Aperte In Materia di Responsabilità Extracontrattuale dell'Internet Provider. Una Sintesi di Diritto Comparato,* in *Dir. Inf.,* 2000, 856 ss.;
- BUGIOLACCHI *L., Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti dell'attuale approccio case by case*, *(Commento a Trib. Milano 25 Maggio 2013 ord.)*, in 78(6) *Resp. civ. prev*., 2013, 1997;
- BUGIOLACCHI, *Ascesa e declino della figura del "provider attivo"? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in 4 *Resp. Civ. Prev.*, 2015, 1261-1270;
- BUITEN, DE STREEL, PEITZ, *Rethinking Liability Rules for Online Hosting Platforms*, in 28(2) *Int. J. L. Inf. Tech.,* 139-166, (2020);
- BUITEN, *The Digital Services Act From Intermediary Liability to Platform Regulation,* in 12 *JIPITEC*, 361-380, (2021);
- BURRELL, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, in *B. D. & Soc.*, 1-12, (2016);
- BUSCH, MAK, *Putting the Digital Services Act in Context: Bridging the Gap Between EU Consumer Law and Platform Regulation,* in 10 *J. Eur. Cons. Mar. L.*, 109-115, (2021);
- CARROLL, *The pyramid of corporate social responsibility: to- ward the moral management of organizational stakeholders,* in 34(4) *Business Horizons*, 39-48, (1991);
- CARVALHO, ARGA E LIMA, FARINHA, *Introduction to the Digital Services Act, Content Moderation and Consumer Protection*, in 3(1) *Rev. Dir. Tec.,* 71-104, (2021);
- CASSANO, BUFFA, *Responsabilità del Content e dell'Host Provider,* in *Corr. Giur.,* 2003;
- CAUFFMAN, GOANTA, *A New Or- der: The Digital Services Act and Consumer Protection*, in 12(4) *Eur. J. R. Reg.*, 758-774, (2021);
- CELESTE, *Digital Constitutionalism. A New Systematic Theorisation*, in 33/1 *Int. Rev. of Law*, *Comp. and Tech.*, 76-99, (2019);
- CHARLES DE SECONDAT, *L'esprit des loi*, Barrillot & fils, Geneva, 1748;
- COLANGELO, MAGGIOLINO, *ISPs' copyright liability in the EU digital single market strategy,* in 26(2) *Int. J. L. Inf. Tech.*, 142-159, (2018);

- COLARUOTOLO, *Facebook e hyperlinking illecito degli utenti. L'inerzia ingiustificata del prestatore di servizi è fonte di responsabilità civile e risarcitoria, nota a Trib. Roma 15.02.2019, RTI v. Facebook-Ponzone,* in *Riv. dir. ind*., 2019, 328;
- COULDRY, MEJIAS., *The costs of connection: how data is colonizing human life and appropriating it for capitalism*, Stanford University Press, Stanford, 2019;
- CRANE, MATTEN, MOON, *Corporations and Citizenship*, Cambridge University Press, Cambridge, 2008;
- CUSTERS, CALDERS, SCHERMER, ZARSKY, EDS., *Discrimination and Privacy in the Information Society*, Springer, Berlin, 2013;
- DE GREGORIO*, From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society*, in 11(2) *Eu. J. Leg. Stud.* 65-103, (2019);
- DE GREGORIO, *The rise of digital constitutionalism in European Union',* in 19(1) *Int. J. Const. L.*, 41-70, (2021);
- DELMASTRO, NICITA, *Big data. Come stanno cambiando il nostro mondo,* Bologna, Mulino, 2019, 37;
- DE STREEL, HUSOVEC, *The e-commerce Directive as the cornerstone of the Internal Market - Assessment and Options for Reform,* European Parliament, Luxembourg, 1-52, (2020);
- DEVINS, FELIN, KAUFFMAN, KOPPL, *Law and Big Data,* in 27(2) *Corn. J. L. Pub. Pol.*, 357-413, 2017;
- DI CIOMMO, *Internet, Diritti della Persona e Responsabilità Aquiliana del Provider,* in *Dan. Resp.*, 1999, 754;
- DI SALVO, *Deplatforming, l'attacco a Capitol Hill e la nuova sfera pubblica privatizzata*, in 18(3) *St. Cult., Riv. Quad.,* 2021, 449;
- EGGERS, GARRO, GRIMMER, *No evidence for systematic voter fraud: A guide to statistical claims about the 2020 election,* in 118(45) *Proc. Nat. Ac. Sci.*, 1-7, (2021);
- FACCI, *La responsabilità dei providers*, in ROSSELLO, FINOCCHIARO, TOSI*, Commercio elettronico*, Giapichelli, Torino, 2007;
- FLORIDI, TADDEO, *The Moral Responsibilities of Online Service Providers,* in 31 *L., Gov. a. Tech. Ser.*, 13-43, (2017);
- FLORIDI, *The fight for digital sovereignty: what it is, and why it matters, especially for the EU*, in 33(3) *Phil. & Tech.*, 369–378, (2020);

- FLORIDI, *The European Legislation on AI. A Brief Analysis of its Philosophical Approach*, in 34(2) *Phil. and Tech.*, 215-22, (2021);
- FLORIDI, *Trump, Parler, and Regulating the Infosphere as Our Commons,* in 34 *Phil. & Tech.*, 1-5, (2021);
- FROSIO, GEIGER, *Taking Fundamental Rights Seriously in the Digital Service Act's Platform Liability Regime*, in *Eur. L. J.,* 1, (2022);
- FRYDMAN, RORIVE, *Regulating Internet Content Through Intermediaries in Europe and the USA*, in 23(1) *Z. f. Recht.*, 41-60, (2002);
- GAMBINI, *Le responsabilità civili dell'Internet service provider*, Edizioni Scientifiche Italiane, Napoli, 2006;
- GAMBINI, *Gli hosting providers tra doveri di diligenza professio- nale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in 2 *Cost. it.*, 2011;
- GEDDES, *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, in 43(4) *Col. Journ. L. A.*, (2020);
- GRIMMELMANN, *Virtual World Feudalism,* in 118 *Y. L. Jour. Poc.*, 126-130, (2009);
- GRIMMELMANN, *Speech Engines,* in 98 *Min. L. Rev.,* 868-952, (2014);
- GROZDANOVSKI, *In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law*, in 58 *Com. Mar. L. Rev.*, 99-136, (2021);
- GUERINI, *Fake New e Diritto Penale: la Manipolazione Digitale del Consenso nelle Democrazie Liberali,* Giapichelli, Torino, 2020;
- HERDEN,, ALLIU,, CAKICI, *ET AL.*, *Corporate Digital Responsibility*. in 29 *NachhaltigkeitsManagementForum*, 13-29, (2021);
- HINDS, WILLIAMS, JOINSON, *"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica Scandal*, in 143 *Int. J. Hum. -Comp. Stud.,* (2020);
- HOBOKEN, *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines*, in 27 *Inf. L. Ser.*, (2012);
- HOLZNAGEL, *Responsibility for Harmful and Illegal Content as Well as Free Speech on the Internet in the United States of America and Germany,* in ENGEL, KELLER (EDS), *Governance of Global Networks in Light of Differing Local Values,* Nomos, Baden Baden, 2000;
- HOLZNAGEL, *Platform Liability for Hate Speech & the Country of Origin Principle: Too Much Internal Market?*, in 21(4) *Comp. L. Rev. Int.,* 103-109, (2020);

- HUSOVEC, *Injunctions aganist intermediaries in the European Union. Accountable but not liable?*, Cambridge University Press, Cambridge, 2017;
- HUSOVEC, *How Europe Wants to Redefine Global Online Copyright Enforcement*, in 16 *TILEC Discus. Pap.,* (2019);
- IANNARELLI*, La regolazione privatistica delle relazioni di mercato nell'attuale contesto*, in *Riv. Cri. di Dir. Priv.*, 297, (2020);
- JOHNSON, POST, *Law and Borders: The Rise of Law in Cyberspace,* in 48(5) *Stan. L. Rev.*, 1367-1402, (1996);
- JULIA-BARCELO, *Liability for Online Intennediaries: A European Perspective*, in 12 *E.I.P.R.*, 1-9, (1998);
- MACAVANEY ET AL., *Hate Speech Detection: Challenges and Solution*, in 14(8) *Pl. O.*, 1-16, (2019);
- KLONICK, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in 131 *Harv. L. Rev.*, 1599-1670, (2018);
- KOSSEFF, *The Twenty-Six Words That Created the Internet*, Cornell University Press, London, 2019;
- KOTLER, HOLLENSEN, OPRENSIK, *Social media marketing. Marketer nella rivoluzione digitale*, Hoepli, 2019;
- LARROYED, *When Translations Shape Legal Systems: How Misguided Translations Impact Users and Lead to Inaccurate Transposition – The Case of "Best Efforts" Under art. 17 DCDSM*, in *SSRN,* 1-32, (2020);
- LOBEL, *The Law of the Platforms,* in 101 Min. L. Rev., 87-166, (2016);
- LYNSKEY, *Regulation by Platforms: The Impact on Fundamental Rights*, in BELLI, ZINGALES (eds), *Platform Regulations How Platforms are Regulated and How They Regulate Us*, FGV Direito Rio, Rio de Janeiro, 2017;
- MAIETTA, *Il sistema delle responsabilità nelle comunicazioni via internet,* in CASSANO, CIMINO (EDT.), *Diritto dell'Internet e delle nuove tecnologie telematiche,* CEDAM, Padova, 2009, 511;
- MANSELL, JAVARY, *Emerging Internet Oligopolies: A Political Economy Analysis*, in MILLER, WARREN J SAMUELS EDS., *An Institutionalist Approach to Public Utilities Regulation*, Michigan State University Press, Michigan, 2002, 162-201;
- MENKES, *Freedom of speech in the age of digitalization - Opportunities and* threats, in *The Eu. Un. Dig. Sing. Mar. Eu.'s Dig. Transf.*, 35-62, (2022);

- METZGER ET AL., *Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law – Comment of the European Copyright Society,* in *SSRN*, 1-21, (2020);
- MILLWARD**,** *Private and Public Enterprise in Europe: Energy, Telecommunications and Transport, 1830–1990,* Cambridge University Press*,* Cambridge, 2008;
- MITTLESTADT ET AL., *The Ethics of Algorithms: Mapping the Debate,* in *B. D. & Soc.*, 1-21, (2016);
- MOAZED, JOHNSON, *Modern Monopolies: What It Takes to Dominate the 21st Century Economy,* St Martin's Press, New York, 2016;
- MONTI, *Privatizzazione della censura e internet platforms: la libertà di espressione e i nuovi censori dell' agorà digitale*, in 1 *Riv. It. Inf. Dir.*, 2019, 35;
- NEMITZ, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, in *Phil. Trans. of the R. Soc. A*, (2018);
- NUCCIO, GUERZONI, *Big Data: Hell or Heaven? Digital Platforms and Market Power in the Data-Driven Economy*, in 23(3) *Comp. & Ch.,* 312-328, (2019);
- PALAZZOLO, *Il "Domain Name",* in 2 *N. Giur. Civ. Com.,* II, 2000, 168;
- PANKOKE, *Von der Presse-zur Providerhafthung*, C.H. Beck, Munchen, 2000;
- PASCUZZI, *Il Diritto nell'Era Digitale,* Il Mulino, Bologna, 2010;
- PASQUALE, *The Black Box Society. The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge, 2015;
- PERLINGIERI, *Profili civilistici dei social networks*, Edizioni Scientifiche Italiane, Napoli, 2014;
- PETRUSO, *La responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a confronto*, Giappichelli, Torino, 2019, 140;
- POELL, NIEBORG, VAN DIJCK, *Platformisation*., in 8(4) *Int. Pol. Rev.*, (2019);
- PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service provider,* in 7(1) *Dan. Resp.*, 2002, 5-10;
- POSNER, WEY., *Radical marktets. Uprooting capitalism and democracy for a just society*, Princeton University Press, Princeton, 2018;
- QI, EDGAR-NEVILL, *Social networking searching and privacy issues*, in 16(2) *Inf. Sec. Tec. Rep.*, 74-78, (2011);
- QUINTAIS, SCHWEMER, *The Interplay between the Digital Services Act and Sector Regulation: How Special is Copyright?,* in 13(2) *Eur. J. R. Reg.*, 191-217, (2022);

- REMMEL, *Scientists want virtual meetings to stay after the COVID pandemic,* in 591 *Nat.,* 185-186, (2021);
- RICCIO, *Profili di responsabilità civile dell'Internet Provider*, in STANZIONE, *Quaderni del Dipartimento di Diritto dei rapporti civili ed economici nei sistemi giuridici contemporanei,* Dipartimento di diritto dei rapporti civili ed economici nei sistemi giuridici contemporanei, Salerno, 2000;
- RICCIO, *La Responsabilità Civile degli Internet Providers,* Giapichelli Editore, Torino, 2002;
- RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in 3 *Riv. dir. civ*., 2020, 652;
- RIIS, SCHWEMER, *Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation*, in 22(7) *Journ. Int. L.*, 1-21, (2019);
- RIORDAN, *The Liability of Internet Intermediaries*, OUP, Oxford, 2016;
- ROBERTO, ZINI, FELICI, RAO, NOUSSAN, *Potential Benefits of Remote Working on Urban Mobility and Related Environmental Impacts: Results from a Case Study in Italy*, in 13(1) *Ap. Sci,*, (2023);
- ROGERS*, Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media,* in 35(3) *Eu. J. Com.*, 213–229, (2020);
- RODRÍGUEZ DE LAS HERAS BALLELl*, Il paradigma della responsabilità degli intermediari digitali nel contesto di una economia di piattaforme (platform economy*), in 1 *Dir. Com. Sc. Int.*, 2018, 203ss;
- ROSATI, *Material, personal and geographic scope of online intermediaries' removal obligations beyond Glawischnig-Piesczek (C-18/18) and defamation*, in 41(11) *Eur. Int. Prop. Rev.*, 672-682, (2019);
- ROSEN, *Who Decides? Civility v. Hate Speech on the Internet,* in 2(13) *A. Bar Ass.: Ins. L. & Soc.*, (2013);
- SAVIN, *The EU Digital Services Act: Toward a More Responsible Internet,* in 24(7) *The J. of Int. Law,* 15-25, (2021);
- SAVIOZZI, *Imprenditorialità*, Egea-Pixel, 2017;
- SAVOVA, MIKES, CANNON, *The Proposal for an EU Digital Services Act: A closer look from a European and three national perspectives: France, UK and Germany,* in 22(2) *Comp. L. Rev. Int.*, 38-45, (2021);

- SCHERER, PALAZZO, *The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy,* in 48 *Journal of Management Studies*, 899-931, (2011);
- SCHNEIDER, *<<Verificabilità>> del trattamento automatizzato dei dati personali e tutela del segreto commerciale nel quadro europeo,* in 2 *Merc. concorr. regole,* 2019, 327;
- SCOLA, *Digital Services Act: occasioni mancate e prospettive future nella recente proposta di regolamento europeo per il mercato unico dei servizi digitali***,** in 1 *Contr. Imp. Eur.,* 2022;
- SCUDERI, *La responsabilità dell'Internet Service Provider alla Luce della Giurisprudenza della Corte di Giustizia Europea, causa c-610/15, 14 giugno 2018,* in *Dir. Mer. Tec.,* 2018*,* 1-16;
- SICA, *Giurisprudenza nazionale ed europea e frammentazione legislativa della responsabilità civile del provider*, in MANCALEONI, POILLOT (EDT.), *National Judges and the Case Law of the court of Justice of the European Union*, Romatre-press, Roma, 2021;
- SIANO, *La sentenza Scarlet della Corte di Giustizia: punti fermi e problemi aperti*, in PIZZETTI, *I diritti nella "rete" della rete. Il caso del diritto di autore*, Torino, Giappichelli, 2011, 81-96;
- SICA, ZENO-ZENCOVICH, *Manuale di Diritto dell'Informazione e della Comunicazione,* CEDAM, Torino, 2007;
- SPOERRI, *On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market*, in 10(2) *J. Int. Prop. Inf. Tech. E-Com. L.*, 173-186, (2019);
- SUGANTHI, ET AL., *Deep learning model for deep fake face recognition and detection,* in 8 *P. Comp. Sci.*, 1-20, (2022);
- SUZOR, *Lawless: The Secret Rules That Govern Our Digital Lives*, Cambridge University Press, Cambridge, 2019;
- TERESZKIEWICZ, *Digital Platforms: Regulation and Liability in the EU Law*, in 6 *Eur. Rev. Priv. L.,* 903-920, (2018);
- TEUBNER, *Societal Constitutionalism: Alternative to State-Centred Constitutional Theory?,* in, JOERGES, SAND, TEUBNER EDS., *Transnational Governance and Constitutionalism,* Hart Publishing, London, 2004, 3-28;
- TEUBNER, *The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors,* in 69(3) *Mod. L. Rev.*, 327-346, (2006);

- TOMMASI, *Protocolli TCP/IP e Problematiche Contrattuali di Accesso alla Rete Internet,* in SIROTTI GAUDENZI (EDT.), *Trattato Breve di Diritto della Rete. Le Regole di Internet*, Maggioli Editore, Rimini, 2001;
- TOSI, *Le Resposnsabilità Civili,* in TOSI, (EDT.), *I Problemi Giuridici di Internet. Dall'E-Commerce all' e-business,* Giuffrè Francis Lefebvre, Milano, 2003;
- TOSI, *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca. a margine dei recenti casi "Google Suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale*, in 61(1) *Riv. Dir. Ind.*, 2012, 44;
- *TOSI, Responsabilità civile per fatto illecito degli Internet Service Provider tra tipizzazione normativa ed evoluzione tecnologica, in AA. VV., Digesto Discipline Privatistiche, sez. civ., Decimo Aggiornamento, UTET, Torino, 2016, 688;*
- TOSI, *Responsabilità civile degli hosting provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilita' ex post***,** in 1 *Il Dir. Af.,* 2020, 1;
- TURILLI, FLORIDI, *The Ethics of Information Transparency*, in 11(2) *Eth. Inf. Tech.*, 105-112, (2009);
- TRUDEL, *Les Responsibilités dans Cyberspace,* in UNESCO, ECONOMICA, *Les Dimensions Internationales du Droit du Cyberspace,* Paris, 2000, 235-269;
- VAN DIJCK, *Datafication, Dataism and Dataveillance. Big Data between Scientific Paradigm and Ideology,* in 12(2) *Surv. and Soc.*, 197-208, (2014);
- VAN DRUNEN*, The Post-Editorial Control Era: How EU Media Law Matches Platforms' Organisational Control with Cooperative Responsibility*, in 12(2) *J. Med. L.,* 166-190, (2020);
- VAN HOBOKEN, *Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU*, in 13 *Int. J. Com. L. Pol.,* 1-21, (2009);
- VEALE, EDWARDS, *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in 34 *Comp. L. & Sec. Rev.*, 398-404, (2018);
- WEBER, STAIGER, *Cloud Computing: A cluster of complex liability issues,* in 20(1) *Eur. J. Cur. Leg. Is.*, 2014;
- WIELSCH, *Private Law Regulation of Digital Intermediaries*, in 2 *Eu. Rev. of Priv. Law*, (2019);

- WILMAN, *Het voorstel voor de Digital Services Act: Op zoek naar nieuw evenwicht in regulering van onlinediensten met betrekking tot informatie van gebruikers,* in *Ned. Tijds. V. Eur. Rec,* 27-36, (2021);
- WU, *Collateral Censorship and the Limits of Intermediary Immunity*, in 87 *Notr.. D. L. Rev.*, 293-350, (2011);
- ZARSKY, *Transparent Predictions,* in 4 *Uni. Illin. L. Rev.,* 1503-1570, (2013);
- ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete,* in *Riv. Trim. Dir. Proc. Civ.*, 2018, 411;


# SITOGRAPHY


- AMNESTY INTERNATIONAL, *What the EU's Digital Services Act means for human rights and harmful Big Tech business models,* July 07, 2022, https://www.amnesty.org/en/wp-content/uploads/2022/07/POL3058302022ENGLISH.pdf;
- ANDREWS, *We Need European Regulations for Facebook and Google,* in *London School of Economics blog*, December 13, 2016, https://blogs.lse.ac.uk/medialse/2016/12/13/we-need-european-regulation-of-facebook-and-google/;
- ANGELOPOULOS, *CJEU in UPC Telekabel Wien: A totally legal court order...to do the impossible*, in *Kluwer Copyright Blog*, 2014, https://copyrightblog.kluweriplaw.com/2014/04/03/upc-telekabel-wien/;
- APA, FRIGERIO, MONTINARI, *The Court of Cassation rules on the active and passive hosting providers debate in the RTI v. Yahoo! Case,* in *Portolano Cavallo inform@,* 5 April 2019, https://portolano.it/en/newsletter/litigation-arbitration/the-court-of-cassation-rules-on-the-active-and-passive-hosting-providers-debate-in-the-rti-v-yahoo-case;
- BARATA, *Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act*, https://cdt.org/insights/positive-intent-protections-incorporating-a-good-samaritan-principle-in-the-eu-digital-services-act/;

- BARLOW, *A Declaration of Independence of the Cyberspace,* in *Electronic Frontier Foundation*, February 8, 1996, www.eff.org/cyberspace-independence;
- BORGOMANERI, SIGNORELLI, *Il recepimento della direttiva Copyright in Italia: ora è tempo di responsabilizzare,* in *Agenda Digitale,* 03 August 2021, https://www.agendadigitale.eu/cultura-digitale/il-recepimento-della-direttiva-copyright-in-italia/;
- BUCHANAN ET AL., *How a Pro-TrumpMob Stormed the US. Capitol,* in *N.Y. TIMES*, January 7, 2021, https://www.nytimes.com/interactive/2021/01/06/us/trump-mob-capitol-building;
- CHELIOUDAKIS, *The Glawischnig-Piesczek v Facebook case: Knock, knock. Who's there? Automated filters online*, in *KU Leuven CiTiP*, 2019, https://www.law.kuleuven.be/citip/blog/the-glawischnig-piesczek-v-facebook-case-knock-knock-whos-there-automated-filters-online/;
- CICCONE, *Deplatforming» Trump: la giusta decisione di Facebook e Twitter di bloccare gli account del presidente uscente*, in *Valigia Blu*, January 9, 2021, https://www.valigiablu.it/deplatforming-trump-facebook-twitter/;
- CORNILS, *Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries*, in *Governing Platforms*, 2020, https://algorithmwatch.org/de/wp-content/uploads/2020/05/Governing-Platforms-legal-study-Cornils-May-2020-AlgorithmWatch.pdf;
- Council of Europe Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World,* 72, 2014, https://book.coe.int/en/commissioner-for-human-rights/7321-pdf-the-rule-of-law-on-the-internet-and-in-the-wider-digital-world.html;
- CUNIBERTI, *Potere e libertà nella rete*, in *Media Laws*, October 24, 2018, https://www.medialaws.eu/rivista/potere-e-liberta-nella-rete/;
- DANIEL, *Elon Musk's $44 billion Twitter purchase is 'one of the most overpaid tech acquisitions in history,' Wedbush's Dan Ives says. Twitter's fair value is only $25 billion*, in *Fortune*, October 27, 2022, https://fortune.com/2022/10/27/elon-musk-twitter-purchase-most-overpaid-tech-history-dan-ives-wedbush/;
- Directorate-General for Internal Policies, *Providers Liability: from the e-Commerce Directive to the Future,* 2017, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf;

- European Audiovisual Observatory, *Unravelling the Digital Services Act Package,* 11, October 21, 2021, https://www.obs.coe.int/en/web/observatoire/press-releases-2021/-/asset_publisher/alYLDl7HvAtD/content/unraveling-the-digital-services-act-package;
- EUROPEAN COMMISSION, *Public consultation on the regulatory environment for platforms, online intermediaries and the collaborative economy,* 9, January 26, 2016, https://digital-strategy.ec.europa.eu/en/library/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud;
- EUROPEAN COMMISSION, *Code of conduct on countering illegal hate speech online,* June 30, 2016, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en;
- EUROPEAN DIGITAL RIGHTS (EDRI), *More responsibility to online platforms – but at what cost?,* July 19, 2019, https://edri.org/our-work/more-responsibility-to-online-platforms-but-at-what-cost/;
- FERRARIS, *Digital Service Act approvato dal Parlamento europeo: le novità sugli intermediari online*, in *Il Quotidiano Giuridico,* July, 13, 2022, https://www.altalex.com/documents/2022/07/13/digital-service-act-approvato-parlamento-europeo-novita-intermediari-online;
- FRESHELDS BRUCKHAUS DERINGER, *Very large online platforms' and 'very large online search engines' – how are they designated and what does it mean?*, in *The Digital Services Act - Change or Challenge? – Lexology*, May 10, 2023, https://www.lexology.com/library/detail.aspx?g=0fa9ebaf-86d1-433f-bc86-4cb4cd3f3e8b;
- GOZZO, *Responsabilità del motore di ricerca nel caso di "caching",* October 25, 2012, https://francescogozzo.com/motore-di-ricerca-responsablita/;
- HOFFMANN, GASPAROTTI, *Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act",* CEP study, March 2020, https://www.readkong.com/page/liability-for-illegal-content-online-weaknesses-of-the-eu-8865627;
- HOWELL O'NEILL, *Apple and Google's Covid-Tracing Tech Has Been Released to 23 Countries*, in *MIT Technologies Review*, May 20, 2020, https://www.technologyreview.com/2020/05/20/1002001/apple-and-googles-covid-tracing-tech-has-been-released-to-22-countries/;

- IPO Code of of Practice on Search and Copyright (UK), Art. 22, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609478/code-of-practice-on-search-and-copyright.pdf;
- JÄÄSKINEN, December 09, 2009, case *L'Oreal and others v. eBay*, C-324/09, § 141-142, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62009CC0324;
- KELLER, TARKOWSKI, *Digital Public Space – A missing policy frame for shaping Europe's digital future*, *Open Future,* (2021), https://openfuture.pubpub.org/pub/digital-public-space-policy-frame/release/2;
- KUCZERAWY, *The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?,* April 24, 2018, https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/.;
- KUCZERAWY, *Active vs. passive hosting in the EU intermediary liability regime: time*
- *for a change ?*, in *KU Leven CiTiP Center for IT & IP law*, 07 August 2018, https://www.law.kuleuven.be/citip/blog/active-vs-passive-hosting-in-the-eu-intermediary-liability-regime-time-for-a-change/;
- KUCZERAWY, *To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive*, in *KU Leuven CiTiP*, 2019, https://www.law.kuleuven.be/citip/blog/to-monitor-or-not-to-monitor-the-uncertain-future-of-article-15-of-the-e-commerce-directive/;
- KUCZERAWY, *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*, in *Verfassungsblog,* 2021, https://verfassungsblog.de/good-samaritan-dsa/;
- LAURENT ET AL., *SABAM v. Netlog (CJEU C 360/10) ... as expected!*, in *Kluwer Copyright Blog,* February 20, 2012, https://copyrightblog.kluweriplaw.com/2012/02/20/sabam-v-netlog-cjeu-c-36010-as-expected/;
- MADIEGA, *Reform of the EU Liability Regime for Online Intermediaries,* May 1, 2020, 1, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf;
- MANETTI, *Regolare Internet*, in *Media Laws*, 35, July 15, 2020, https://www.medialaws.eu/rivista/regolare-internet/;

- MATHESON, *EU Digital Services Act: What Does it Mean For Online Platforms?*, in *Lexology*, October 19, 2022, https://www.lexology.com/library/detail.aspx?g=740ef9f9-b28e-4597-add0-73c8cf764bab;
- METZ, *The New Chatbots Could Change the World. Can You Trust Them?,* in *The New York Times,* December 10, 2022, https://www.nytimes.com/2022/12/10/technology/ai-chat-bot-chatgpt.html;
- MILMO, *The twisty, drama-filled Elon Musk-Twitter saga: a timeline*, in *The Guardian*, October 28, 2022, https://www.theguardian.com/technology/2022/oct/28/elon-musk-twitter-saga-timeline;
- NOOR, *Should We Celebrate Trump's Twitter ban? Five Free Speech Experts Weigh in*, in *The Guardian,* January 17, 2021, https://www.theguardian.com/us-news/2021/jan/17/trump-twitter-ban-five-free-speech-experts-weigh-in;
- NORDEMANN, *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, 2018, 10, https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf;
- OKABE-MIYAMOTO, LYUBOMIRSKY, *Social Connection and Well-Being during COVID-19,* in *World Happiness Report,* (2021), https://worldhappiness.report/ed/2021/social-connection-and-well-being-during-covid-19/;
- ORRICK (APOSTLE, HAGEDORN, SCHRODER, YAVORSKY, EGAN SUSSMAN, KAWKABANI), *The European Commission's Digital Services Act (DSA) is Approved: What You Need to Know,* October 28, 2022, https://www.orrick.com/en/Insights/2022/10/The-European-Commissions-Digital-Services-Act-is-Approved-What-You-Need-to-Know;
- Opinion of Advocate General Maciej Szpunar, 2 June 2022, Christian Louboutin v. Amazon, Joined Cases C-148/21 and C-184/21, ECLI:EU:C:2022:422, par. 65-72, https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220096en.pdf;
- Opinion Jääskinen, Case C-324/09, L'Oréal paras 138-141, maxime 141, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62009CC0324;
- PALUMBO, *Il Digital Services Act diventa legge,* in *Deberti Jacchia Franchini Forlani*, 2, November 8, 2022, https://www.dejalex.com/2022/11/il-digital-services-act-diventa-legge/?lang=it;

- PAOLUCCI, *Il blocco dei social di Trump e la libertà di espressione online,* February 15, https://www.iusinitinere.it/il-blocco-dei-social-di-trump-e-la-liberta-di-espressione-online-35567;
- PAUL, *Elon Musk withdraws $44bn bid to buy Twitter after weeks of high drama*, in *The Guardian*, July 9, 2022, https://www.theguardian.com/technology/2022/jul/08/elon-musk-buy-twitter-withdraw;
- PAUL, *Elon Musk completes Twitter takeover and 'fires top executives'*, in *The Guardian*, October 28, 2022, https://www.theguardian.com/technology/2022/oct/27/elon-musk-completes-twitter-takeover;
- PAULSON, ROGERS, *Victory in France: Court rules in favor of the Wikimedia Foundation,* 20 June 2016, https://diff.wikimedia.org/2016/06/20/france-legal-victory/;
- PEGUERA, *Mensajes y mensajeros en internet: la responsabilidad civil de los proveedores de servicios intermediarios,* in *UOC*, 2001, 3, https://www.uoc.edu/web/esp/art/uoc/0103008/peguera.html;
- PEGUERA, *The New Copyright Directive: Online Content-Sharing Service Providers Lose ECommerce Directive Immunity and Are Forced to Monitor Content Uploaded by Users (Article 17),* in *Kluwer Copyright Blog*, 2019, http://copyrightblog.kluweriplaw.com/2019/09/26/the-new-copyright-directive-online-content- sharing-service-providers-lose-ecommerce-directive-immunity-and-are-forced-to-monitor-content-uploaded-by-users-ar- ticle-17/;
- PINSENT MASONS, *A guide for online intermediaries on the scope of the EU Digital Services Act,* October 28, 2022, https://www.pinsentmasons.com/out-law/guides/guide-digital-servicesactforonlineintermediaries#:~:text=Online%20platforms%20are%20considered%20a,information%2C%20they%20disseminate%20it%20too;
- Political Guidelines for the Next European Commission 2019-2024, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_en;
- POLLICINO, G. DE GREGORIO, *L'Alba di Nuove Responsabilità sulle Piattaforme Digitali: il Digital Services Act,* in *Agenda Digitale,* December 15, 2020, https://www.agendadigitale.eu/sicurezza/privacy/lalba-di-nuove-responsabilita-sulle-piattaforme-digitali-il-digital-services-act/;
- PRISCO, *Finanza sostenibile, l'impatto ESG sulla gestione dei contenuti online: i nuovi standard SASB*, in *Agenda Digitale*, August 26, 2022,

https://www.agendadigitale.eu/mercati-digitali/finanza-sostenibile-limpatto-esg-sulla-gestione-dei-contenuti-online-i-nuovi-standard-sasb/;

- QUINTAIS, *Commission's Guidance on Art. 17 CDSM Directive: The Authorisation Dimension,* in Kluwer Copyright Blog, June 10, 2021, http://copyrightblog.kluweriplaw.com/2021/06/10/commissions-guidance-on-art-17-cdsm-directive-the-author- isation-dimension/;
- RODOTÀ, *Libertà, Opportunità, Democrazia e Informazione,* in *Convegno Internet e Privacy – Quali Regole?,*1998, https://www.privacy.it/archivio/garanterelrod.html;
- ROSATI, *Italian Supreme Court considers search engines hosting providers and finds them potentially eligible for the application of the hosting safe harbour,* July 3, 2022, https://ipkitten.blogspot.com/2022/07/italian-supreme-court-considers-search.html;
- SCHANZER, *Can Lawmakers Save Democracy from Big Tech?,* in *Georgetown Journal of International Affairs,* September 7, 2021, https://gjia.georgetown.edu/2021/09/07/can-lawmakers-save-democracy-from-big-tech/;
- SHEERIN, *Capitol riots: "Wild" Trump tweet incited attack, says inquiry*, in *BBC*, January 6, 2021, https://www.bbc.com/news/world-us-canada-62140410;
- Sustainability Accounting Standards Board, *Content Moderation Taxonomy: A Foundation for Standard Setting on Issue of Content Moderation,* 2020, https://www.sasb.org/wp-content/uploads/2020/12/Content-ModerationTaxonomy-v7b.pdf;
- STARK, STEGMANN, JÜRGENS & MAGIN, *Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse*, 52, May 26, 2020, https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf;
- TIMMERS, *Debunking Strategic Autonomy*, 1, https://directionsblog.eu/debunking-strategic-autonomy/.;
- TWITTER, *Permanent Suspension of @realDonaldTrump,* in *Twitter blog,* January 8, 2021, https://blog.twitter.com/enus/topics/company/2020/suspension.html;
- UK Committee on Standards in Public Life, *Intimidation in Public,* December 13 2017, https://www.gov.uk/government/publications/intimidation-in-public-life-a-review-by-the-committee-on-standards-in-public-life;
- UN, *Transforming our World: The 2030 Agenda for Sustainable Development,* 2015, Goal 9, https://sdgs.un.org/2030agenda;

- VAN EECKE, TRUYENS, *EU study on the legal analysis of a single market for the information society: New rules for a new age?*, 2009, https://op.europa.eu/it/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722;
- VAN HOBOKEN ET AL., *Hosting intermediary services and illegal content online*, 30-31, 2019, https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en;
- Wikipedia, *January 6 United States Capitol Attack,* 2021, https://en.wikipedia.org/wiki/January_6_United_States_Capitol_attack;
- ZUCKERBERG, in *Facebook*, January 7, 2021, https://www.facebook.com/zuck/posts/101126 81480907401;