Chapter 7 - Conclusion

As this work was written the COVID-19 pandemic crisis hit the world. The consequences of this global emergency, which cost the lives of many people, deprived millions across the world of their livelihoods and ruined many businesses, will be felt over years to come. One immediate effect was that it demonstrated the dependence of our societies on the internet and its intermediaries. More than that, the crisis further increased this dependence as companies replaced business trips and conferences with online meetings, as schools and universities moved their teaching online, as people resorted to online shopping and online social gatherings instead of visiting each other, or going to restaurants, concerts or cinemas. In the face of the world's crisis, "big tech" reaped in record revenues and bolstered its corporate power further. The market capitalisation of the *GAFAM* jumped by over 53% between June 2019 and July 2020 reaching USD6.4 trillion. This was massively boosted by society's turn to the internet and the services of online intermediaries.[2050]

Without these services, to be sure, the disastrous impact of the pandemic would have been even greater, on a medical, social and economic scale. The internet has been essential for many people and their families, businesses and public services in a time of isolation and disruption.

Yet, the increasing reliance of people on online intermediaries like social media and online marketplaces has reinforced the serious challenges of unlawful content online. Dis- and misinformation, hate speech, extremist propaganda and counterfeit products have surged on the internet to unseen levels.[2051] They have reinforced general concerns about the stability of

---

2050 Richard Waters, Hannah Murphy and Patrick McGee, 'Big Tech Defies Global Economic Fallout with Blockbuster Earnings' (31 July 2020); 'Big 5 US Tech Giants Hit $6.4 Trillion in Market Cap, a 53% Jump in a Year – 24/7 Wall St.' <https://247wallst.com/technology-3/2020/07/21/big-5-us-tech-giants-hit-6-4-trillion-in-market-cap-a-53-jump-in-a-year/> accessed 20 August 2020; Peter Eavis and Steve Lohr, 'Big Tech's Domination of Business Reaches New Heights' *The New York Times* (19 August 2020)

2051 Hannah Murphy, Dave Lee and Siddharth Venkataramakrishnan, 'Facebook Groups Trading Fake Amazon Reviews Remain Rampant' *FT.com* (12 August 2020); Sylvain Rolland, 'Coronavirus : Internet infesté par les arnaques et les fake news' *La Tribune* (20 February 2020)<https://www.latribune.fr/technos-m

democratic societies.[2052] Traditional media, like newspapers and public television, which are bound to standards of fact-based research and integrity, have been displaced as news sources. The new information sources, however, do not subscribe to the same standards. They derive money from people uploading, reading, watching, sharing and commenting. The more users interact, the more money is gained through advertisements. The problem is that news distribution models which prioritise content that receives the most attention do not do well when it comes to promoting quality and unbiased information, which is essential in times of crisis.[2053] It does well, however, for the profit revenues of social media giants and other online platforms. The additional efforts of *Facebook, Twitter, Amazon, Google* and others to counter the tide of harmful and unlawful content were a start, but not more than that. They have not led to a significant change in the availability of unlawful content.[2054]

At the same time, the debate on the role and responsibilities of online intermediaries also shows a public change of mind. The neutral and merely technical nature of the early internet intermediaries of the 1990s and the Web 1.0 is largely seen as a thing of the past. Chapter 2 demonstrated that today internet intermediaries are not just essential for facilitating our access to the internet and information. They have also become the world's

---

edias/internet/coronavirus-internet-infeste-par-les-arnaques-et-les-fake-news-840839.html> accessed 20 August 2020; Deutscher Ärzteverlag GmbH Ärzteblatt Redaktion Deutsches, 'Onlinespiele und soziale Medien: Corona verstärkt die Sucht' [2020] *Deutsches Ärzteblatt* <https://www.aerzteblatt.de/archiv/214932/Onlinespiele-und-soziale-Medien-Corona-verstaerkt-die-Sucht> accessed 20 August 2020. Zoe Thomas, 'Misinformation on Coronavirus Causing "Infodemic"' *BBC News* (13 February 2020) <https://www.bbc.com/news/technology-51497800> accessed 20 August 2020.

2052 Jennifer Cobbe and Elettra Bietti, 'Rethinking Digital Platforms for the Post-COVID-19 Era' (*Centre for International Governance Innovation*, 12 May 2020) <https://www.cigionline.org/articles/rethinking-digital-platforms-post-covid-19-era> accessed 20 August 2020.

2053 Ben Scott and Taylor Owen, 'Governing Platforms after COVID-19' (*Centre for International Governance Innovation*, 18 August 2020) <https://www.cigionline.org/articles/governing-platforms-after-covid-19> accessed 20 August 2020.

2054 Dave Lee and Hannah Murphy, 'Facebook Fails to Curb Spread of Medical Misinformation, Report Finds' *FT.com* (19 August 2020). Hannah Murphy, Judith Evans and Alistair Gray, 'Facebook Accused of Failing to Deliver on Advertisers' Boycott Demands' *FT.com* (2 August 2020). Laura Urquizu, 'Counterfeiting Is a Bn-Dollar Problem. COVID-19 Has Made It Far Worse' (*Fast Company*, 4 May 2020) <https://www.fastcompany.com/90500123/counterfeiting-is-a-bn-dollar-problem-covid-19-has-made-it-far-worse> accessed 20 August 2020.

most powerful corporate actors. This happened on the back of a digital transformation instigated by Web 2.0 and its new interactivity. Online intermediaries evolved from technical facilities that hosted and enabled access to information of third parties to true information management systems. Third party information and the traffic resulting from it is a treasure trough of valuable marketing data. This means that platforms, far from being neutral, actively manipulate user interaction and take decisions on what content is seen by whom, and in which order. Even more so, they now own significant parts of the internet's infrastructure, making them systemically relevant for many essential services.[2055]

Chapter 3 outlined the challenges of adapting the law to these sweeping changes, which have caused a surge in unlawful content and harms that users are exposed to on a daily basis. Law, however, is known to be lagging behind. Considering the lightning changes that the internet has introduced, this is a major concern. The EU regulatory framework that regulates the liability exemption conditions of today's online platforms is based on assumptions that started to change already 15 years ago. At the time, the utilitarian policy view was that the budding internet sector needed to be protected against looming liabilities.

This work suggests that the three key challenges that courts and policymakers have grappled with, and which were analysed in Chapter 3, need to be resolved through a new responsibility framework. First, the neutrality condition that guarantees wide ranging exemptions from liability for the content hosted, sounds like an outlandish concept judged by today's realities. It is remarkable that companies like *Facebook* are to this day still seen as neutral, passive and mere technical facility providers by both national courts and the CJEU.[2056] National courts are, however, increasingly seeing online platforms as active parties. They even allocate primary or enhanced liabilities to these actors. Overall, however, the ECD liability exemption condition of neutrality is still interpreted in different ways across the EU.

Secondly, the definition of actual knowledge of unlawful activity or content has been problematic from the outset. For a start, NTD processes are not harmonised by the ECD. Yet, since actual knowledge for neutral hosts is tied to receiving a notification, courts have often had to go back and de-

2055 Stephan Bohn, Nicolas Friederici and Ali Aslan Gümüsay, 'Too Big to Fail Us? Platforms as Systemically Relevant' (*Internet Policy Review*, 11 August 2020) <https://policyreview.info/articles/news/too-big-fail-us-platforms-systemically-relevant/1489> accessed 20 August 2020.

2056 *Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18* (n 463) para 22.

fine when a notice, where it was not regulated by national law, would confer that knowledge. More importantly, the CJEU broke ground by defining the diligent economic operator duties for online intermediaries. This exploded the narrow concept of actual knowledge. Again, however, national courts indulged in varying interpretations even after *L'Oréal v eBay*. This is due to a variety of factors: different approaches to the question of neutrality, varying interpretations of due care, different intermediary business models, the concrete circumstances of the case at hand and courts' varying technical understanding and willingness to go deeper. It is also heavily determined by national secondary liability approaches. The actual knowledge standard concept, it is suggested, should be merged into a wider corporate responsibility standard in which a diligent economy operator would be assumed to know about certain activities that take place within its infosphere.[2057] Again, today's intermediaries are almost omniscient and highly sophisticated content governors. Exploiting and analysing data is at the very heart of their business model. It should also be at the heart of their efforts to prevent unlawful behaviour.

The third controversy concerns the scope of obligatory proactive infringement prevention efforts. This is intimately related to the above two issues. Again, the ECD is ambiguous here, because it gives courts and authorities the possibility to prevent specific infringements while forbidding the imposition of general monitoring. The concept of general monitoring, however, is not clearly defined. As content monitoring and filtering techniques have been making continuous progress, while details about their true use by major platforms remain unclear, this is a moving target for courts. It took courts considerable time to acknowledge more generally that stay-down orders did not result in general monitoring obligations where identical information is concerned. When it comes to similar kinds of content courts made varying assessments. The latest ruling by the CJEU on this matter seems to suggest that the decision could depend on the type of violation, with IP infringements being less likely to justify an expansion of proactive monitoring duties to similar violations. The semantic complexity of hate speech or defamation, by contrast, may justify a broader interpretation of proactive duties towards similar content, as long it does not involve human reassessment.[2058] The impact of broad monitoring duties for intermediaries on fundamental rights, such as freedom of speech, priva-

2057 Floridi (n 801).

2058 *Opinion of Advocate General Szpunar on Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18* (n 264) paras 68–69.

cy and the freedom to conduct a business is undisputed. This analysis suggests, however, that Article 15 ECD is an inappropriate tool in today's fast moving and diverse internet that will continue to cause more conflicting interpretations. Even more, the quest over finding the dividing line between general and specific monitoring duties has impeded the more important task of defining proportional and effective obligations for online intermediaries in the fight against unlawful content. Any decision over the proportionality of preventive measures, such as risk-based content filtering and monitoring, should be made on a more differentiated, sectoral basis. Different violations trigger different fundamental rights and call for specific balancing exercises. This could be done through a duty of care standard which allows for different scopes of responsibilities depending on the harm, or nature of violation.

Another realisation from Chapter 3 is that the patchwork of different liability assessments and outcomes is closely related to different national secondary liability approaches. If a future intermediary responsibility framework wants to drive legal predictability and uniform approaches in the EU digital single market, it would need to go down the politically thorny road of finding a solution that bypasses the application of national laws on intermediaries. The complexity of this issue becomes even more apparent in the sectoral analysis of Chapter 4.

This analysis has demonstrated the intricate differences that exist in the regulatory environment for unlawful content and the enforcement options available against intermediaries. In fact, the vertically layered, multi-level regulatory structure of the EU is enriched by sector specific rules with different vertical layering structures. In addition, many courts have been applying laws in a diagonal fashion,[2059] by borrowing from other content areas' intermediary concepts. Several atomising trends have been identified. First, the unharmonised nature of substantive law provisions, such as defamation, hate speech or the exceptions and limitations of copyright have made a unified application of the ECD almost impossible. The 1881 French Press Law or the 2013 UK Defamation Act are two examples where national laws impose specific intermediary rules. This ultimately affects the way online platforms' content management practices and duties are being seen on a normative level. For example, the difference in substantive law affects whether infringing content is seen as manifestly illegal, which, in

2059 Sophie Stalla-Bourdillon, 'Uniformity v. Diversity of Internet Intermediaries' Liability Regime: Where Does the ECJ Stand?' (2011) 6 Journal of International Commercial Law and Technology 51, 52, 57.

turn, plays into the assessment of the liability exemption conditions. This would need to be solved through further harmonisation at EU level, which in the case of defamation law appears improbable. It was attempted, for example, in the area of copyright through the recent DSMD. More harmonised areas, such as trademark law, product and food safety regulation and, to some extent, terrorist content and hate speech, promise to be more adapted to an EU wide intermediary responsibility framework.

Secondly, the limited and more general arsenal of secondary liability exemptions offered through EU law[2060] is eclipsed by a rich repertoire at Member State level. The ECD framework is superimposed on an elaborate national secondary liability landscape that exists in ordinary national law as well as in sectoral law. Next to the intrinsic problems and ambiguities of the ECD, this is probably the second most important factor for the disparate interpretation and application of the intermediary liability exemptions framework across the EU. As of today, legislators and courts use the ECD as an additional option to existing national intermediary provisions, in conjunction with them[2061] or by replacing them almost exclusively with local secondary liability approaches.

Third, regarding enforcement regimes, there are significant differences in the options available against intermediaries. In the public law dominated areas of terrorist content and product regulation, there is a marked engagement of law enforcement and surveillance authorities with intermediaries. In private law areas, concerning personality or economic rights, enforcement happens mainly through courts. Although this work did not address the sanctions regimes tied to intermediary obligations, it is suggested here that a specific framework that punishes non-compliance with a duty of care standards should be imposed by a new Digital Services Act, similar to the GDPR.[2062]

Lastly, the minimum harmonisation approach of the ECD also means that some Member States have developed their own NTD procedures, through law or self-regulatory arrangements, while others have not regulated this at all. This in turn has had an influence on the definition of the knowledge standard in the jurisdiction and in the content area concerned, as well as procedural obligations. A new duty of care standard would need to harmonise NTD procedures.

2060 Leistner (n 336) 78–89.
2061 Oster (n 816); Benabou (n 334).
2062 Regulation 2016/679 (GDPR) Articles 83 & 84, Recital 129.

Lawmakers at both EU and national level have reacted differently to these challenges. Many policy makers started off with self–regulatory initiatives that are explicitly supported through the ECD. With traction from online platforms lacking, some have followed this up with more interventionist policy action. The regulatory choices of these initiatives differ. In the area of copyright, the DSMD has now removed OCSSPs from the scope of the ECD. The new obligations of OCSSPs are to be put in place through self-regulatory arrangements between intermediaries and the rightsholder industry. The AVMSD uses a tentatively co-regulatory model in the fight against hate speech and content harmful for minors on VSPs. The proposed TERREG anti-terrorism online regulation ventures further into a more traditional rule-making approach. Amongst the national initiatives, the *NetzDG* favours a more self-regulatory approach, while the now largely defunct *Loi Avia* deployed co-regulatory measures.

Chapter 4 has shown that intermediary liability provisions and their enforcement appear to disintegrate into specific sectoral and even national practices. This work, however, warns against giving in to this seemingly more flexible and pragmatic approach. Abandoning horizontal principles of online intermediary responsibility risks ignoring essential commonalties that relate to the practices of today's online platforms. First, the pressure to allocate enhanced responsibilities to intermediaries is a common feature across all sectors analysed here. They all call for moral responsibilities that are commensurate with the intrusive and encompassing business models and their deep involvement and integration into the act of information intermediation. In some areas, such as copyright or trademarks, this has pushed legislators and courts even to allocating primary liability, thus breaking a regulatory paradigm. Whether this is justified or not, the analysis here supports the view that the distinction between neutral and active intermediaries is outdated and should be abandoned across all content sectors. Secondly, many of the large integrated platforms operate across different content areas and potentially give rise to several harms: platforms like *Facebook, YouTube* or *Twitter* may facilitate economic, personality, consumer protection and public security related harms. Common horizontal responsibility norms would make therefore for more legal certainty for both users and platform operators themselves. Third, online platforms work according to similar underlying business models and architectural design decisions. They are focussed on exploiting user data, or behavioural surpluses. Fourthly, at least the large, dominating platforms have expanded their automated content management practices to create systems that detect and remove unlawful content. They enforce mainly along their own

private content policies, which are driven by commercial concerns, with a secondary regard for the applicable laws. However, these policies remain largely hidden to those stakeholders most concerned by their application. These private content management practices have a significant impact on fundamental rights. The ubiquity and power of online platforms on the internet means that these private norms have become quasi law and the intermediaries akin to parallel states. They override the public interest criteria formulated and enforced by democratically elected governments. This tendency was observed in each of the content sectors analysed.

Chapter 5 showcased the problems authorities face when confronted with unlawful and unsafe products and food sold via online marketplaces. The case studies are exemplary for the capability gaps of enforcers and courts when confronted with the role of new actors that are regulated through a different regime. Regulators are either not familiar with or do not have the competencies to make use of the possibilities offered by the ECD. When, in addition, that regime provides generous liability exemptions to actors that play an essential role in the wide availability of regulated products, it has left MSAs at a loss to address the surge of non-compliant products on the internet. The main obstacles for an effective enforcement are formidable. The sheer amount and speed of unlawful products appearing (disappearing and re-appearing) on marketplaces across various jurisdictions has overwhelmed a system that is highly fragmented, relies on more complex and slower risk assessments and is weakened by budget constraints. Cooperation with online intermediaries appears to improve slowly, albeit from a low basis. It is, however, non-committal and piecemeal. The second problem is that enforcement authorities, although technical experts in their own field, are naturally not aware of the business models and technical functionalities of online platforms. They may therefore misjudge the real impact and influence that integrated online marketplaces have on the distribution of products.

However, the areas of product and food safety also pose unique chances and learnings for a new online intermediary responsibility framework. MSAs in the areas surveyed have knowledge about the legality and illegality of content. These kinds of enforcers do not exist in the area of IP rights or speech. The co-regulatory framework of the *New Approach,* harmonised technical standards and food safety certifications, provide structures that could be conducive to regulating intermediary responsibility.

Chapter 6 has explored the creation of such a *New Approach* style regulatory framework of online platform responsibility. Dissatisfaction with the current regime has generated an increasing number of proposals for a new

regulatory system. All of these envisage greater responsibilities of intermediaries for the content they host and exploit. The majority converge on the idea that the distinction between passive and active intermediaries should be a thing of the past. More than that, most agree that today's Web 2.0. platforms steer and manipulate user behaviour. Combined with emerging gatekeeping power to information and the autonomous sway over content management they exercise quasi-public functions. Many proposals advocate for a move from liabilities to responsibilities on the lines of CSR, duty of care and risk management. As much as they agree on these common points, they differ in scope and the regulatory choice. More systemic, horizontal proposals appear to favour public involvement, while sectoral and procedural approaches rely more on self-regulation.

This work proposes a co-regulatory approach that applies a horizontal, principles-based framework that imposes duty of care style responsibility tied to statutory harms. Such a system, it was argued, could exploit synergies between already existing sectoral approaches. It would also facilitate an easier interlinkage with other legal domains that have become crucial when addressing critical issues of online platform dominance, such as competition law, data protection or consumer law.[2063]

Self-regulation, although a 'natural' approach of internet governance may not be appropriate any longer, given the seriousness of the harms caused by unlawful content, the autonomous and elusive content management practices of large online platforms and their gatekeeping powers. Past self-regulatory attempts, it was shown, have also lacked traction and efficacy. Through co-regulation, the state would get a chance to reclaim authority in an area that is essential for the long-term stability of democratic societies and social justice. Imposing responsibilities on private actors to prevent harms that effect public interests and fundamental rights is also in line with wider trends of corporate social responsibility and risk-based management. Most online platforms are now big and sophisticated enough to manage such obligations. It would bring intermediary regulation into line with the way states have been trying to respond to the constant challenge of our modern societies.

Risk regulation, CSR or standardisation are all means, it was shown, to deal with the socio-economic changes brought about by information technology and globalisation. The above chapters have demonstrated the de-

2063 Tambini and Moore (n 232) 399–406; Valcke, Graef and Clifford (n 1653) 710–711.

gree to which the state has lost epistemic authority in this area[2064] and needs to rely on private expert networks.[2065] In the area of online platform regulation, expert knowledge and technical expertise is, however, dominated and influenced by online intermediaries. A co-regulatory system, such as proposed here, would keep oversight over public interest principles and fundamental rights under state authority. Such principles and the related harms would be established through a framework regulation that replaces the ECD. That new Act could reference the sectoral EU rules that address the defined harms. The use of technical standards for duty of care for each harm would capture the much-needed expertise of industry stakeholders, such as intermediaries, technology service providers, researchers and civil society stakeholders. This system allows for flexibility, both by allowing for the formulation of harm specific due diligence obligations and by being adaptable to technical developments. The technical (duty of care) standards could be referenced in the sectoral rules that are mentioned in the new framework ECD, such as for example the DSMD, the AVMSD, the MSR or a new TERREG.

Like with any regulatory system there are also risks. Standardisation and risk regulation, if set up without due care and clearly defined procedural safeguards, may be subject to regulatory capture. Regulators are in dire need to improve their governance readiness because they will need to assess and audit compliance with technical standards that impose fairness obligations on content algorithms, technical design principles and business models of online platforms. In the EU, technical standardisation faces some particular problems related to democratic legitimacy and accessibility.

However, this appears to be manageable compared to the profound challenges the EU and many other countries around the world face opposite the societal harms caused by the content intermediation practices of powerful internet platforms. It is time to put in place enhanced responsibilities that are in line with the power and influence these commercial intermediaries exert over expression, information and markets.

2064 Schepel (n 34) 25.
2065 Haas (n 38) 4–7. Chowdhury and Wessel (n 1845) 337.