Chapter 1 - Introduction

A. General background

It is by now commonplace that the information society and the internet are unprecedented in the way they have and will affect humankind.

> *"… almost like the weather, the flow of information defines the basic tenor of our times, the ambience in which things happen, and, ultimately, the character of a society. How and what you think depends on what information you are exposed to. … We sometimes treat the information industries as if they were like any other enterprise, but they are not, for their structure determines who gets heard."*[2]

We now live in a society where connection to the internet has become for many an essential part of access to information and participation in social and economic life. Some countries have even started to declare access to the internet a fundamental right.[3]

As stated by *Castells*, knowledge and information generation have not only become direct sources of productivity but also have a direct effect on the productivity of information processing and knowledge creation itself, leading to a new technological paradigm.[4] This technology paradigm means that (information) technology today penetrates the "core of life and mind."[5]

Some go even further and say that we have been entering a new age in which the exchange of information and the digital traces left by our everyday lives, be it shopping, spare time activities, professional communication

---

2 Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Atlantic 2012) 12.

3 For example in France: *Décision 2009-580 DC - 10 juin 2009 - Loi favorisant la diffusion et la protection de la création sur internet - Non conformité partielle* [2009] Conseil Constitutionnel CSCX0913243S, FR:CC:2009:2009580DC [12]; Greek Constitution, (Official English language translation of the Greek Constitution, Hellenic Parliament) 2008 para 5A; Electronic Communications Act (Estonia) (English Version) 2006 paras 69–70.

4 Manuel Castells, *The Rise of the Network Society* (2nd ed, Blackwell Publishers 2000) 17.

5 ibid 76.

or even our most private actions are surveyed constantly. Our behaviours and the "big data" gained from it are constantly analysed, predicted and influenced for commercial purposes. Moreover, this activity is currently in full swing of expanding to the offline world.[6]

Internet intermediaries are at a critical juncture of this digital information society. They enable individuals and organisations to find, exchange, share and produce information, to buy and sell products and services, to entertain, create and express themselves on the internet. We know these companies as search engines (*Google*), social networks (*Facebook*), user generated content or video sharing platforms (*YouTube*), online marketplaces (*Amazon*, *eBay*), content aggregators (*Booking.com*, *Reddit*) or sharing economy platforms (*Airbnb*), to name but a few. Being a critical layer of the internet, they exercise not only platform power, the power to connect, influence, amplify and disconnect user activity, but they have also built hugely profitable businesses through exploiting the data left by users on their platforms and elsewhere.[7]

The rise of these powerful actors and their influence has created controversies. It is increasingly accompanied by demands for stronger regulatory action and public accountability of these businesses, many of which have become global corporate behemoths. It would be an understatement to say that internet intermediaries, or online platforms, are subject to intense public debate. The concerns voiced over their business practices are manifold and fundamental. They range from allegations of privacy violations, abuse of market power, unfair commercial practices, allowing electoral manipulation, facilitating copyright piracy and counterfeit sales, promoting hate and violence, to more general claims of undermining democracy. At the heart of these problems lies a combination of the aforementioned essential function of online platforms in the information society and opaque business practices *vis-à-vis* platform users.

It is difficult to say whether the criticism is targeted more at the role of the most dominant platform businesses, like *Google*, *Apple*, *Facebook*, *Ama-*

6 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (Profile Books 2019). Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin Books 2016).

7 John Naughton, 'Platform Power and Responsibility in the Attention Economy' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 382.

zon and Microsoft (the GAFAM),[8] or the responsibilities of internet intermediaries in general. What can be said is that there is currently a fully blown debate over the responsibility of online platforms for the content made available by them and for the way they manage and use the information collected on a massive scale from users.

This work focusses on one of the critical aspects mentioned above: the liability of online intermediaries for information, or content uploaded by users onto their platforms. It will do so by looking at the EU context. More precisely, this work will look at the current challenges of the framework of EU intermediary liability exemptions when it comes to preventing and removing unlawful content on online platforms.

This work attempts to answer two research questions:

1) Is the current legal framework regulating content liability exemptions of online platforms under the ECD still adequate when it comes to combating illegal content?
2) Are there alternative models for intermediary regulation that are better suited to include internet intermediaries in the fight against illegal content?

Unlawful content can take many forms: it can be copyright violating music and video clips, child pornography, counterfeits, illegal hate speech and incitements to violence, such as terrorist content, defamatory postings, or illegal and unsafe product offers.

The fact that unlawful content is a growing problem on the internet, including on "legal" platforms, can be witnessed by a flurry of regulatory activity by the European Commission and Member States in recent years. The European Commission's 2018 Recommendation on measures to effectively tackle illegal content online or the 2020 Digital Services Act Package are more recent prominent examples.[9] The 2018 Communication notes

8 The GAFA: Google, Apple, Facebook, Amazon; and, if including Microsoft, the GAFAM. Zuboff (n 5) ll 445–481 and Patrick Barwise and Leo Watkins, 'The Evolution of Digital Dominance' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 21–25.

9 European Commission, 'Commission Recommendation of 1.3.2018 on Measures to Effectively Tackle Illegal Content Online, C(2018) 1177 Final' (European Commission 2018). European Commission, 'The Digital Services Act Package' (*Shaping Europe's digital future - European Commission*, 2 June 2020) <https://ec.europa.eu/digital-single-market/en/digital-services-act-package> accessed 4 November 2020.

that illegal content hosted on the internet remains a serious problem and it encourages online platforms to detect and remove unlawful content more proactively and effectively.[10] Meanwhile, the proposed Digital Services Act aims at defining increased obligations on digital services providers in order to address more effectively the problem of illegal content online.[11] These problems are not new, however. The EU noted the proliferation of illegal content on the internet consistently over the last 20 years.[12] As the platform economy thrives, internet penetration and connection bandwidth grow, and the online economy makes serious strides in transforming many areas of the offline world, this should not come as a surprise. Every new opportunity, especially one as vast as the digital revolution and the internet, also opens the door for abuse and new criminal activity. This is not made easier when considering that the internet has also challenged substantive law, for example on copyright.[13]

In the face of these breath-taking developments the legal framework has, until now, remained remarkably static. In the EU, the E-Commerce Directive[14] (ECD) has been regulating without change in this area since the year 2000. Drafted in the late 1990s and modelled largely on the US Communications Decency Act[15] (CDA) and the Digital Millennium Copyright Act (DMCA),[16] it offers online platforms far reaching exemptions from liability if they are neutral and purely technical, have no actual knowledge of illegal content and remove it expeditiously once notified of its existence.

---

10 European Commission, 'C(2018) 1177 Final' (n 8) paras 4–9.

11 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 2020 1.

12 European Commission, 'Online Services, Including e-Commerce, in the Single Market, A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services, Accompanying the Document, SEC(2011) 1641 Final' (European Commission 2012). Decision No 1151/2003/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (OJ L 162).

13 Digital copies, mashups, sharing of content through linking or streaming have profoundly changed traditional copyright concepts. Bernd Justin Jütte, 'The EU's Trouble with Mashups: From Disabling to Enabling a Digital Art Form' (2014) 5 JIPITEC 172.

14 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market 2000 (OJ L 178).

15 Communications Decency Act 1996 (47 USC § 230) s 230.

16 The Digital Millennium Copyright Act 1998 (17 USC § 512).

These content liability exemptions have, however, come under progressive pressure over the last 10 years at least.[17] From the large variety of academic, policy and wider society sources, several arguments are commonly being put forward in favour of obliging internet platforms to take wider responsibilities for unlawful content on the internet:

- unlawful content keeps proliferating despite legislative efforts to motivate online platforms to do more to help preventing and removing it;
- many online platforms have become powerful corporations and have formidable financial means that they should better deploy for this purpose;
- platforms are not passive hosts any longer, but actively exploit (big) data and information, including illegal content, in order to make money;
- the technological means to prevent, detect and remove illegal content have improved significantly and online platforms are at the forefront in this area;
- due to their central position in the internet infrastructure, online platforms are technically best placed and have moral obligations to combat illegal content effectively.

In order to answer the first research question, this work will analyse these arguments by mapping out the regulatory landscape and the enforcement challenges related to the wide ambit of illegal content on online platforms.

17 As early as 2004: Lilian Edwards, 'The Changing Shape of Cyberlaw' (2004) 1 SCRIPT-ed 363, 364; Leonie Kempel and Patrick Wege, 'Die Haftung von Plattformbetreibern für „eigene Inhalte" – Welchen Einfluss hat ein Managementsystem auf den Umgang mit Haftungsrisiken?' in Nadine Klass, Silke von Lewinski and Henning Große Ruse-Khan, *Nutzergenerierte Inhalte als Gegenstand des Privatrechts: Aktuelle Probleme Des Web 2.0.* (Springer 2010); Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market L. Rev. 1455 but also more explicitly in: D Friedmann, 'Sinking the Safe Harbour with the Legal Certainty of Strict Liability in Sight' (2014) 9 Journal of Intellectual Property Law & Practice 148.

It should be noted from the start that based on his prior research[18] and professional experience[19] the author advocates for enhanced, legally mandated responsibilities of online platforms to fight unlawful content. Yet, the current policy debate is less and less divided on *whether* platforms should have increased responsibilities rather than on *how* this should be achieved. This may lead critics to argue that, if there is mounting agreement on the need for reform, then why dissect the deficiencies of the current framework in such detail? The answer is that analysing the problems of the current intermediary liability system can provide useful lessons for a new regulatory model. In its last chapter before the conclusion, this work attempts to address this topic and respond to the second research question by exploring an adequate regulatory policy response. There are a variety of solutions debated currently. They range from self-regulatory approaches involving voluntary agreements by industry to more incisive regulatory interventions that see broad obligations imposed on online platforms. At the more extreme end, there are even considerations of subjecting the largest online platforms to tighter regimes along public utility regulation or even splitting them up.[20] Some of this appears to have been taken up at least

18 The author has outlined the arguments and a potential approach (based on technical standards) towards enhanced responsibilities for internet intermediaries first in his 2012 LLM Dissertation written at the University of Edinburgh: Carsten Ullrich, 'Online Intermediaries' Liability 2012: As the Digital Economy Comes of Age, Does the Industry Need to Take On More Responsibilities?' (Social Science Research Network 2012) SSRN Scholarly Paper ID 3594317 28–29 <https://papers.ssrn.com/abstract=3594317> accessed 22 July 2020, in further publications (see Bibliography), and most recently in Mark D Cole, Christina Etteldorf and Carsten Ullrich, *Cross-Border Dissemination of Online Content: Current and Possible Future Regulation of the Online Environment with a Focus on the EU E-Commerce Directive*, vol 81 (1st edn, Nomos 2020) 200–207

19 The author has worked for eight years as regulatory compliance, fraud detection and internal audit manager in a global internet company and managed, amongst others, operational notice and takedown and content removal processes for the company's EU marketplace and regulatory risk related to unsafe and non-compliant products.

20 Julie E Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 369, 378–379; Lina M Khan, 'Amazon's Antitrust Paradox' [2017] The Yale Law Journal 96, 797–892; K Sabeel Rahman, 'Regulating Informational Infrastructure: Internet Platforms As The New Public Utilities' (2018) 2 Georgetown Law Technology Review 234; Frank Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) 17 Theoretical Inquiries in Law 487, 497–503. James Ball, 'How to Cut Big Tech down to Size' (25 January 2019) <https://www.prospectmagazine.co.uk/science-and-technology/how-to-cut-big-tech-down-to-size> accessed 19 August 2020.

partly by the EU Commission during the preparatory work for the new Digital Services Act (DSA) package.[21] This initiative aims to reform the current liability exemptions framework for online intermediaries under the ECD by supplementing it with additional obligations, but will also look to impose stricter regulatory measures on gatekeeper platforms to counteract anti-competitive effects.[22]

This work is the result of a doctoral research project. It aims to make a novel contribution in two aspects:

First, it will complement the current analysis of the regulatory landscape of enforcing against unlawful content *vis-à-vis* online platforms in two areas: product safety and food safety law. These areas have so far received very little attention in academic literature. It will be argued that the characteristics of product and food legislation and its specific enforcement landscape pose unique challenges in e-commerce. Nevertheless, they can provide useful lessons when constructing a new regulatory responsibility framework for online platforms.

Secondly, it will explore a regulatory model for content regulation and liability rules of online platforms, based on risk regulation and duty of care. This co-regulatory solution borrows from the *New Approach*, a system created by the EU in the 1980s, which relies on harmonised technical standards and which was initially used in product regulation.[23] It proposes the definition of public interests and fundamental rights which are harmed by unlawful content on online platforms. Online platforms, given their eminent role in contemporary society would be charged with responsibilities, along duties of care, in order to protect these public interests and values, while the current liability exemptions would be overhauled and reduced.

---

21 European Commission, 'The Digital Services Act Package' (n 8).

22 Laure Kayali, 'Brussels' Plan to Rein in Big Tech Takes Shape' *POLITICO* (30 September 2020) <https://www.politico.eu/article/digital-services-act-brussels-plan-to-rein-in-big-tech-takes-shape-thierry-breton-margrethe-vestager/> accessed 4 November 2020. The alleged anti-competitive effects of large gatekeeper platforms (the *GAFAM*) will not be in the focus of this work. However, the pre-dominance of these networks has a significant impact on the real power and sway of content management practices of these platforms and the availability of unlawful content. It will therefore play a role when analysing the enforcement challenges under the current ECD framework and when developing a reform proposal for intermediary responsibility.

23 Council Resolution 85/C 136/01 of 7 May 1985 on a new approach to technical harmonization and standards 2010; European Commission, 'New Legislative Framework - Growth' (*Growth*) <https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en> accessed 2 July 2020.

Harmonised technical standards would lay down the technical and procedural requirements which platforms need to implement in order to protect public interests.

B. Structure

Chapter 2 will provide a brief general overview of the history of the internet and its technical architecture. This technical background serves as a basis for charting the emergence of intermediaries as main power houses of the internet and the corporate world today. Internet intermediaries, or online platforms, sit at the top layer of the internet's content agnostic, distributed and open architecture. However, their rise to power has seen them invade, and successively capture, large parts of its infrastructure of servers and their connections.

The intermediary typology offered in this chapter will serve to visualise the spread of online platforms into almost all sectors of today's economies and the exchange of information between people. Finally, a description of new multi-sided platform dynamics and the power exercised by the leading players in this area today will underline the socio-technical and economic importance of internet intermediaries. This excursion is meant to create the context for the analysis of the challenges faced in regulating these players and obliging them to take on responsibilities that are commensurate with their economic power and societal significance.

Chapter 3 will start with an overview of the history of the emergence of the current legal system of internet intermediary liability. As online platforms have become an essential layer of today's web architecture, the discussion over internet regulation has become inseparable from the question of how to regulate internet intermediaries. Internet regulation, or internet law, is a wide and fluid term. From the variety of literature, it appears to encompass issues relating to the internet's infrastructure and content.[24] This would correspond to the basic function of the internet: transporting (via an infrastructure) digital information (content) from one piece of ter-

24 See for example: Jan Aart Scholte, 'Polycentrism and Democracy in Internet Governance' in Uta Kohl (ed), *The Net and the Nation State - Multidisciplinary Perspectives on Internet Governance* (Cambridge University Press 2017) 165.; Jacqueline D Lipton, *Rethinking Cyberlaw: A New Vision for Internet Law* (Edward Elgar Publishing 2015) 5.; Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access' (2000) 52 Fed. Comm. L. J. 561, 576.

minal equipment to another.[25] The domain name system, communications protocols, the telecoms network, internet access providers, content servers and hosts, information stored and transmitted through the net, but also end devices, are typical components. Internet intermediaries are one part of this picture, although an increasingly prominent one.

On the other hand, internet regulation draws into its orbit all those legal areas which have been significantly influenced by the internet, such as data protection, copyright law, consumer protection, freedom of expression,[26] competition law, labour law or even more general legal concepts such as jurisdiction.[27]

This will be backed up by more general theoretical justifications for holding intermediaries accountable for the positive actions of others. These concepts had an impact on the first intermediary liability cases of the 1990s. They also served as a basis for the intermediary liability provisions in the EU and beyond. First, the current horizontal framework, set out by the ECD almost 20 years ago will be demonstrated. This will be compared to the regimes set up in the US, Australia, Canada, China and India. The analysis of the first three jurisdictions will chart out the different approaches that Western democracies have chosen towards regulating intermediaries. Meanwhile, the analysis of the Indian and Chinese frameworks serves as a reminder that the future of the internet will be significantly influenced by these emerging and most populous economies, which set different policy objectives.

The EU analysis will show how the pressures exerted on this framework have grown as the internet and online platforms have made massive strides into influencing our everyday lives and economic organisation. The ambiguous and controversial issues, which started to shine through already in the first years after the ECD's implementation, have only become more pronounced over time. Numerous case law from the last 15 years exposes significant problems with the application of the ECD when it comes to deciding,

25 Chris Reed, *Internet Law: Text and Materials* (2nd ed, Cambridge University Press 2004) 8.

26 Tatiana-Eleni Synodinou, *EU Internet Law: Regulation and Enforcement* (Springer Berlin Heidelberg 2017) v.

27 Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (First edition, Oxford University Press 2017) 1–3.

- when an intermediary assumes liability for illegal content, i.e. when its intermediation activity is passive or active;
- when it can be assumed to have actual knowledge or control of the information it hosts;
- the scope of preventive activities that platforms can be obliged to perform, i.e. the demarcation line between a specific and a (prohibited) general obligation to monitor for unlawful content.

The case law discussed will draw from both EU and Member State judgements, but also refer, where appropriate, to case law of the European Court of Human Rights (ECtHR) and from outside Europe, such as the US, Canada, China and elsewhere.

Chapter 4 will offer a broad sectoral analysis of the variety of (unlawful) content hosted by platforms today. In the early days of the internet, legally controversial content related mainly to defamation, hate speech or child pornography, and was often communicated through newsgroups.[28] Even copyright infringing music file-sharing through peer-to-peer networks became a widespread and noticed phenomenon only after 2000.[29] It may not have played a role at all in the drafting phase of the ECD. By contrast, the kind of material hosted on Web 2.0 platforms today spans a much larger variety. The sectoral analyses will be structured in a similar, yet not identical way, for each type of unlawful content. Altogether seven subject matter areas will be treated: defamation, hate speech, terrorist content, copyright, trademark law, product safety and food safety.[30]

---

28 Lars Davies, 'Internet and the Elephant' (1996) 24 Int'l Bus. Law 151–159.

29 Pheh Hoon Lim and Louise Longdin, 'P2P Online File Sharing: Transnational Convergence and Divergence in Balancing Stakeholder Interests' (2011) 33 European Intellectual Property Review 2011 690.

30 An original plan to include child pornographic content and pharmaceutical products into the sectoral analysis was abandoned due to reasons of space and time. With regards to the ample legal literature on the fight against child pornography and child abuse online the following sources shall be recommended: Yaman Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (Taylor & Francis Group 2008); Abhilash Nair, *The Regulation of Internet Pornography Issues and Challenges* (Routledge 2019). For further information on the fight against illegal and unsafe pharmaceutical products, see: Tim K Mackey, Phyo Aung and Bryan A Liang, 'Illicit Internet Availability of Drugs Subject to Recall and Patient Safety Consequences' (2015) 37 International Journal of Clinical Pharmacy 1076; OECD and European Union Intellectual Property Office, *Trade in Counterfeit Pharmaceutical Products* (OECD 2020) <https://www.oecd

First, the emergence of unlawful online content in each area will be sketched out. This will be followed by an analysis of EU-wide and national regulation of the sectoral subject matter. This analysis will expose differences in the more private law subject matter areas of defamation and hate speech, which lie within the national competency of Member States, as opposed to more mixed set-ups in the areas of copyright or terrorist content. The fully harmonised areas of trademark law and product and food regulation carry again different characteristics. The same can be said for the enforcement regimes, which in the areas that touch on public law, such as product, food regulation and terrorist speech are occupied by law enforcement and/or market surveillance authorities with a pronounced experience and approach in this area. By contrast, other sectoral regimes rely more on private law, contractual arrangements, where enforcement happens mainly through courts. The interaction of the specific sectoral regimes with the intermediary liability provisions of the ECD provides a first picture of disunity. On a second level, the interpretation of courts of the intermediary liability provisions have been varying since the inception of the ECD in 2000. The CJEU, as will be shown, had some, but arguably too little harmonising influence in this matter. The third factor of complexity is introduced by Member States. In some areas they have incorporated additional intermediary liability provisions into their substantive laws, while on a more general level, ordinary law principles of intermediary or secondary liability also interact in different ways with the ECD.

In a second step, the private enforcement practices of intermediaries in each of the sectors will be reviewed. Online platforms have charted ahead largely unimpressed by regulatory complexities and superimposed on users their own, often global standards of content regulation through their terms and conditions, or content policies. Whether and how these comply with local standards and policy objectives will be analysed in more detail. The rise of Web 2.0, social media, UGC platforms and online marketplaces added yet more complexity. The sheer volume, speed, interactivity and the increasing automation and opacity with which the global platforms manage and exploit user data for their commercial ends has made unlawful content almost endemic.

-ilibrary.org/governance/trade-in-counterfeit-pharmaceutical-products_a7c7e054-en> accessed 12 June 2020; Carsten Ullrich, 'Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective' (2017) 8 JIPITEC 111, 121–122;

The analysis will conclude with a review of sectoral regulatory initiatives at both national and EU level and how these relate to the wide liability protections enjoyed by Web 2.0 platforms under the ECD. The aim of Chapter 4 is to demonstrate the complexity and sheer size of the challenges at stake from a legal, technological and socio-economic point of view. This charting exercise will also reveal the multi-level regulatory character of the intermediary liability universe.

A purely sectoral approach towards enforcement, it might be argued, would not only be a missed opportunity, because it would prevent enforcers and legislators to learn from each other. Moreover, it would likely fail due to regulatory overload on both enforcers and businesses. Meanwhile, a one size fits all, rigid horizontal approach would not sufficiently take account of the different types of online platform business models.

Chapter 5 will introduce case studies which explore the challenges of effectively identifying and removing unlawful content from online platforms in two areas: non-food consumer products and food products. The choice of these two areas is deliberate. The challenges of enforcing copyright, trademarks, hate and defamatory speech and terrorist content have already been discussed more widely throughout academic literature, with copyright being a particularly well covered topic.[31]

By contrast, academic coverage of the challenges of enforcing product and food safety law online is patchy at best. Product and food safety regulation are complex, with an elaborate regulatory and enforcement regime. Product regulation is *New Approach* regulation. This is a highly technical, co-regulatory system, in which the public interest requirements are laid down in broad product directives, covering for example protective equipment, toys, radio equipment or medical devices. The implementation of these legal requirements in product design relies largely on voluntary harmonised technical standards, drawn up by industry and following a risk-based approach. Meanwhile, enforcement lies squarely within the hands of Member States, represented by a patchwork of national market surveillance authorities (MSAs). Food safety regulation operates on a similar basis, although not being part of the *New Approach*.

---

31 For example : Sandra VI Schmitz, *The Struggle in Online Copyright Enforcement: Problems and Prospects* (1. edition, Nomos 2015); Bernd Justin Jütte, *Reconstructing European Copyright Law for the Digital Single Market: Between Old Paradigms and Digital Challenges* (1. edition, Nomos ; Hart Publishing 2017); João Pedro Quintais, 'Global Online Piracy Study' (Institute for Information Law (IViR), University of Amsterdam 2018); Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International BV 2017).

The two case studies deal with the enforcement of product and food safety law on online platforms. They are based on 13 detailed and targeted interviews and survey results gained from both MSAs and food safety authorities (FSAs) across Europe, conducted over the period from November 2017 to March 2019. MSAs and FSAs shared the challenges they face when enforcing product legislation *vis-à-vis* online marketplaces and in e-commerce in general, in a national, European and global context. The feedback received confirms that a slow, highly fragmented, sectoral enforcement system is up against significant obstacles when facing the horizontal challenge of e-commerce. There is a general mismatch between the broad liability protections of online platforms and their potential usefulness and leverage in helping to keep unsafe and illegal products off the internet. Meanwhile, efforts to co-opt online marketplaces more into these efforts have so far hit against the wall of the ECD and its liability protections.

On the other hand, the *New Approach* regulation opens some interesting avenues with regards to intermediary liability. Products need to comply with mandatory technical specifications, which follow broad public interest criteria, defined by essential requirements in the law. Industry-designed and state-approved technical standards help economic actors to implement the mandatory technical specifications and provide an assumption of compliance. Could this also be a *modus operandi* for governing the responsibilities of internet intermediaries?

On a conceptual level, Chapters 2 to 5 are setting the foundations for advocating for a change in the current intermediary liability rules. Chapter 6 aims to propose such a regulatory framework. It will reopen the more general analysis of internet regulation of Chapter 2. First, an overview of a number of proposals to reform online intermediary provisions, made mainly by academics over recent years, will be discussed. The first such attempts were made as early as 2007, with the frequency of proposals increasing over the last five years. These reform proposals themselves testify for the broadly perceived and mounting need to reform the current regime. They all investigate a move from pure limited liability to broader responsibilities for reasons that should have become clear from the analysis provided in Chapters 3 to 5. Yet, the proposed regulatory tools and the intensity of regulation vary widely. They reach from self-regulatory approaches and co-regulation to partly more interventionist state involvement. This variety of approaches will set the scene for a more detailed analysis of the regulatory tools that may be appropriate for effectively regulating online platforms, with a view to stem the flow of unlawful content and activity that is a persisting problem on today's internet.

These tools will be put into the context of the cyclic nature of technological innovation, which is but an undercurrent of an increasing complexity of our societies over the last 200 years. The social fabric of our lives and societies is becoming more complex, and arguably that trend has only been amplified by globalisation and the information society revolution. These developments have been famously analysed by *Durkheim*[32] who, working in the middle of the second industrial revolution,[33] at the end of the 19th century, saw society and moral values overturned by mass urbanisation, mass production and the first means of mass communications. He called this state *anomie*. He noticed that the ever-progressing division of labour in capitalist society led to new, more specialised and denser professional, administrational and judicial functions, in which the state had a less and less central role as a rule setter.[34] New actors and relations fill the anomic state of modern societies with new normative values. His theory is today seen as a precursor to modern theories of governance and the emergence of co-regulatory systems.[35]

Policymakers are confronted by the regulatory challenges of the new technology paradigm of the information age.[36] The "jurisdictional puzzle" of the internet[37] and increasing demands on globally operating online platforms to provide transparency over their (algorithmic) content management decision, are just two illustrative issues.[38] In this multi-level regulatory environment, the legal norms are being formulated and enforced through hybrid systems of private and public ordering. Regulators rely increasingly on epistemic communities in the form of professional networks.[39] Content regulation on online platforms and its enforcement expose this multilevel regulatory and transnational maze in an exemplary way. This more theoretical discussion of different regulatory tools will

32 Émile Durkheim, *De la division du travail social (1873)* (Presses Électroniques de France 2013).
33 Castells (n 3) 33–38.
34 Durkheim (n 31) s 688.
35 Harm Schepel, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets* (Hart Pub 2005) 21.
36 Cohen (n 19)
37 Svantesson (n 26).
38 Kenneth A Bamberger, 'Technologies of Compliance: Risk and Regulation in a Digital Age' (2009) 88 Tex. L. Rev. 669, 688–689. He demonstrates the challenges of the state mandating and overseeing technical governance, risk and compliance systems (GRC) as part of risk regulation in tech industries.
39 Peter M Haas, 'Introduction: Epistemic Communities and International Policy Coordination' (1992) 46 International Organization 1.

serve as a reminder that the regulatory responses to the challenges posed by unlawful content on online platforms need to take these complexities into account. A regulatory solution will need to be specialised, technically flexible and scalable. It will need to answer the transnational challenges posed by the internet and globalisation. At the same time, it needs to be democratically accountable and transparent.

In the final part of Chapter 6, a co-regulatory framework of intermediary responsibility will be proposed, which attempts to respond to these demands. This system tries to apply the analysis made in the course of this work by moving away from the current liability exemption provisions to a more flexible, yet enhanced responsibility structure. Responsibility is more in line with contemporary forms of corporate governance. Responsibility is defined through broad public interest criteria which internet platforms would need to safeguard, given their important functions in today's society. In this sense, the proposal will apply features of the *New Approach* regulation discussed in the case studies. This work will go further and venture into describing the different risk management stages on a procedural level. A practical example of such a duty of care risk management standard will be showcased. This standard was developed in cooperation with *REACT*, an Amsterdam-based non-profit trade organisation that is dedicated to fighting counterfeiting. It covers the area of trademark infringements and lays down requirements that a responsible online marketplace would need to adopt in the prevention and fight against counterfeits and unsafe and illegal products. A detailed version can be found in ANNEX III. This system could eventually be incorporated into a technical standard, borrowing again from the *New Approach* and exploring a solution based on responsive regulation.[40] The standard would serve as a proof of compliance with the statutory responsibilities imposed on online platforms in the fight against illegal content or activity. It will be discussed whether this approach necessitates a change of the ECD, and what such a modification could look like. This discussion will also provide some brief comparative analysis and evaluation of the Digital Services Act package, which the Commission published in December 2020 and which coincided with the

40 Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992) chs 1, 4, where the authors describe how regulatory systems and government intervention should respond to specific market conduct, institutional and regulatory culture and history.

completion of this work.[41] This analysis was added during the final stages of preparing this work for publication in spring 2021.

C. Methodology

Chapter 2 gives an account of the emergence of internet intermediaries from an economic and socio-technical point of view. The research is descriptive for the historic and typological explanation of intermediaries. It is supplemented by an evaluative analysis of the position of internet intermediaries within modern society. The analysis relies mainly on a review of secondary legal sources from academia, policy makers and international organisations and from sources in neighbouring areas of law, such as economics (competition) and social sciences (history, sociology).

This descriptive approach is continued in Chapters 3 and 4. These Chapters deal with the emergence of the intermediary regulatory framework in the EU and the US and the sector specific legal provisions for most types of unlawful content found on online platforms. This descriptive approach is complemented by an analysis of the main failures and challenges of this current legal setup.[42] This part relies on a review of primary legal sources, namely case law and statutes, as well as secondary resources, such as doctrinal literature from academia and regulatory policy analysis from public institutions and industry.

This work focusses on the EU intermediary regulatory frameworks. It does not systematically pursue a comparative approach. However, it would be a serious miss if one failed to refer to the US when analysing internet intermediary regulation. The US was the first country to put in place laws dealing specifically with online intermediaries. This influenced other regulatory approaches worldwide. The analysis in Chapter 3 also includes comparisons with Australia, Canada, China and India. Some jurisdictions may offer potentially new and more effective approaches in legislation and enforcement. These differences in legislation and enforcement are also relevant when discussing the position of governments *vis-à-vis* large, globally

41 European Commission, 'The Digital Services Act Package' (n 8).

42 Descriptive research is used in the sense that it builds the ground for evaluative and conceptual argumentation in the latter parts of the work: see also Mark van Hoecke, 'Legal Doctrine: Which Method(s) for Which Kind of Discipline?' in Mark van Hoecke (ed), *Methodologies of legal research: which kind of method for what kind of discipline?* (Hart 2011) 18.

operating intermediaries as normative and executive powers in content regulation on a global scale.[43] Secondly, a discussion of the problems of applying the EU intermediary liability rules in reality would not be complete if it failed to highlight the varying interactions between EU Member States' national laws, legal approaches to secondary liability and the ECD. These differences play out at a horizontal level, when discussing doctrines of indirect liability in general, but also when looking at sectoral applications, in e.g. hate speech or copyright. For this reason, elements of a comparative analysis are included in Chapters 3 and 4. Every effort has been made to call out analysis across different jurisdictions and to offer summary outlines of main differences and commonalities.

Despite Brexit, which was decided shortly before the research for this work had started, abundant references to UK intermediary legislation and case law are made throughout this work. Both the horizontal analysis in Chapter 3 and the sectoral analysis in Chapter 4 include the UK, and England and Wales, in reviews of selected Member State case law and legislation at various points. The case studies in Chapter 5 also draw on feedback received from UK stakeholders. At the time of writing the UK was still part of the EU. Its law-making and its court rulings were influenced and determined by the ECD and various other EU acts and CJEU rulings. UK intermediary case law and national sectoral legislation, which includes specific obligations for internet intermediaries, is rich and varied. This has contributed to the diverse and multifaceted interpretations of the protections and obligations attributed to online intermediaries and their enforcement in the EU. Moreover, the UKs common law tradition has left a unique mark on the way online intermediary responsibilities and enforcement options have been approached in the EU. This singular influence is set to continue affecting EU policy making in this area. For all of these reasons, UK case law and legislation up to the end of 2020 have been included as an integral part of the analysis of EU online intermediary responsibilities *vis-à-vis* unlawful content.

The two case studies on the application of intermediary liability provisions in the areas of product safety and food safety in Chapter 5 follow a descriptive approach. They are based on a qualitative, pre-structured sur-

43 Luca Belli and Cristiana Sappa, 'The Intermediary Conundrum' (2017) 8 JIPITEC 183, 185–190.

vey,[44] conducted either in the form of personal interviews, held on location or by telephone, with market surveillance authorities across EU Member States, or by soliciting the completion of the survey sheet that was used during the personal interviews. The pre-structured survey imposes a set of common questions, thus allowing for empirical verification of certain assumptions. These interview questions were meant to incite interlocutors to expand in more detail on the practical enforcement challenges in their daily work. The template of the survey can be found in ANNEX I.

The pre-structured approach was deemed the most appropriate method because it allowed for a more in-depth and informal discussion while limiting the risk of interlocutors wandering off the topic. Secondly, the structured discussion also helped respecting the time accorded by the authorities, usually 2 – 3 hours. Third, it ensured comparability of the answers. The survey was constructed and verified using the methodology elaborated by *Jacob, Heinz and Décieux.*[45]

Chapter 6 uses conceptual analyses[46] in order to develop an alternative regulatory approach to online intermediary regulation. Building on the analysis in the previous chapters, the proposed framework is compared to the status quo in Europe and tested against moral, socio-economic and policy goals. The justifications for the proposed approach were derived from analysing primary legal sources in case law and secondary sources in academic research, but also from wider (non-legal) social science, namely sociology, economics and philosophy.

---

44 Harrie Jansen, 'The Logic of Qualitative Survey Research and Its Position in the Field of Social Research Methods' (2010) 11 Forum Qualitative Sozialforschung / Forum: Qualitative Social Research 4 <http://www.qualitative-research.net/index.php/fqs/article/view/1450> accessed 6 August 2019.

45 Rüdiger Jacob, Andreas Heinz and Jean Philippe Décieux, *Umfrage: Einführung in die Methoden der Umfrageforschung* (3., überarb. Aufl, Oldenbourg 2013).

46 Robert S Summers, 'The New Analytical Jurists' (1966) 41 New York University Law Review 861, 866–875. Mark van Hoecke (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart 2011) v.

D. Definitions, assumptions and limitations

1. Definitions

I. Internet intermediaries – intermediary service providers

The OECD defines internet intermediaries as entities that

> *"bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."*[47]

This simple and precise and definition appears to capture also the concept of intermediary service providers (ISP) under the EU's E-Commerce Directive (ECD).[48] Intermediary service providers (ISPs) are information society service providers (ISSPs) as per the Technical Standards and Regulations Directive,[49] which facilitate services that consist of the transmission of information[50] and storage (hosting) of information[51] for the service recipient. In other words, ISPs can be considered a sub-category of ISSPs. For example, an online retailer selling products on its own account would be considered an ISSP but not an intermediary service provider (ISP). By contrast, an online marketplace that lists offers from various sellers/retailers would be considered an ISP. Likewise, an online insurance agency or an online travel agency would be an ISSP but not an intermediary. However, an online price comparison engine for insurance services or a platform offering accommodation from third parties, such as hotels or private individuals, would be considered an ISP.[52]

The terms internet intermediary, online intermediary and intermediary service provider (ISP) will be used interchangeably in this work.[53]

---

47 OECD, 'The Economic and Social Role of Internet Intermediaries - DSTI/ICCP(2009)9/FINAL' (OECD 2010) 9.

48 Directive 2000/31 (ECD) s 4.

49 Directive 2015/1535/EU 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 2015 (OJ L 241) Article 1 (1). See also Chapter 3

50 Directive 2000/31 (ECD) Articles 12, 13.

51 ibid Article 14.

52 For more detail see also Alfred Büllesbach (ed), *Concise European IT Law* (2nd ed, Kluwer Law International 2010) 696–698.

53 ISPs can therefore be considered a sub-category of ISSPs.

II. Online platforms

This work discusses the governance of online platforms. It should be stated from the outset that until the recent DSA proposal there was no legal agreed definition of online platforms.[54] The EU had until then refrained from attempting to create one, noting the variety of technological and business models and the fast-paced developments in this sector.[55] Notwithstanding this lack of a definition in law, there is ample literature within economics that offers definitions of platforms and online platforms. The economic discussion of platforms also deals with the particular aspects of two or multi-sided markets in the digital environment and how this affects rule-making as well as competition.[56]

For the purposes of this work, the term "online platform" refers to those ISPs that act as information hosts as specified under Article 14 (1) ECD.[57] More specifically, it refers to socially media and UGC networks, online marketplaces and sharing economy services as online platforms. Online platforms generally provide "infrastructure and enable interactions between suppliers and users for the provision of goods, services, digital content and information online."[58]

A typology of these different information hosts will be provided in Chapter 2.

ISP terminology	Corresponding ECD Article
internet intermediary/online intermediary, intermediary service provider (ISP)	Articles 12 – 14
internet access provider (IAP)	Article 12

54 Bertin Martens, 'An Economic Policy Perspective on Online Platforms' (Institute for Prospective Technological Studies 2016) Digital Economy Working Paper 2016/05 JRC101501.

55 European Commission, 'Commission Staff Working Document Online Platforms Accompanying the Document Communication on Online Platforms and the Digital Single Market SWD(2016) 172 Final' 2–3.

56 Michael L Katz and Carl Shapiro, 'Systems Competition and Network Effects' (1994) 8 Journal of Economic Perspectives 93. Kevin J Boudreau and Andrei Hagiu, 'Platforms Rules: Multi-Sided Platforms as Regulators' in Annabelle Gawer (ed), *Platforms, markets and innovation* (Paperback edition reprinted, Edward Elgar 2014).

57 First part of the first sentence: "…an information society service … that consists of the storage of information provided by a recipient of the service,…"

58 European Commission, 'Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices SWD(2016) 163' 121. European Commission DSA proposal (n 10) Article 2 (h).

caching service	Article 13
online/internet platform; online/internet host	Article 14

Table 1 - ISP terminology

III. Illegal versus unlawful content

The title of this work refers to *unlawful* content. It was originally planned to write about *illegal* content and activities on online platforms. This would have been in line with the wording in the ECD.[59] In everyday use both terms are often deployed synonymously. However, on closer observation *illegality* is a positive formulation, which defines forbidden actions.[60] Meanwhile, *unlawfulness* is a negative, non-exclusive term which refers to all acts disapproved by or against the law due to them being immoral or conflicting with public policy.[61] Other legal resources attribute both terms with the same meaning.[62] This is confirmed in everyday usage.[63] Given the above, *illegal* acts would refer to a finite number of defined acts, whereas the term *unlawful* can be assumed to include non-defined acts along defined (*illegal*) acts.

This becomes important when one considers the impact the internet and digitisation have made on society. While this work sides with the view that what is illegal offline should be illegal online, the internet and the intermediation practices of online platforms have led to new phenomena that are still being evaluated from a moral point of view. There are now more acts that, while not straightforwardly defined as illegal, may conflict with hitherto widely accepted ethics and morals. Moreover, some illegal acts may have become subject to a new moral re-evaluation by society.

59 Directive 2000/31 (ECD) Recitals 40, 44, 45, 46. 48 & Articles 14, 15.

60 'What Is UNLAWFUL? Definition of UNLAWFUL (Black's Law Dictionary)' (*The Law Dictionary*, 7 November 2011) <https://thelawdictionary.org/unlawful/> accessed 18 February 2019.

61 ibid.

62 The Cambridge Dictionary for example defines both terms as 'not allowed by law'. 'UNLAWFUL | Meaning in the Cambridge English Dictionary' <https://dictionary.cambridge.org/dictionary/english/unlawful> accessed 28 September 2020; 'ILLEGAL | Meaning in the Cambridge English Dictionary' <https://dictionary.cambridge.org/dictionary/english/illegal> accessed 28 September 2020.

63 The reasoning is complicated by the fact that illegal acts are also commonly seen as any act outside a given law, while in their strictest use this merely relates to explicitly defined acts outside the/a law.

Prominent examples can be the copyright infringing activities through peer-to-peer file sharing, the evolving jurisprudence on communication to the public on the internet in copyright law, or the public discussion on disinformation on social media, which is caused by the almost indiscriminate facilitation of massive amounts of content, products and advertisements through internet intermediaries. The term unlawful therefore seems to be corresponding better to the *Durkheimian* state of *anomie* that society today faces *vis-à-vis* certain business and information management practices in the digital economy.[64]

IV. Material content

This work deals with unlawful content hosted or shared on online platforms. For the purposes of this work, this is the kind of content or information which users or businesses upload to platforms for other users/businesses. This will be defined as *material* content. Subsequently, when talking about content or information uploaded to or hosted and shared on online platforms this will refer to the material content. Material content would be at the heart of an online platform's business model. For example, for *Facebook,* material content is all information, be it written text, sounds or moving images, which users upload and share with other users. Likewise, content posted by advertisers on *Facebook* would also be material content. On an e-commerce marketplace, such as *Amazon* or *Alibaba,* the material content would be all information related to and including products offered for sale by third parties, sponsored advertising or customer reviews.

This work uses the term *content* in an encompassing fashion, by relating to all material content or information hosted on online platforms, including speech, any type of media, but also listings of products and service offers.[65]

There are, however, other types of content or information on platforms. For example, ISPs are required to provide legal disclaimers, inform customers on the use of cookies or, depending on the kind of business, in-

64 Zuboff (n 5) ll 3398–3438; Jan Blommaert, *Durkheim and the Internet: On Sociolinguistics and the Sociological Imagination.* (Bloomsbury Publishing Plc 2018) ll 475–481.

65 This is similar to the approach by the Commission in its DSA Proposal: European Commission DSA proposal (n 10) Recital 12.

form and receive consent from users on the use of personal data. This ancillary information is not covered by the term material content in this work.

V. Unlawful activity and unlawful content/information

The liability protections of the ECD apply to illegal information and activity.[66] Unlawful activity, which comprises illegal activity, is usually related to the acts of offering or sharing unlawful information, services or products via the platform. This process usually involves uploading information to the platform. For example, in the context of e-commerce that activity would be the sale of a counterfeit product by a seller through an online marketplace. In the context of incitement to violence it would be the intentional act of uploading this kind of information onto an intermediary site and sharing it with other users. This work refrains from distinguishing between unlawful content and activity. The distinction may be relevant with regards to the sanctions incurred by the uploading user. For a platform's liability, or responsibility, it remains however legally irrelevant whether it is unlawful information or activity that occurred on the platform. It may have an impact on potential technical mitigation strategies in a risk-based compliance framework. But this will, where relevant, be discussed and called out in Chapter 4. For reasons of clarity and brevity unlawful content will therefore include unlawful activity.

VI. Harmful content

The limitation to unlawful content would imply that everything that is "legally allowed" on online platforms is out of the scope of this work. Policymakers and societal stakeholders in the EU and elsewhere have, however, repeatedly stated that harmful, contentious or offensive content that is not unlawful remains a problem on the internet, and on online platforms in particular. Typically, this concerns media content harmful to vulnerable groups, such as children, but also the spread of disinformation.[67]

66 Directive 2000/31 (ECD) Article 14 (1) (a).

67 Mark Bunting, 'Keeping Consumers Safe Online: Legislating for Platform Accountability for Online Content' (Communication Chambers 2018) 20–22, 26. European Commission, *A Multi-Dimensional Approach to Disinformation: Report of*

While certain information or (moving) images might be legal in general, they may become unlawful when exposed to children. Therefore, it is commonly the responsibility of the entity which makes this content available to the public to restrict or give users the opportunity to identify and suppress it. The recently recast Audiovisual Media Services Directive (AVMSD) has, for example, put such obligations in place for video sharing platforms (VSPs).[68] On the other hand, legal, but wrong or distorting information and news may acquire new meaning and significance in a social media environment of mass sharing and commenting. This may then have the potential to undermine societal values.[69] The EU is distinguishing its legislative approach on illegal content to that from "not necessarily illegal but potentially harmful" content.[70] Tackling the latter may indeed not warrant the same degree of urgency and also require a more careful balancing exercise with other fundamental rights, such as freedom of expression.[71] This work will only consider harmful or contentious content to the extent that it spills over into spheres of unlawfulness. The proposed solution to combat unlawful information online explored in the last chapter would, however, be adaptable to the management of this kind of content, subject to additional safeguards. In fact, it would be an integral part of a risk-based approach that a platform operator be able to understand the risk harmful (but legal) content poses in the context of its specific business model and the technology used.

---

the Independent High Level Group on Fake News and Online Disinformation (2018) 10–11.

68 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities 2018 (OJ L 303) Art. 28b.

69 Natali Helberger, Jo Pierson and Thomas Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34 The Information Society 1, 7.

70 European Commission, 'Communication: Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms COM (2017) 555 Final' (2017) 6.

71 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 Online Disinformation: A European Approach COM(2018) 236 Final' (European Commission 2018) 1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236> accessed 19 July 2019.

VII. Platform users

Online platforms engage a number of different parties who partake in various ways in information and transactions hosted on their servers. In the context of this research, *users* means all businesses, consumers or other entities and parties which interact in some way or another with the platform, be it as, a) uploaders of content, sellers, advertisers (i.e. the "recipients of services" in the sense of the Technical Standards and Regulations Directive[72]); b) consumers and businesses downloading, purchasing or receiving or otherwise consuming content and products on online platforms, and c) other parties which engage with platforms by e.g. filing notice-and take-down requests of allegedly unlawful content to online platforms, or by requesting information or remedies in the exercise of their rights, and the like.

2. Assumptions

This being a predominantly legal analysis, no new empirical data on the availability and scale of unlawful content and activity promulgated through internet intermediaries will be provided here. It has been stated abundantly by governments, regulators, international organisations, academia and industry sources that, for all of their positive and beneficial contribution to contemporary society, online platforms are also seen as important conduits for the spread of unlawful content. This work will provide analysis and data from secondary sources where needed for the argumentation in order to substantiate this ongoing problem.

3. Limitations

I. Sanctions

Platforms which fall foul of their duties under the liability exemptions framework of the ECD are subject to sanctions imposed under national

72 Directive 2015/1535/EU 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 Article 1 (1) (b).

law.[73] These are typically non-criminal, secondary liability sanctions. Platforms which are found to be situated outside of the liability protections of Article 14 ECD because they are seen as active hosts which exercise control over the information,[74] would be directly liable for the tort or crime relating to the illegal information on their site. This may range from criminal sanctions in the case of terrorist content to civil sanctions in cases of IP infringements or defamation to name but a few. Given the variety of information, content and activity on platforms, this work cannot cover the sanction regimes of all the possible torts and crimes involved across the different Member States.

Moreover, the work will not attempt to sort out or redefine the complex and diverging national sanctions regimes relating to secondary liability for a platform's failure to comply with the ECD. This discussion focusses on the duties and responsibilities of online platforms in removing and preventing unlawful content. The solution proposed in this work will introduce a negligence based responsibility framework that aims to clarify and broaden the applicability of secondary liability, thus potentially limiting findings of primary liability. The design of a sanctions regime for secondary liability could be a fitting topic for further research in this area. Alternatively, it could be a unique chance to create a separate, free-standing sanctions regime that is directly attached to the new responsibilities of the framework proposed here.

II. Substantive law affecting online platforms

As mentioned above, the online platform landscape is diverse and constantly evolving. The current debate about the role of these businesses touches on many aspects. Unlawful content is just one part of this debate.

A discussion on unlawful content on internet platforms will invariably interface with these other legal aspects which are all linked to the various *fundamental rights* that are impacted by the activity of platforms and by any efforts to prevent and remove unlawful content. The most notable ones are human dignity,[75] the respect for private and family life,[76] the rights of chil-

73 Directive 2000/31 (ECD) Article 14 (3), 20.
74 ibid Recital 42.
75 Charter of Fundamental Rights of the European Union 2009 Article 1.
76 ibid Article 7.

dren,[77] the protection of personal data,[78] freedom of expression and information[79], the freedom to conduct a business[80] or the right to property.[81] The role of these fundamental rights is crucial when discussing liabilities, responsibilities and the regulation of online intermediaries in the fight against unlawful content. It deeply affects the balancing exercises of courts and the efforts of legislators when drawing up rules for online intermediaries. As overarching and encompassing principles they evoke a number of other, neighbouring substantive law areas that therefore become also relevant when discussing intermediary liability.

Data protection is a key concern as online platforms have made big data the substance of their business models. Big data is generated from the information users post, share and consume on the internet and from the services they offer to other users. It plays a role when talking about platforms' control over this data, which includes in many cases personal data. Control means that platforms collect, process and commercialise personal information on a massive scale. Could it be argued that the degree to which platforms exercise control from a data protection perspective influences the content liabilities of these platforms under the ECD, which only exempts passive hosts, with no control over the information they host? In addition to that, taming the flow of unlawful information on platforms will impact data protection where (algorithmic) content management decisions are made more transparent and where risk-based preventive content filtering involves processing of user data. It also plays a role when courts, law enforcement or other parties require the disclosure of the identity of service recipients that engage in allegedly infringing activities.

Consumer law is impacted when discussing the role of platforms that unwittingly facilitate the sale of counterfeits, pirated content, fake or unsafe consumer products or advertising for such products. The sections on trademarks, product and food safety will illustrate how e-commerce platforms impact on consumer protection objectives and how this affects commercial practices regulated under consumer law.

*Competition law a*nd abuse of market power become important when looking at the current dominance of a handful of large players in key on-

77 ibid Article 24.
78 ibid Article 8.
79 ibid Article 11.
80 ibid Article 16.
81 ibid Article 17.

line markets.[82] *Google*, *Amazon*, *Facebook*, *Apple* and *Microsoft (the "GAFAM")*, have all been subject to competition law cases at EU and global level regarding their activities. Meanwhile, traditional competition law approaches need to be adapted to the characteristics of multi-sided platforms.[83] The regulatory solution proposed at the end of this work will need to take account of a lopsided market structure in which a few large players could dominate and profit from a co-regulatory system at the expense of smaller players. As such, market competition concerns may have an influence on formulating new responsibilities, with large, systemic platforms that provide public goods being, for example, subject to stricter requirements.[84]

IT and cyber security will play a role when talking about transparency obligations of online platforms with regards to algorithmic decision-making, content management and other co-regulatory mechanisms as well as safeguarding user rights, such as privacy and other personality rights.

Other legal areas touched by digitisation and the emergence of online platforms are *copyright and trademark law*, *defamation law*, *incitement to violence*, *anti-terrorist law*, *the protection of minors, or product regulation.* Some of these areas are within the full competency of Member States while others are subject to shared competencies as per the EU treaties. This work cannot discuss the substance of these laws in detail, some of which are subject to intense debate due to the influence of the internet. It will however deal with substantive aspects of these laws where this touches on the roles and responsibilities of internet intermediaries. This will be done in Chapter 4.

---

82 see for example: Martin Moore and Damian Tambini (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018).

83 OECD, 'Rethinking Antitrust Tools for Multi-Sided Platforms' (2018) <www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm> accessed 30 July 2019.

84 Alexandre De Streel and Martin Husovec, 'The E-Commerce Directive as the Cornerstone of the Internal Market: Assessment and Options for Reform.' (European Parliament 2020) 45–46 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf> accessed 2 November 2020; Ben Wagner, 'Free Expression? Dominant Information Intermediaries as Arbiters of Internet Speech' in Damian Tambini and Martin Moore (eds), *Digital dominance: the power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 220–221, 232–236.