4 From Parallel Tracks to Overlapping Layers

4.1 The Intimate Connection between Content and Data

The consolidation of platform powers raises concerns for constitutional democracies. Delegated and autonomous powers question the role of constitutionalism in protecting fundamental rights while limiting the exercise of powers. Nonetheless, the role of European digital constitutionalism cannot be entirely understood without examining another layer of complexity, precisely the intimate relationship between content and data in the algorithmic society. The challenges for fundamental rights like freedom of expression, privacy and data protection do not just come from platform powers but also from the blurring boundaries between the technological framework and legal regimes governing content and data.

At the end of the last century, the Union approached the liability of online intermediaries in relation to content and data in separate ways. While the e-Commerce Directive was introduced to govern the field of online content by defining the legal responsibility of online intermediaries concerning third-party illicit content,[1] the Data Protection Directive focused on regulating the processing of personal information.[2] Both systems provide definitions, pursue specific objectives and are encapsulated by different legal instruments. The legal divergence between the two regimes has also been expressly clarified by the

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000) OJ L 178/1.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31.

e-Commerce Directive whose scope of application does not include 'questions relating to information society services covered by Directives 95/46/EC and 97/66/EC'.[3] In other words, the Data Protection Directive and the e-Commerce Directive started running on parallel tracks from a legal point of view.

This political choice made perfect sense in the aftermath of the Internet. At that moment, online intermediaries were predominantly performing passive activities offering access or hosting services mainly to businesses rather than to billions of consumers. It is not a coincidence that the relationship between content and data was of limited concern for the European Commission when drafting the respective legal regimes. Online intermediaries offer services without interfering with the information they transmit and host while acting as processors in relation to the data uploaded by third parties. Therefore, the technological divergence between the field of content and that of data was one of the primary reasons for the legal divergence in the regulation of these fields.

In the meantime, the fields of content and data have experienced a process of technological convergence. Online intermediaries have become more active by offering services to share information which is indexed and organised through the processing of data.[4] Over the years, several actors have developed new services based on the processing of content and data. Together with the traditional providers of Internet access providers and hosting providers, new players have started to offer their digital services such as search engines (e.g. Google and Yahoo), platforms that allow communication, exchange and access to information (e.g. Facebook and Twitter), cloud computing services (e.g. Dropbox and

[3] e-Commerce Directive (n. 1), Article 1(5)(b). Recital 14 defines this rigid separation by stating that: 'The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC . . . and Directive 97/66/EC . . . These Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States'. However, the same Recital does not exclude that 'the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet'.

[4] Giovanni Sartor, 'Providers Liability. From the eCommerce Directive to the Future' (2017) in-depth analysis for the IMCO Committee www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf accessed 21 November 2021.

Google Drive), e-commerce marketplaces (e.g. e-Bay and Amazon) and online payment systems (e.g. Paypal).

This framework has inevitably affected the legal regimes of content and data. Despite the original parallel track, content and data have started to overlap even from a legal standpoint as an answer to the challenges driven by technological convergence. Within the framework of the Digital Single Market strategy, the Union has introduced new legal instruments indirectly leading to a legal convergence between content and data. In other words, the shift from parallel tracks to overlapping layers (or the move from technological and legal divergence to convergence) is a crucial piece of the puzzle to understand the framework in which platforms exercise their powers and shape democratic values. The blurred lines in the field of content and data are not neutral from a constitutional perspective. The technological convergence has challenged the parallel tracks in the fields of content and data, thus raising several challenges for the protection of legal certainty as well as fundamental rights.

Within this framework, the shift from parallel tracks to overlapping layers contributes to examining platform powers and understanding the role of European digital constitutionalism. This chapter aims to analyse the evolving technological and legal intersection between content and data in the algorithmic society. The first part examines the points of convergence and divergence between the legal regimes introduced by the e-Commerce Directive and the Data Protection Directive. In the second part, two examples underline how the relationship between the two systems has evolved, looking in particular at how technological convergence has led to overlapping layers between the two legal fields which were conceived on parallel tracks. The third part examines three paths of legal convergence in the phase of European digital constitutionalism.

4.2 An Evolving Relationship on Different Constitutional Grounds

At the end of the last century, the Union could not have foreseen how content and data would have started to become increasingly interrelated. When the liability regimes for content and data saw the light, there were no social media platforms, e-commerce marketplaces and other digital

https://doi.org/10.1017/9781009071215.005 Published online by Cambridge University Press

services. The role of intermediaries was merely that of passively offering storage, access and transmission of data across the network.

Within this framework, content and data were running on parallel tracks as also showed by the minimum interaction between the Data Protection Directive and the e-Commerce Directive. This gap was also the result of different constitutional paths for freedom of expression, privacy and data protection in Europe. When dealing with freedom of expression in Europe, it is possible to look at such fundamental right from at least three different perspectives. Freedom of expression is enshrined in the Charter and in the Convention as well as in each Member State's Constitution.[5] The predominance of freedom of expression in Europe finds its roots in the French Declaration of the Rights of Man and of the Citizen which protected 'the free communication of thoughts and of opinions'.[6] Since the nineteenth century, freedom of expression has been developed as an answer to the political power exercised by public authorities and then became the basis for protecting other rights such as the right to education and research.

Instead, the European path towards the constitutional recognition of privacy and data protection as fundamental rights started from the evolution of the concept of privacy in the US framework.[7] From a merely negative perspective, the right to be left alone, or the right to privacy, characterised by predominant liberal imprinting, has firstly emerged in Europe within the framework of the Convention. As will be examined in Chapter 6, this liberty has then evolved towards a positive dimension consisting in the right to the protection of personal data as an answer to the progress of the welfare state, the development of new automated processing techniques like databases[8] and then digital technologies.

Therefore, data protection in the European framework constitutes a relatively new individual right developed as a response to the rise of the information society driven by new automated technologies and, primarily, the Internet. In other words, if the right to privacy was enough to meet the interests of individuals' protection, in the information society, the widespread processing of personal data, also through automated means, has made it no longer sufficient to just safeguard

[5] Eric Barendt, *Freedom of Speech* (Oxford University Press 2017).
[6] French Declaration of the Rights of Man and of the Citizen (1789), Art. 11.
[7] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
[8] Alan F. Westin, *Privacy and Freedom* (Atheneum 1967).

privacy but has also led to complementing this negative protection with a positive dimension consisting of the right to data protection.

Nonetheless, even indirectly, the fields of content and data have shared some points of contact since the adoption of the Data Protection Directive and the e-Commerce Directive. Both instruments were adopted to face the challenges of new information technologies to the internal market.[9] As underlined in Chapter 2, the Union was more concerned with focusing on ensuring the smooth development of the internal market by pursuing a digital liberal approach. To ensure this goal, the Union underlined the need to protect fundamental values. On the one hand, the Data Protection Directive identifies the right to privacy and data protection as the beacon to follow to 'contribute to economic and social progress, trade expansion and the well-being of individuals',[10] whereas the e-Commerce Directive protects freedom of expression since 'the free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression'.[11] As a result, the two legal regimes have been conceived with a clear political perspective: ensuring the smooth development of the internal market by providing new rules and adapting fundamental freedoms to the new technological scenario.

These constitutional observations do not exhaust the relationship between the two systems. The parallel track between content and data is also based on other grounding differences between the two regimes. The e-Commerce Directive focuses on exempting online intermediaries from liability and tackling illegal content rather than establishing procedures in this case, while the Data Protection Directive follows the opposite path. European data protection law does not focus on

[9] Data Protection Directive (n. 2), Recital 4. Moreover, Recital 14 states that 'given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data'. e-Commerce Directive (n. 1), Recital 1. 'The European Union is seeking to forge ever closer links between the States and peoples of Europe, to ensure economic and social progress; in accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured; the development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples'.

[10] Data Protection Directive (n. 2), Recital 2.

[11] e-Commerce Directive (n. 1), Recital 9.

exempting secondary liability or prohibiting the processing of personal data but rather on tackling unlawful processing. The two regimes have been built on parallel tracks characterised by different focal points. On the one hand, the content regime under the e-Commerce Directive is based on secondary liability for third-party illegal content or behaviours. On the other hand, the Data Protection Directive has introduced a system of liability of the controller independent from third-party conducts.

However, even these considerations are just a part of the jigsaw. When focusing on the liability regime system of content and data, some scholars observed that the two regimes should not be considered as mutually exclusionary but should be understood beyond a literal interpretation.[12] Precisely, before the adoption of the e-Commerce Directive, the Commission recognised the horizontal nature of the liability of online intermediaries involving 'copyright, consumer protection, trademarks, misleading advertising, protection of personal data, product liability, obscene content, hate speech, etc.'.[13] Even after the adoption of the e-Commerce Directive, the Commission stressed the general scope of the liability of online intermediaries in relation to third-party content.[14] Besides, the e-Commerce Directive provides another clue when it specifies that different civil and criminal regime of liability at domestic level could negatively affect the internal market.[15] This interpretative provision could be understood as a goal towards harmonisation of the liability systems covering any type of online content to reduce legal fragmentation which would undermine the development of the internal market.

Within this framework based on a parallel track, content and data started to overlap at least in three cases.[16] First, when users commit an

[12] Mario Viola de Azevedo Cunha and others, 'Peer-to-Peer Privacy Violations and ISP liability: Data Protection in the User-Generated Web' (2012) 2(2) International Data Privacy Law 50.

[13] Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce (COM(97)0157 C4-0297/97), 203.

[14] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), COM(2003) 702 final.

[15] e-Commerce Directive (n. 1), Recital 40.

[16] Bart van der Sloot, 'Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe' (2015) 3 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 211.

infringement through online intermediaries' networks (e.g. defamation), the e-Commerce Directive applies, thus shielding the liability of online platforms. Therefore, online platforms are not liable provided that they remove the infringing content if they become aware of the users' illicit conduct. Second, when users infringe privacy and data protection rules through online intermediaries' networks, the Data Protection Directive applies in relation to users. In this case, platforms are liable just for primary infringements of data protection rules and not for users' illicit conducts. Third, where users infringe a right falling outside the scope of data protection rules (e.g. hate speech) and platforms are required to provide details about the infringing users or to implement filtering systems, both the e-Commerce Directive and the Data Protection Directive apply.

In the last case, it is possible to find a first (but indirect) point of contact between the two regimes. More specifically, in *Promusicae*,[17] a collecting society representing producers and publishers of musical and audiovisual recordings asked Telefonica, as access provider, to reveal personal data about its users due to alleged access to the IP-protected work of the collecting society's clients without authors' prior authorisation. The question referred to the ECJ was directed at understanding if an access provider could be obliged to provide such information to the collecting society according to the legal framework provided for by the Enforcement Directive,[18] the Infosoc Directive,[19] and the e-Privacy Directive.[20] The ECJ found that Member States are not required to lay down an obligation requiring intermediaries to share personal data to ensure effective protection of copyright in the context of civil proceedings. It is for Member States to strike a fair balance between the rights at issue and take care to apply general principles of proportionality. However, even in this case, although the system of content and data (in this case, the e-Privacy Directive) participated in the same reasoning of the ECJ, the mutual influence between the two regimes was still not clear at that time.

[17] Case C-275/06 *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU* (2008).
[18] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (2004) OJ L 195/16.
[19] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (2001) OJ L 167/1.
[20] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L 201/37.

Likewise, in *LSG*,[21] the ECJ recognised that the rules of the Enforcement Directive, the Infosoc Directive and the e-Privacy Directive do not prevent Member States from establishing a reporting obligation for online intermediaries concerning third parties' traffic data in order to allow civil proceedings to commence for violations of copyright. Even in this case, the ECJ specified that such a system is compatible with Union law provided that Member States ensure a fair balance between the different fundamental rights at stake. The same orientation was confirmed in *Bonnier Audio*,[22] where the ECJ stated that EU law does not prevent the application of national legislations which, in order to identify an Internet subscriber or user, allow in civil proceedings to order an online intermediary to give a copyright holder or its representative information on the subscriber to whom the Internet service provider provided an IP address which was allegedly used for an infringement.

The overlap between content and data started to be clear to the ECJ even in *Google France*.[23] According to the ECJ, Google 'processes the data entered by advertisers and the resulting display of the ads is made under conditions which Google controls'.[24] The court then observed that this activity does not deprive Google of the exemptions from liability provided for in the e-Commerce Directive. Likewise, in the *L'Oreal* case,[25] the court did not follow the aforementioned path, recognising, instead, that eBay processes the data entered by its customer-sellers. Besides, the ECJ observed that the provision of assistance like the optimisation of the presentation of the offers for sale in question or promoting those offers leads the provider to playing an active role since it controls the data relating to the offers. Therefore, '[i]t cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31'.[26] In these cases, the ECJ identified a connection between the data processed by the platform and its active role in relation to the exemption of liability.

[21] Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH* v. *Tele2 Telecommunication GmbH* (2009).
[22] Case C-461/10 *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB* v. *Perfect Communication Sweden AB* (2012).
[23] Joined cases C-236/08 to C-238/08 *Google France SARL and Google Inc.* v. *Louis Vuitton Malletier SA* (C-236/08), *Google France SARL* v. *Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL* v. *Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08) (2010).
[24] Ibid., 115.
[25] Case C-324/09 *L'Oréal SA and Others* v. *eBay International AG and Others* (2011).
[26] Ibid., 116.

Although these cases could provide a first overview of a primordial legal overlap between the regimes of data and content, both systems remained formally far from each other. In other words, this phase was still characterised by technological and legal divergence in the field of content and data. These considerations do not provide any significant ground for understanding how and why the two regimes have started to overlap. The parallel tracks in the legal regime of content and data are not just the result of the adoption of two different legal instruments but also of a different technological environment at the end of the last century. The next section examines how the rise of online platforms has triggered the technological convergence of content and data and underline the legal convergence of the two fields.

4.3 The Blurring Lines between Content and Data

Online platforms are complex creatures playing multiple roles in the algorithmic society. On the one hand, they operate as data controllers when deciding the means and the purposes of processing personal data, but they can also be considered processors for the data they host. On the other hand, platforms actively organise users' content according to the data they collect from users while also hosting content and relying on an exemption of liability for third-party illicit conducts.

Social media are the most evident example of the intersection between content and data. The moderation of content and the processing of data is not performed by chance. Expressions are moderated with the precise scope of ensuring a peaceful environment where users can share their ideas and opinions. These expressions are also data whose processing allows platforms to offer micro-targeting advertising services.[27] Likewise, search engines organise their content according to billions of search results for providing the best targeted services to attract advertising revenues. These examples do not exhaust the way in which content and data are increasingly converging from a technological perspective, but they can lead to defining the intimate relationship between the two fields.

[27] Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).

The blurring lines between content and data in the digital environment challenge these two systems based on parallel legal regimes. In the framework of content, online intermediaries are defined as entities offering access, caching or hosting services whose activity is exempted from secondary liability due to their passive nature.[28] These providers are shielded from liability due to the technical operations they perform. They can be liable when they start to play a more active role showing awareness of the content they host. In other words, the more providers perform their activities in an active way (e.g. creating content), the more they could be subject to liability. Access providers are not responsible provided that they do not initiate the transmission, select the receiver of the transmission, select or modify the information contained in the transmission.[29] Without focusing on caching providers,[30] hosting providers are not liable for the information stored in their digital spaces provided that two alternative conditions are satisfied. Firstly, online intermediaries are not liable when they do not have actual knowledge of illegal activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent. Secondly, the exemption of liability also covers the case when online intermediaries, upon obtaining such knowledge or awareness, act expeditiously to remove or disable access to the information.[31]

While there are no issues in considering Vodafone or Verizon as access providers and Facebook or Twitter as hosting providers, the situation is more complicated when focusing on search engines like Google (i.e. information location tool services). The definition of 'information society service' would cover their activities.[32] Nonetheless, it is not entirely clear if search engines fall under any of the three types of

[28] e-Commerce Directive (n. 1), Recital 42. 'The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored'.

[29] Ibid., Art. 12(1)(a–c).

[30] Ibid., Art. 13(1)(a–e).

[31] Ibid., Art. 14(1)(a–b).

[32] Ibid. According to Recital 18: '[I]nformation society services are not solely restricted to services giving rise to online contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive

service providers mentioned above. It is not by chance that the e-Commerce Directive clarifies that '[i]n examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services', thus leaving Member States this choice.[33]

Moving to the field of data, the Data Protection Directive adopts a different approach. It does not exempt online intermediaries from liability according to their passive roles but provides a comprehensive definition of data controllership.[34] 'Data controller' is indeed defined as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.[35] Within this framework, the data controller can be defined as the governor of personal data since it can exercise a form of decision-making.[36] This power consists of the possibility to select the 'purposes and means', thus subjecting the data subject's personal data to the goals of the data controller.[37]

Unlike the field of content, this definition reflects an active engagement rather than a passive and technical role. Online intermediaries falling within this definition govern the processing of personal data. In other words, these definitions reflect the lack of a common starting point between the two regimes. On the one hand, as far as the legal regime of content is concerned, online intermediaries are depicted as

them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data'.

[33] Ibid., Art. 21. The reasons for such a choice came from the passive activity of search engines which do not take editorial decisions over content. They are not either the source of information they index or able to remove this information online. For instance, Some Member States (e.g. Portugal and Spain) have considered search engine services as hosting providers. See Joris van Hoboken, 'Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU' (2009) 13 International Journal of Communication Law & Policy 1.

[34] The ECJ has shown how much this definition could be interpreted broadly. See Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* v. *Wirtschaftsakademie Schleswig-Holstein GmbH* (2018).

[35] Data Protection Directive (n. 2), Art. 2(d).

[36] Brendan Van Alsenoy, 'Allocating Responsibility Among Controllers, Processors, And "Everything In Between": The Definition of Actors and Roles in Directive 95/46' (2012) 28 Computer Law & Security Review 30.

[37] It is worth mentioning that this situation becomes more intricate when data controllership is exercised by more than one entity. In this case, two or more actors govern the processing of personal data and, therefore, determining which entity is in control or responsible could be not an easy question to answer.

passive entities responsible only when they perform activities as content providers. Whereas data controllers are the key players of the data protection system since they actively define the modalities according to which data is processed.

The data controller is not the only relevant figure in the field of data. The Data Protection Directive also provides the definition of 'processor', who is the 'natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.[38] It is evident how the role of data processors is subject to the data controllers' guidelines and, therefore, its role can be defined as passive rather than active. In other words, the data controller is the brain of data governance, the processor is the brawn. The definition of data processor fits with purely passive providers, that neither determine the means nor the purpose of the data processing. According to the WP29, '[a]n ISP providing hosting services is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If, however, the ISP further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing'.[39] Put another way, when online intermediaries only process data of third-party services such as hosting a specific website, they operate as mere passive providers and data processors. Whereas, when the data is processed for the purposes and according to the modalities defined by online intermediaries, this actor plays the role of an active provider and of a data controller.

As Erdos underlined, it is possible to identify '(i) those that are not only intermediary "hosts" but also only data protection "processors" (labelled "processor hosts"), (ii) those which are intermediary "hosts" but also data protection "controllers" (labelled "controller hosts") and (iii) those which are data protection 'controllers' and not intermediary "hosts" (labelled "independent intermediaries")'.[40] While the exemption of liability for online intermediaries was introduced to protect entities by virtue of their passive role, nowadays, the use of automated

[38] Data Protection Directive (n. 2), Art. 2(e).

[39] Working Party Article 29, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf accessed 21 November 2021.

[40] David Erdos, 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' (2018) 26 International Journal of Law and Information Technology 189, 192.

systems of filtering and processing preferences have led these entities to perform activities whose passive nature is hard to support. As a result, nowadays, some online intermediaries perform no longer a merely passive role, but they are increasingly involved in active tasks. Therefore, the old-school rules in the framework of online intermediaries could not fit within the algorithmic society where online platforms actively run their business at the intersection between content and data.

While mere hosting services would fall under the first category (passive provider/data processor), online platforms, such as social networks and search engines, are likely to fall under the second relationship (active providers/data controllers). Passive hosting providers such as web service applications do not choose how to process large amounts of data, but they limit themselves to offering hosting services playing the role of data processor. This shift should not surprise since, as examined in Chapter 3, online platforms process content and data for profit relying on automated decision-making technologies. This active role at the intersection between content and data transforms the role of online intermediaries from passive providers and data processors to active providers and data controllers.

These considerations are the grounding reasons to understand how online platforms play the double role of hosting providers and data controllers in the algorithmic society. This situation is the primary example of the technological convergence between the two fields which has been characterised by legal divergence since the end of the last century. The following subsections examine the evolution of this relationship by focusing on two landmark cases showing how technological convergence has challenged the legal regime of content and data, thus paving the way towards legal convergence overcoming parallel tracks.

4.3.1 Active Providers and Data Controllers

Looking at the Italian framework, the *Google* v. *Vivi Down* saga provides clues to understand the evolution of the relationship between content and data.[41] The case arose from a video showing an autistic boy being bullied by his classmates uploaded to the Google video platform.[42] This

[41] It is worth mentioning that this case is not the only example of how Member States have interpreted the intersection between the fields of content and data in the last years. Nevertheless, the Italian saga allows us to deal with the core of this chapter. See Erdos (n. 40).

[42] See Oreste Pollicino and Ernesto Apa, *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective* (Egea 2013); Giovanni Sartor and Mario

https://doi.org/10.1017/9781009071215.005 Published online by Cambridge University Press

situation involved both content, that is, in this case, the video itself as uploaded to Google Video, and data, most notably the health data of the victim which was ultimately processed through the hosting of the footage. It should thus not come as a surprise that the charges brought against the executives of Google concerned, on the one hand, the failure to prevent the crime of defamation against the minor, pursuant to Articles 40 and 595 of the Italian criminal code, and, on the other hand, the unlawful processing of personal data pursuant to Article 167 of Legislative Decree 196/2003.

The Court of Milan acquitted the defendants from the crime of defamation, excluding that Google, as a hosting provider, had an obligation to prevent crimes committed by its users.[43] Legislative Decree 70/2003, implementing the e-Commerce Directive in the Italian legal order, excludes the obligation to monitor content disseminated by users. Instead, the Milan Court of first instance condemned three executives from Google for the crime of unlawful processing of personal data, sentencing them to a six-month suspended conviction. According to the court, Google should have warned the uploaders about the obligations to respect when uploading online content as well as the consequences of potential violations.

The Milan Court of Appeals overturned the 2010 first instance ruling and found the Google executives not guilty of unlawful data processing.[44] Therefore, Google was not responsible for either defamation nor unlawful processing of personal data. The appeal decision was based on the general principle that Google was not aware of the content since it had no general duty to monitor user-uploaded content on its systems. Besides, the search engine could not be considered a data controller. Service providers were completely alien to the information stored when the e-Commerce Directive was introduced. However, according to the court, today such a statement is arguably not consistent any more with the state of the art. In today's world, the services that online intermediaries offer are not limited to the technical process that simply sets up and provides access to the network. They make possible for users to share their own content and other people's content on the

Viola de Azevedo Cunha, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (2010) 18(4) International Journal of Law & Information Technologies 15; Raul Mendez, 'Google Case in Italy' (2011) 1(2) International Data Privacy Law 137.

[43] Court of Milan, decision no. 1972/2010.

[44] Court of Appeals of Milan, decision no. 8611/2013.

network and they cannot escape from complying with data protection laws.

By recalling the decision of the court of first instance, the court observed that active hosting providers could be subject to more onerous duties than passive hosting providers. This extension of duties would descend from the organisation and selection of information. Data processing would then make online intermediaries aware of the indistinct flow of data. Nevertheless, the court clarified that this situation does not lead to a sort of chain reaction resulting in an extension of online intermediaries' liability for whatever third-party offences relating to the communication and upload of particular categories of data. In this case, the court argued that Google could not be considered a data controller.

The mix of these observations reflects how the layers of content and data tend to overlap. In this case, the core issue regards data protection since it concerns the assessment of the crime of unlawful data processing, so that the Data Protection Directive applies. As a result, Google could not rely on the exemption of liability since these rules are enshrined in a separate legal instrument whose scope of application does not extend to matters involving data protection. Nevertheless, the Milan Court of Appeals mixed the two systems in its reasoning with the result that the boundaries between the two regimes started to become increasingly blurred.

The Italian Supreme Court, upholding the decision of the Milan Court of Appeals, clarified the boundaries of the previous decision in relation to the qualification of hosting providers as data controller.[45] The Supreme Court dismissed the appeal of the public prosecutor confirming that hosting providers are not required to generally monitor data entered by third parties in its digital rooms. According to the court, although the illegal processing of personal data had occurred, as the video actually contained health data of the minor, this criminal conduct was only attributable to the uploader. The hosting provider was not aware of the illicit content and, as soon as the authority notified the provider, the content was promptly removed from the online platform.

In this case, the Supreme Court expressly addressed the topic of the coordination between the regime of the liability of online intermediaries and data protection, as implemented in the Italian legal order respectively by Legislative Decree 70/2003 and 196/2003. The court

[45] Italian Supreme Court, decision no. 5107/2014.

observed that the exclusion of data protection from the scope of application of Legislative Decree 70/2003 clarifies that the protection of personal data is governed by rules outside the scope of platform liability for hosting third-party content. Therefore, the two regimes should be interpreted together, meaning that the regime of online intermediaries clarifying and confirming the scope of the data protection regime. The role of the data controller implies the existence of decision-making powers with regard to the purposes, the methods of personal data processing and the tools used. Put another way, the data controller is the only subject who can fulfil these tasks. In the view of the Supreme Court, this role is compatible with the system of the e-Commerce Directive. Precisely, the court observed that as long as the illicit data is unknown to the service provider, this entity cannot be considered as the data controller, because it lacks any decision-making power on the data itself. When, instead, the provider is aware of the illicit data and does not take action for its immediate removal or to make it inaccessible in any case, it fully assumes the status of data controller.

The decision of the Supreme Court was based on a mix between the legal regimes of content and data. Even more importantly, this observation underlines a critical evolution of the role of online intermediaries whose neutral functions turned into a more active involvement characterised by the determination of the scope and purposes of personal data processing.

4.3.2 From the Takedown of Content to the Delist of Data

Another opportunity to examine the evolving relationship between content and data in the algorithmic society comes from the ECJ. Judicial activism has not only played a critical role in building a bridge between digital liberalism and the new phase of European digital constitutionalism but has also contributed to indirectly underlining how the regimes of content and data are destined to overlap in the framework of the algorithmic society. The *Google Spain* case is a landmark decision for several reasons but, for the purposes of this chapter, it is a clear example of convergence between the regimes of content and data.[46]

Without going back on the facts of the case and on the primary legal issues already underlined in the previous chapter and analysed by extensive literature,[47] it is interesting to highlight how, although the

[46] Case C-131/12 *Google Spain SL and Google Inc.* v. *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014).

[47] See Aleksandra Kuczerawy and Jef Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 Columbia Technology

Google Spain case focused on data protection law, it shares similarities with the field of content. Like in the framework of the e-Commerce Directive, the case concerns the removal (*rectius* delisting) of online content including personal data. Under Spanish law, this action would have triggered the responsibility of the search engine, as a hosting provider, to remove the content at stake. In the *Google Spain* case, however, the matter was addressed from the data perspective.

This case still shows some first steps towards legal convergence. The opinion of the Advocate General Jääskinen provides interesting clues, precisely, when he rejected the idea of search engines as data controllers.[48] This conclusion came from the interpretation of the notion of data controller based on the idea of 'responsibility' over the personal data processed 'in the sense that the controller is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their processing as personal data'.[49] This last view circularly comes back to the argument of the Italian Supreme Court when underlining the link between the notion of data controller and its responsibility in terms of awareness. This argument highlights the potential merge of the fields of content and data. In other words, the responsibility of data controllers results from their awareness when they process personal data, such as is the case of online intermediaries in the field of content. According to the Advocate General, the search engine provider just supplies an information location tool which does not make it aware of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. More particularly, he observed that '[i]n the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way'.[50]

Law Journal 219; Frank Pasquale, 'Reforming the Law of Reputation' (2015) 47 Loyola University of Chicago Law Journal 515; Oreste Pollicino and Marco Bassini, 'Reconciling Right to Be Forgotten and Freedom of Information in the Digital Age. Past and Future of Personal Data Protection in the EU' (2014) 2 Diritto pubblico comparato ed europeo 641.

[48] Opinion of the Advocate General Jääskinen in the case *Google Spain* C-131/12, 25 June 2013.

[49] Ibid., 82.

[50] Ibid., 84.

https://doi.org/10.1017/9781009071215.005 Published online by Cambridge University Press

The Advocate General did not exclude that upon certain conditions even a search engine does exercise control on personal data and may therefore be subject to the obligations set forth under the Data Protection Directive in its capacity as data controller. The owner of a search engine has control over the index and can filter or block certain content.[51] A search engine can be required to apply exclusion codes on source pages to prevent the retrieval of specific content. Even with respect to the cache copy of the content of websites, in the case of a request for its updating by the owner, the search engine has actual control over personal data.[52]

The assumption behind this finding is based on considering the liability of search engines dependent on their active role based on awareness. In light of that, the opinion reached the conclusion that Google could not be considered a data controller.[53] The conclusion of the Advocate General shows how the two legal regimes inevitably overlap. The assessment about whether a search engine can be considered a data controller has been based on legal arguments resembling the framework of the e-Commerce Directive. In other words, the impossibility to control personal data in the case of delisting was connected to a passive role incompatible with data controllership.

Focusing on the ECJ's decision, even though the court agreed that the indexing of information retrieved from the website of third parties amounts to a processing of personal data, this point has remained the only common finding between the opinion of the Advocate General and the decision of the court. As far as the divergence between the two approaches is concerned, it is when answering the question as to the nature of the search engine as data controller that the court takes an opposite path. The ECJ's decision firmly recognised that search engines are data controllers, especially because these actors play a decisive role 'in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published'.[54] Therefore, the ECJ abandoned the idea of awareness and responsibilities advanced by the Advocate General and focused on the current effects of

[51] Ibid., 92.
[52] Ibid., 93.
[53] Ibid., 100.
[54] C-131/12 (n. 46), 36, 37–40.

the search engines' activities. Put another way, the court dismantled any potential convergence going back to parallel tracks.

A critical point lies within the ECJ's observation that excluding search engines from the notion of data controller would be contrary to the objective of the provision, which is to ensure effective and complete protection of data subjects. In order to ensure an effective protection of data subjects, it is necessary to adopt a broader definition of data controller. This consideration is also explained by the interest of the ECJ in ensuring effective protection of the right to privacy as underlined in Chapter 2. The finding of the court in *Google Spain* does not seem to be supported by the actual manner in which search engines act when indexing third-party webpages, but rather by the crucial implications that said activity produces with regard to the protection of personal data. The argument advanced by the Advocate General, according to whom an online intermediary qualifies as data controller only upon certain conditions, is thus rejected. The search engine provider amounts to a data controller regardless of the fact that the owner of a website has chosen to implement exclusion protocols or taken other arrangements for excluding the content of the same from being retrieved. The fact that the owner of a website does not indicate that, in the view of the court, does not release the search engine from its responsibility for the processing of personal data carried out as such.

It cannot be excluded that defining search engines as data controllers would be incompatible with data protection law since these actors would not be able to comply with all the obligations applicable to data controllers.[55] It is worth underlining that, when recognising Google as a data controller, the ECJ has underlined that such role should be carried out 'within the framework of its responsibilities, powers and capabilities', thus providing a safety valve against the disproportionate extension of data protection law obligations to search engines.[56]

Although this part of the decision would show the lack of intention to reduce the gap between the legal regimes of content and data, an example of the blurring line between the two fields comes from the paragraphs of the decisions where the ECJ supported the right to delist by interpreting the provisions of the Data Protection Directive.[57] The ruling of the ECJ raises several questions on the legal regime of search

[55] Miquel Peguera, 'The Shaky Ground of the Right to Be Delisted' (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 507.
[56] C-131/12 (n. 46), 38.
[57] Data Protection Directive (n. 2), Arts. 12(b), 14(a).

engines in the field of data and content. The primary question is whether search engines' results have not been considered as third-party content since they are generated from content providers such as users and hosted by search engines as service providers. It is true that the ECJ was called to answer the questions raised by the national judge through the preliminary reference mechanism focused on data protection laws. Nonetheless, since the right to delist has been clustered within the framework of personal data, the application of the e-Commerce Directive is not under discussion. The *Google Spain* decision did not refer to the legal framework of the e-Commerce Directive. The ECJ just focused on whether Google should be considered subject to European data protection law and its obligations without thinking about the consequences for the moderation of third-party content subject to delisting. Without knowing it, the ECJ built an important bridge between the fields of content and data.

The exclusive focus on data protection law does not mean that the decision had not produced effects on the regime of liability in the field of content. In this case, the ECJ led to the creation of a new complaint-based system mirroring the notice-and-takedown system established by the e-Commerce Directive.[58] From a broader perspective, the decision affects the framework of liability of search engines. Despite the high level of protection of fundamental rights, the ECJ has also delegated to search engines the task of balancing fundamental rights when assessing users' requests to delist online content. The right to delisting provides a broader remedy than the obligation to remove required of online platforms in case of awareness of illicit content. Search engines are required to assess users' requests which should not be based on alleged illicit content but on their personal data. Therefore, platforms can exercise their discretion in deciding whether to proceed with the delisting, so that, in this case, search engines perform a 'data moderation' rather than a 'content moderation'.

The two takedown procedures are not identical but similar. The notice-and-takedown mechanism was introduced in the field of content not only as the result of the liability exemption to online intermediaries but also to incentivise these actors to keep their spaces clean from illegal

[58] Stavroula Karapapa and Maurizio Borghi, 'Search Engine Liability for Autocomplete Suggestions: Personality, Privacy and the Power of the Algorithm' (2015) 23 International Journal of Law & Information Technology 261.

content online.[59] The 'notice-and-takedown' and the 'notice-and-delist' mechanisms are different, especially since they come from two different legal frameworks. Notice-and-takedown aims to tackle illegal third-party content while, in the field of data, notice-and-delist deals with legal content linked by the search engines' activities. The former mainly concerns the liability for third-party behaviours while the latter focuses on platforms' primary misconducts.

Nonetheless, both procedures affect content. Even if, at first glance, the right to delist would address the removal of links to publication including personal data, such an activity is highly dependent on the content in question due to the balancing between data protection and freedom of expression. It is not by chance that Keller underlined that the case of the right to be forgotten online looks like 'a textbook intermediary liability law'.[60] Even more importantly, failing to comply with these systems upon receiving users' notice would lead search engines to be liable. The fact that engines are data controllers would mean that they can exercise a sort of control over information and, particularly, on personal data. This situation seems to be in contrast with the ban on general monitoring obligations established by the e-Commerce Directive. In other words, although the *Google Spain* case does not deal with the framework of content, this decision moves the notice-and-takedown approach from the field of content to data without assessing the technological and legal boundaries between the two regimes.

4.4 From Legal Divergence to Convergence

The regimes of content and data have already shown a certain degree of technological convergence in the digital environment. While the relationship data processor/passive provider (e.g. web hosting) does not raise particular issues, the second model (data controller/active provider) questions the legal separation of the two regimes.

Despite the increasing connection between content and data, at first glance, this intersection has not led the Union to adopt a new approach to platform liability in the framework of the algorithmic society. In the field of content, the Union has introduced new rules addressing the

[59] OECD, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives' (2011) www.oecd.org/internet/ieconomy/48685066.pdf accessed 21 November 2021.

[60] Daphne Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the Eu 2016 General Data Protection Regulation' (2018) 33 Berkley Technology Law Journal 297, 354.

https://doi.org/10.1017/9781009071215.005 Published online by Cambridge University Press

intersection between content and data.[61] A parallel track approach is still primary when looking at the Directive on Copyright in the Digital Single Market (Copyright Directive),[62] and the amendments in the framework of the Audiovisual Media Service Directive (AVMS Directive).[63] Similarly, the GDPR, as well as the Proposal for a Regulation on Privacy and Electronic Communications,[64] govern privacy and data protection law.

The rise of digital constitutionalism in Europe does not imply that the Union's approach can be considered coherent with the intertwined challenges in the fields of expressions and data. Within this framework, in *La Quadrature du Net*,[65] the ECJ addressed a case concerning the intersection between the legal regimes of content and data. The case concerned the lawfulness of Member States' legislation, laying down an obligation for providers of electronic communications services to forward users' traffic data and location data to a public authority or to retain such data in a general or indiscriminate way. The ECJ confirmed that EU law precludes this form of surveillance, precisely, the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combatting crime in general or of safeguarding national security.[66] For the

[61] Several European legal instruments provide a specific legal framework in respect of specific types of illegal contents online. In particular, Directive 2011/93/EU requires Member States to take measures to remove web pages containing or disseminating child pornography and allows them to block access to such web pages, subject to certain safeguards. Directive (EU) 2017/541 regards online content removal in respect of online content constituting public provocation to commit a terrorist offence. It should not be forgetting also Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, it is possible for competent judicial authorities to issue injunctions against intermediaries whose services are being used by a third party to infringe an intellectual property right.

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

[63] 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 303/69.

[64] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

[65] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* v. *Premier ministre and Others* (2020).

[66] See also Case C-207/16 *Ministerio Fiscal* (2018); Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB* v. *Post- och telestyrelsen* and *Secretary of State for the Home Department* v. *Tom Watson and Others* (2016); Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd*

purposes of understanding the relationship between content and data, it is worth stressing that the ECJ observed that the protection of the confidentiality of communications and of natural persons with regard to the processing of personal data in the context of information society services is governed only by European data protection law.[67] The court has not only underlined that this field falls within the field of data but also that 'the protection that Directive 2000/31 is intended to ensure cannot, in any event, undermine the requirements under Directive 2002/58 and Regulation 2016/679'.[68]

Notwithstanding the parallel tracks approach seems predominant from this formal perspective, the substantive margins of convergence between the field of content and data underline a trend towards legal convergence as driven by European digital constitutionalism. The convergence between these two systems can be analysed from at least three perspectives described in the next subparagraphs. Firstly, paths of convergence between content and data in the digital environment are the result of the relationship between freedom of expression and data protection at the constitutional level. If, on the one hand, these two fundamental rights have led to parallel legal regimes, on the other hand, they pursue the same constitutional mission to protect democratic values. Secondly, the regime of content is increasingly approaching the system of data based on procedural safeguards. The Union has shifted its attention to regulating the procedures based on which content is processed without dealing with their legal qualification. The third path of convergence looks at the overlapping layers between the regimes of liability in the field of content and data.

4.4.1 Constitutional Conflict and Converging Values

It is no mystery that the information society has increasingly raised the attention on the protection of freedom of expression, privacy and personal data. In the case of the Union, the threats of digital technologies implemented by transnational private actors are one of the primary reasons triggering the rise of a new phase of digital constitutionalism. Nevertheless, what is worth observing in this case does not only concern the risks for these fundamental rights but also the increasing paths

v. *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (2014).

[67] Joined Cases C-511/18, C-512/18 and C-520/18 (n. 65), 199.

[68] Ibid., 200.

of converging values between freedom of expression, privacy and data protection.

Even before the advent of online platforms, freedom of expression has met, firstly, privacy as the right to be left alone, and, then, data protection due to the rise of new processing technologies. For instance, the interest to access relevant information for the public interest typically clashes with the right to privacy. The notion of 'intellectual privacy' can show the intersection between private sphere and freedom of expression.[69] As underlined by Richards, intellectual privacy is 'a zone of protection that guards our ability to make up our minds freely'.[70] Surveillance affects not only privacy and data protection but also freedom of expression. Users cannot only be concerned about the control of their private spheres, but also limit the sharing of their opinions and ideas. This could also happen when digital technologies enabling the profiling of users' behaviours are used to manipulate opinions. The conflictual connection between expressions and privacy has become closer through the passing of time. Their interrelation has not basically changed with the rise of the information society. There has been an amplification of cases where these fundamental rights clash with each other.

In the European framework, the scope of the Data Protection Directive confirms this tension between data and content since it did not only introduce a broad notion of personal data but also covered models of processing and disseminating information protected by the right to freedom of expression enshrined in the Charter and the Convention. Therefore, it is possible to agree that 'from its inception, the entirety of European data protection has been correctly understood to be in inherent tension with such rights'.[71] Even beyond the extensive definitions in the field of data, the Data Protection Directive also provided a specific exemption from data protection obligations 'solely for journalistic purposes or the purpose of artistic or literary expression ... only if they are

[69] Julie Cohen, 'Intellectual Privacy and Censorship of the Internet' (1998) 8(3) Seton Hall Constitutional Law Journal 693.

[70] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* 95 (Oxford University Press 2015).

[71] David Erdos, 'From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection' (2015) 52 Common Market Law Review 119, 121.

necessary to reconcile the right to privacy with the rules governing freedom of expression'.[72]

It is also possible to observe that, as also indirectly suggested in *Lindqvist*,[73] the Data Protection Directive already embedded a certain balance by allowing data protection to influence the standard of the right to freedom of expression.[74] This system of exemption subjected the right to freedom of expression to the logics of the data protection system whose scope is likely to cover different forms of expressions.

There is not a general hierarchy between these two fundamental rights at the European constitutional level. Even in *Google Spain*, it is true that the ECJ recognised the prevalence of the fundamental rights of data subjects over the interest of Internet users to access information. At the same time, the ECJ observed that the balance may depend on 'specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life'.[75]

This clash is the result of two different constitutional goals aimed to protect conflicting rights like secrecy and public disclosure. In other words, the meeting of freedom of expression, privacy and data protection is the result of a conflict rather than a convergence between constitutional interests. From this perspective, the relationship between these rights can be defined as adversarial (freedom of expression versus privacy/data protection). The solution to this natural conflict has traditionally consisted of the balancing between fundamental rights made *ex ante* by lawmakers and *ex post* by courts.[76] At first glance, the conflict between these two rights could be considered a form of convergence since both rights contribute to influencing the scope of

[72] Data Protection Directive (n. 2), Art. 9. See *Google Spain* (n. 46); Case C-73/07 *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi Oy and Satamedia Oy* (2008) ECR I-9831.

[73] Case C-101/01 *Lindqvist* (2003) ECR I-12971, 82.

[74] Magdalena Jozwiak, 'Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union. The Vulnerability of Rights in an Online Context' (2016) 23(3) Maastricht Journal of European and Comparative Law 404.

[75] *Google Spain* (n. 46), 81.

[76] Eric Barendt, 'Balancing Freedom of Expression and Privacy' (2009) 1(1) Journal of Media Law 49.

protection of each other through balancing activities. Nevertheless, their clash can also be considered as an example of divergence since both systems aim to protect different rights from their constitutional perspective.

Although these considerations are still applicable in the algorithmic society, the relationship between freedom of expression, privacy and data protection is not only adversarial but also cooperative (freedom of expression and privacy/data protection). This cooperation lies in the joint mission underpinning these fundamental rights consisting of protecting democratic values. Freedom of expression, privacy and data protection are pillars of democratic societies. Without the possibility of expressing opinion and ideas freely, it is not possible to qualify a society as democratic. Likewise, without relying on the protection of the private sphere and procedures on the processing of personal data, it would not be possible to safeguard privacy and tackle an imbalance of powers between data controllers and subjects coming from the consolidation of an opaque sphere of data ignorance.

The common mission of these two fundamental rights emerged when examining the rise of a democratic phase of digital constitutionalism. Despite their natural conflictual relationship, both fundamental rights have shown their ability to provide the Union with constitutional instruments to answers platform powers. The measures adopted at the European level to regulate the process of content moderation and processing of automated decision-making processes are two clear examples of the mission of freedom of expression, privacy and data protection to protect democratic values in the algorithmic society. Their conflictual relationship can also be seen as a cooperative relationship linked by a common democratic goal.

4.4.2 From Content to Process

Another path of legal convergence comes from the transformation of content regulation that is now closer to the structure of data protection law grounded on procedural safeguards. The field of content is not structured on procedures but on qualifying and tackling illegal content. Put another way, the focus is on the *an* but not on the *quomodo*. The e-Commerce Directive does not introduce safeguards in the processing of content when online intermediaries process them as in the case of content moderation. It just defines the roles and responsibilities of online

intermediaries when dealing with illegal content. Hosting providers are just obliged to remove illegal content based on their awareness without any specific procedures. The e-Commerce Directive leaves Member States free to set further safeguards in this process without however requiring them to ensure a minimum and harmonised standard of protection.[77] The only limit is the ban for Member States to introduce general monitoring obligations applying to online intermediaries.[78]

On the other side, European data protection law provides rules governing the procedures for collecting, organising and making available personal data. It determines according to which conditions data should be considered personal, the role and responsibilities of controllers and processors as well as the procedures to follow in the processing of personal data. Failure to comply with this system triggers the liability of data controllers and processors. In other words, the data protection law framework does not care whether data are illicit per se, but whether their processing is unlawful. On the opposite, in the field of content, the focus is on substantive rather than procedural obligations.

The steps in the field of the Digital Single Market strategy have affected this original legal divergence. The fields of content and data look more similar in terms of structure and obligations. As examined in Chapter 2, the Copyright Directive and the AVMS Directive highlight this path of convergence. The Copyright Directive introduces several procedural safeguards in online platforms' content moderation of copyright content.[79] For instance, online platforms are required to put in place an effective and expeditious complaint and redress mechanism which users can access in the event of disputes over the disabling of access to, or the removal of, works or other subject-matter uploaded by them.[80] This obligation leads online platforms to proceduralising their activities like in the field of data. Likewise, the AVMS Directive provides a list of appropriate measures such as the establishment of mechanisms for users of video-sharing platforms to report or flag, or age verification systems for users with respect to content which may impair the physical, mental or moral development of minors. It is worth mentioning that the Union has not abandoned its focus on defining illicit content rather setting managing procedures. The TERREG still tends to define

[77] e-Commerce Directive (n. 1), Recital 46.
[78] Ibid., Art. 15.
[79] Copyright Directive (n. 62), Art. 17.
[80] Ibid., Art. 17(9).

illicit content.[81] The scope of terrorist content is limited by legal definitions and includes cases of incitement and solicitation.[82] At the same time, the TERREG introduces accountability and transparency safeguards in the moderation of terrorist content by hosting providers.[83] Therefore, despite the hybrid solution, this case is another example of how the process of moderation is increasingly going towards procedural obligations characterising the field of data.

The first examples of the shift from content to procedure are primarily the result of the new phase of digital constitutionalism. As discussed in Chapter 5, the Digital Services Act will be another critical step of this convergence, thus making the field of content closer to that of data. [84] It will increasingly move the perspective from content to process by providing horizontal procedural safeguards. The primary threats to freedom of expression in the digital age are connected to the lack of transparency and accountability in the moderation of content. To solve this imbalance of power, the structural shift from content to process has triggered a new path of legal convergence in the algorithmic society.

4.4.3 Content and Data Liability

The GDPR triggered the third path of legal convergence between content and data, precisely concerning the application of the system of the e-Commerce Directive in the field of data protection. The GDPR underlines that its scope should not affect the application of the rules provided for by the e-Commerce Directive, including the provisions on the liability of online intermediaries. However, while waiting for the adoption of the Digital Services Act, which has introduced the same provision in relation to the application of its rules without prejudice to European data protection law,[85] the provision limiting the scope of the e-Commerce Directive is still in force.

[81] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online OJ L 172/79.
[82] Ibid., Art. 2.
[83] Ibid., Arts. 9–11.
[84] 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.
[85] Digital Services Act (n. 84), Art. 1(5)(i).

A literal and narrow reading of the e-Commerce Directive would suggest that the liability exemption only applies to content without concerning the liability of online intermediaries for third-party data protection infringements or the liability of data controllers since these matters would be governed by the Data Protection Directive. As a result, even if online platforms can benefit from the exemption of liability established by the e-Commerce Directive, they remain liable for primary infringements in the field of data. As stated in the e-Commerce Directive, '[t]he implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards ... the liability of intermediaries'.[86] Likewise, the e-Commerce Directive states that 'the protection of individuals with regard to the processing of personal data is solely governed by [data protection laws], which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive'.[87]

Consequently, there are two potential interpretations. Firstly, nothing has changed since the GDPR could not affect the scope limitation established by the e-Commerce Directive. Secondly, it is possible to picture a potential convergence between the two legislative instruments since the GDPR states that its application should not prejudice the application of the e-Commerce Directive, especially concerning the liability of online intermediaries. However, it does not draw a clear line regarding the extension of online intermediaries exemption of liability in the field of data protection.

In the past, scholars addressed this question supporting the abolition of the 'data protection exceptionalism' according to which online intermediaries could not rely on the exemption of liability for third-party data.[88] The solution would consist of deferring to 'data-protection law for the specification of what processing of personal data is illegal, while giving providers immunity for all illegal processing taking place on their platform (including processing that is illegal because of violations of data protection law)'.[89] This perspective is also confirmed by the potential application of the safe harbour regime only to third-party

[86] e-Commerce Directive (n. 1), Recital 14.
[87] Ibid.
[88] Giovanni Sartor, '"Providers" Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?' (2013) 3(1) International Data Privacy Law 3.
[89] Ibid., 5.

content. The extension of this regime should not be considered as an exemption of liability from unlawful processing of personal data performed directly by online intermediaries. Whereas, in relation to online content violating data protection rules, in this case, online intermediaries could rely on the liability regime established by the e-Commerce Directive.

The potential applicability of the e-Commerce Directive in the field of data would not put aside the other provisions of data protection law. On the opposite, it would just lead to derogating provisions of liability for the distribution and storage of third-party content infringing data protection law which would remain the normative point of reference to assess the lawfulness of users' content. Nevertheless, it is worth underlining that an exemption of liability in this case would raise challenges when online intermediaries are also data controllers, so that they would have an active role in processing third-party content infringing data protection law.

Other limitations to the application of the e-Commerce Directive can also be found in the GDPR itself such as the exclusion of the application of data protection rules for 'purely personal or household activity'.[90] However, in this last case, it is necessary to mention that Recital 18 excludes these activities from the scope of the GDPR except for the case in which data controllers or processors provide the means for processing personal data for such personal or household activities.[91] As a result, according to this interpretative provision, even in this case, online intermediaries could be subject to the application of the GDPR while they could rely on their exemption of liability in the field of data if users process data within the scope of the aforementioned exception.

Besides, the GDPR does not refer to the e-Commerce Directive when addressing the liability of data controllers and processors. Regarding the liability of the data controller, the GDPR provides that a controller or processor shall be exempt from liability if they prove that they are not in any way responsible for the event giving rise to the damage. At this point, it would be possible to argue that online intermediaries as passive providers when exercising their functions as data controllers or processors should not be considered liable for third-party conducts.[92] It is necessary to observe that, unlike the Data Protection Directive, the

[90] GDPR, Art. 2(2)(c).
[91] Ibid., Recital 18.
[92] Ibid., Art. 82(3).

GDPR does not provide examples of how a controller might prove the lack of any liability: *force majeure* or error on the part of the data subject.[93] Although the provision could be interpreted in the same meaning that it refers only to events beyond the control of the controller or the processor, however, it is not clear whether even this provision could be used as a defence against third-party illicit behaviours.

These interpretations underline the overlap between the two fields. The extension of the regime of the e-Commerce Directive to third-party content infringing data protection law could also come from a constitutional interpretation based on the balancing between platforms' freedom to conduct business and users' fundamental rights. It is possible to observe that the extension of the scope of the e-Commerce Directive would increase uniformity in online content moderation.[94] If online intermediaries were able to rely on the safe harbour against illicit data processing perpetrated by third-parties, their content moderation processes could benefit from a general extension also to that online content in terms of the freedom to conduct business of online intermediaries. This is also why Keller underlined that the extension of the e-Commerce rule to the field of data would be a matter of fairness.[95]

Since the e-Commerce Directive allows Member States to impose injunctions and filtering systems to online intermediaries to address specific cases, a downside of the potential positive effects of such a system could be the risk of intermediaries encourage intermediaries to proactively monitoring data, most notably personal data, disseminated through their platform as a means to tackle third-party violations. Since, in the algorithmic society, online intermediaries play a more active role in processing data and performing content moderation, this safe harbour extension could encourage platforms to increase their monitoring activities with potential chilling effects for freedom of expression and with troubling effects also on other users'

[93] According to Recital 55, '[A]ny damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive'.

[94] Brendan Van Alsenoy, 'Liability under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 9(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 271.

[95] Keller (n. 60).

https://doi.org/10.1017/9781009071215.005 Published online by Cambridge University Press

fundamental rights like privacy.[96] Besides, the lack of harmonisation between different systems of notice-and-takedown conflicts with the GDPR's harmonisation goal.

It should also not be neglected that allowing online platforms to benefit from the exemption of liability even for third-party content infringing personal data could reduce the procedural safeguards limiting platforms powers. The e-Commerce Directive framework does not provide safeguards in this process. Therefore, users could not complain against platforms' refusal to remove certain data due to the fact that platforms are free to decide the fate of the information they host, especially when that information is likely not to be illicit, such as in the case of delisting requests. Instead, the GDPR recognises data subjects' rights. Even if, as already stressed, these obligations could be an incentive for online intermediaries to extensively monitor their spaces to escape responsibility, however, it is also a way to require them to take users' requests seriously. This framework will raise less concerns once the Digital Services Act is adopted introducing procedural safeguards even in the field of content.

As a result, it is worth wondering how *Google Vivi Down* and *Google Spain* would have been adjudicated if the GDPR was in force at that time. In the lack of judicial interpretation about the two regimes of liability, it is not possible to foresee how the Italian courts and ECJ would have interpreted the two cases. According to this system, as underlined in *La Quadrature du Net*, the ECJ can decide which regime applies by putting aside one of them. Besides, the adoption of the Digital Services Act would not contribute to clarifying this relationship since it just provides that the scope of application should be without prejudice to the application of the GDPR.[97] The only clarification introduced by the Digital Services Act, which adopts the same approach of the GDPR in terms of limiting its scope in relation to European data protection law, concerns the information relating to advertisement, which should be without prejudice to the provision of the GDPR relating to 'the right to object, automated individual decision-making, including profiling and specifically the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising'.[98] One of the primary

[96] See Case C-70/10 *Scarlet Extended SA* v. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011); Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v. *Netlog NV* (2012).

[97] COM(2020) 825 final (n. 84), Art. 1(5)(i).

[98] Ibid., Recital 52.

consequences of this approach is to blur the boundaries between the two regimes, precisely between the notion of 'data controller' and 'active provider' affecting the application of the rules in the field of content and data.

4.5 The Challenges Ahead in the Field of Content and Data

The relationship between content and data has increasingly become intimate with the rise and consolidation of the algorithmic society. Online platforms have led to revolutionary changes in the processing of information and data. Different types of data are published and mixed with other information through systems that organise, promote and aggregate content. From a first phase of technological and legal divergence at the beginning of this century, the legal regimes of online intermediaries and data have slowly started a dialogue triggered by a trend of technological convergence.

From the first contact in *Promusicae*, such a relationship has become more blurred with the advent of online platforms whose business was based on data-driven models. Both layers have started to technologically overlap when focusing on online intermediaries such as search engines and social media which do not merely perform the activity of data processors or passive providers any longer. In *Google Vivi Down* and *Google Spain*, the interpretation of the Italian courts and the ECJ highlighted the complexities in applying a rigid separation between the two systems. The mix of active provider and data controller implies that the rigid distinction in the application of the two regimes (and their parallel track) is questioned by the passive role of online intermediaries. Put another way, if it is not a surprise that the e-Commerce Directive excluded privacy and data protection matters from its scope of application, nowadays, the same political choice would look different when applied to online platforms.

The Union has maintained a system based on a parallel track even in the framework of the Digital Single Market Strategy. There are paths of legal convergence increasingly highlighting the relationship between content and data. Despite the historical differences between the two fields in question, freedom of expression and data protection have shown their ability to overcome the aforementioned legal divergence by sharing the common goal to protect democratic values. This trend is

evident in the phase of digital constitutionalism where, as examined in Chapter 2, the need to protect both fundamental rights has led to a positive regulatory reaction. Likewise, the introduction of procedural safeguards in the field of content is another critical sign of convergence towards the creation of a more transparent and accountable digital environment. The introduction of the Digital Services Act could contribute to providing horizontal procedural safeguards reflecting the system of data protection. Besides, the system of liability in the field of content and data is another example of potential legal convergence even if, in this case, it is still not clear whether the GDPR opens the doors towards overlaps between the two regimes in terms of responsibilities and liability for third-party content and data.

Therefore, although the two systems have been conceived as being on parallel tracks, the path of European digital constitutionalism has led to legal convergence as an answer to technological convergence. It would not be hazardous to argue that the evolution of artificial intelligence technologies will increasingly lead the two systems to collide where data controllers and hosting providers decide how to exploit the value coming from the interrelation of content and data. The cases of content moderation and automated decision-making processes provide some clues of this evolution. Therefore, they deserve to be further analysed within the framework of European digital constitutionalism designing a path to protect fundamental rights and democratic values in the algorithmic society.