European University Institute
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

WORKING PAPERS

RSCAS 2019/36
Robert Schuman Centre for Advanced Studies
Centre for Media Pluralism and Media Freedom

The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?

Giovanni De Gregorio

European University Institute

Robert Schuman Centre for Advanced Studies

Centre for Media Pluralism and Media Freedom

The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?

Giovanni De Gregorio

EUI Working Paper **RSCAS** 2019/36

ISSN 1028-3625

Printed in Italy, May 2019
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

Centre for Media Pluralism and Media Freedom (CMPF) Working Paper Series on 'Freedom and Pluralism of the Media, Society and Markets' benefits from contributions from the CMPF's fellows as well as from leading scholars and experienced practitioners interested in and focused on the subject matter. The Working Papers Series aims at assessing theoretical issues, specific policies, and regulatory questions.

The Centre for Media Pluralism and Media Freedom is co-financed by the European Union. This initiative is a further step in the European Commission's on-going effort to improve the protection of media pluralism and media freedom in Europe and to establish what actions need to be taken at European or national levels to foster these objectives.

The aim of the EUI Centre for Media Pluralism and Media Freedom is to enhance the awareness of the importance of freedom and pluralism of the media, to contribute to its protection and promotion and to develop new ideas among academics, policy makers, regulators, market stakeholders, journalists, and all other directly involved professionals who take part in the public debate.

Abstract

The legal regimes of online intermediaries' liability and data protection have been conceived on parallel tracks. Whereas the Data Protection Directive could not exclude from its scope of application the e-Commerce Directive due to chronological reasons, the latter expressly clarified that its scope does not include data protection matters. The rise of the algorithmic society has blurred this traditional gap. From a merely passive role, new online intermediaries such as search engines and social networks have acquired an increasingly active role in managing online contents. At the same time, their role in deciding how to process personal data has transformed these actors from data processors to controllers. This evolving framework has led to the convergence of the parallel tracks which have started to overlap. In particular, the ECJ decision in Google Spain and the Italian Google Vivi Down saga have shown the intersections between the two regimes. The adoption of the General Data Protection Regulation (GDPR) has contributed to reducing the gap between the regimes of data protection and ISP liability. The GDPR has clarified that the application of the new Regulation should not affect the rules provided for by the e-Commerce Directive, in particular, those regarding ISP's liability. The result could be a potential overlap of two layers which, until the adoption of the GDPR, were conceived from two different perspectives.

Keywords

e-Commerce Directive; GDPR; Privacy; Data Protection; ISP liability; Active providers; Data controller

1. Introduction

The legal regimes of online intermediaries' liability and data protection have been conceived from different perspectives. The first area – intermediary liability – focuses on the legal responsibility of Internet Service Providers (hereinafter, 'ISP') concerning third-party illicit actions occurring within their digital boundaries. The second field – data protection – focuses on regulating the processing of personal information. Both systems provide definitions, pursue specific objectives and are encapsulated by different legal instruments. In other words, the two regimes run on parallel tracks.

Within the EU framework, Directive 95/46/EC (hereinafter, 'Data Protection Directive'),[1] and Directive 2000/31/EC (hereinafter, 'e-Commerce Directive') are the reason for such an original sin.[2] Indeed, Article 1(5)(b) of the e-Commerce Directive expressly excludes from its scope of application matters involving data protection issues. This political choice perfectly makes sense in the aftermath of the Internet. At that moment, online intermediaries were predominantly performing passive activities offering access or hosting services.[3] The web was mainly populated by websites hosting text and small images. It is no by coincidence whether privacy and data protection were not of concern for the European Commission when drafting the ISPs' exemption from liability for third-party illicit behaviours. This system, named 'safe harbour', was essentially based on the premise that online intermediaries offer services without interfering with content and data online.

In the meantime, providers had become more active by offering services to share information which is indexed and organised over the Internet.[4] Over the years, several actors have developed new services based on different business models. In fact, 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 (eg Google or Yahoo), platforms that allow communication, exchange and access to information (eg Facebook, Twitter), cloud computing services (eg Dropbox or Google Drive), e-commerce marketplace (eg e-Bay and Amazon), online payment systems (eg Paypal). Such modern intermediaries are based on data-driven business models where profits derive mostly from tailored advertising thanks to the processing of large amounts of data allowing user's profiling. Algorithms and artificial intelligence technologies allow such actors to process users' information extracting value from data which is the oil of the algorithmic society.[5] Indeed, online intermediaries are peculiar not only for their system of liability but also under data protection law. On the one hand, they could operate as data controllers when deciding how and for which purposes process personal data of their users. On the other hand, these actors actively organise user-generated contents according to the data they collect.

At first glance, today, the lack of coordination between the two systems could appear unreasonable. The relationship between online intermediaries and data has started to become self-evident. The European Commission has shown to be aware of this situation. It is no coincidence if one of the objectives of the Commission in the framework of the Digital Single Market strategy is to ensure that online intermediaries (or platforms) 'protect core values' and increase 'transparency and fairness for

---

1 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.

2 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').

3 See Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer, 2017).

4 Giovanni Sartor, 'Providers Liability. From the eCommerce Directive to the Future' (2017) In-depth analysis for the IMCO Committee <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/ IPOL_IDA(2017)614179_EN.pdf> accessed 2 December 2018.

5 'The world's most valuable resource is no longer oil but data', The Economist (2017) www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

maintaining user trust and safeguarding innovation'.[6] This is because of the role of online platforms in giving access to information and contents to society and, as a result, their impact on users' fundamental rights. As the Commission stressed, this role implies 'wider responsibility'.[7]

There are at least two paths which the EU policy is following picturing a new approach to ISP liability system in the framework of the algorithmic society. The first path is based on hard law obligations to online intermediaries.[8] This approach is evident when looking at the Directive on Copyright in the Digital Single Market,[9] and the amendments in the framework of the AVMS Directive.[10] The second track is based on soft-law regulatory solutions through which the Commission is trying to establish standards for increasing transparency and introducing due process provisions in platforms' decision-making.[11]

However, there is also a third way. The recognition of the crucial role of online intermediaries in the digital environment has also been shown by the extension of the scope of application of Regulation 679/2016 (hereinafter, 'GDPR'),[12] as well as by the Proposal for a Regulation on Privacy and Electronic Communications.[13] Indeed, the GDPR has not only reviewed the EU privacy and data protection legal framework increasing the degree of uniformity between Member States' legislation, but it has challenged the historical gap between the system of the e-Commerce Directive and that of the Data Protection Directive. More specifically, Article 2(4) GDPR provides that 'this Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive'. In terms of ISP's liability for third-party contents, on the one hand, this system would allow online intermediaries to rely on the 'safe harbour' exemption also for third-party contents violating data protection rules as prescribed by GDPR. On the other hand, such an extension would also imply that some online intermediaries – especially

---

6 Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' COM(2016) 288 final.

7 Ibid.

8 See, for example, the proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online, COM(2018) 640 final. Several EU acts 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.

9 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.

10 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.

11 Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online C(2018) 1177 final. See, also, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, COM(2017) 555 final.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

13 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.

hosting providers – could be subject to liability for their dissemination in case of knowledge or awareness according to Article 14 of the e-Commerce Directive.

Within this framework, this work aims to analyse the evolving relationship between the systems of online intermediaries' liability and data protection to understand how and why the two regimes have started to converge in the algorithmic society. In order to achieve this objective, the first part of this work examines the points of contact between the e-Commerce Directive and the Data Protection Directive. In the second part, their evolving relationship is contextualised in the framework of the algorithmic society by providing two examples of judicial interpretation concerning the relationship between the two systems. The third part of this work focuses on the GDPR scope of application underlining the challenges about such a new potential overlapping.

2. An Evolving Relationship

If someone looks at the Internet when the two regimes saw the light, it would be likely to find a digital world without social media platforms, e-commerce marketplaces and other digital services. The role of intermediaries was merely passive offering storing, access and transmission of data across the network.

Within this framework, the Data Protection Directive was adopted in 1995 with the aim to ensure the free flow of personal data from one Member State to another while protecting the fundamental rights of individuals, especially, the right to privacy.[14] Only five years later, the e-Commerce Directive was adopted. Even in this case, the aim was to ensure the free movement of information society services and, at the same time, respect freedom of expression as enshrined in Article 10(1) ECHR.

Whereas the Data Protection Directive could not exclude from its scope the e-Commerce Directive due to chronological reasons, the latter expressly clarified that its scope of application does not include 'questions relating to information society services covered by Directives 95/46/EC and 97/66/EC'.[15] From this point, the Data Protection Directive and the e-Commerce Directive started to run on parallel tracks.

Although this restriction could limit any kind of relationship between the two instruments, it is possible to underline some constitutional point of contacts. Both Directives were adopted in order to face the challenges of new information technologies for the internal market.[16] The primary concern was

[14] Data Protection Directive, Recital 2-3.

[15] E-Commerce Directive, Article 1(5)(b). Recital 14 would define 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 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 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector 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 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'.

[16] Recital 4 of the Data Protection Directive recognises that 'the progress made in information technology is making the processing and exchange of such data considerably easier'. 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'. Recital 1 of the e-Commerce Directive states: '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

to avoid that the development of new digital technologies could frustrate EU fundamental freedoms. However, the threats for the internal market were not the only similarity. Indeed, even more importantly, both instruments refer to the need to protect the fundamental rights of individuals. On the one hand, the Data Protection Directive identifies the right to privacy and data protection as the beacon to follow,[17] whereas, the e-Commerce Directive finds its constitutional root in the protection of freedom of expression.[18] As a result, despite the original gap, the two regimes have been conceived with a clear political perspective: on the one hand, ensuring the smooth development of the internal market adapting fundamental freedoms to the new technological scenario and, on the other hand, protect individuals' fundamental rights.

At this point, these considerations could not constitute a significant ground for understanding how and why the two regimes have started to overlap. However, as it will be described below, this common constitutional standpoint has allowed the two regimes to pursue the same objectives in order to react to common challenges which were not still emerged when the two measures were adopted.

These observations do not exhaust the considerations about the relationship between the two systems. More specifically, some scholars observed that the two regimes should not be considered as mutually exclusionary but needs to be understood beyond a literal interpretation.[19] In particular, before the adoption of the e-Commerce Directive, the Commission recognised the horizontal nature of the ISP's liability involving 'copyright, consumer protection, trademarks, misleading advertising, protection of personal data, product liability, obscene content, hate speech, etc.'.[20] Even after its adoption in 2000, the Commission stressed the general scope of the e-Commerce Directive in relation to third-party contents.[21] Moreover, another clue would be directly provided by the Directive. Indeed, Recital 40 specifies that different civil and criminal liability regime of Member States could affect negatively the internal market. This interpretative provision could be understood as an extension of the scope to any type of online contents in order to reduce legal fragmentation across Member States.[22]

However, even these teleological considerations are only a small part of the jigsaw. Therefore, it is possible to classify at least three types of cases where the two regimes apply in relation to the liability of online intermediaries for third-party infringements.[23] First, when users commit an infringement

---

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'.

17 Data Protection Directive, Recital 2: 'Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals'.

18 E-Commerce Directive, Recital 9: '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 as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression'.

19 Mario Viola de Azevedo Cunha et al., 'Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web' (2012) 2(2) International Data Privacy Law 50.

20 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.

21 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.

22 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.

23 Ibid.

through online intermediaries' networks (e.g. trademark infringement), the e-Commerce Directive applies. Second, when users infringe privacy and data protection rules through the online intermediaries' networks, the Data Protection Directive applies. Third, where an infringement of a right different from data protection one has been initiated by a user and online intermediaries are asked to provide the detail of the user (i.e. personal data) or to implement filtering systems, both the e-Commerce Directive and the Data Protection Directive applies.

In the last case, it is possible to find a first (but indirect) point of contact between the two regimes. More specifically, in *Promusicae*,[24] a collecting society representing producers and publishers of musical and audiovisual recordings, asked Telefonica, an access provider, to reveal personal data about its users, since users were allegedly accessing the IP-protected work of the collecting society's clients without authors' prior authorisation. The question referred to the ECJ was directed to understand if an access provider was obliged to provide such information to the collecting society. The Court found that Member States are not required lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings and when interpreting these Directives, Member States must strike a fair balance between the rights at issue and must take care to apply general principles of proportionality. However, even in this case, although the Data Protection Directive and the e-Commerce Directive participated in the same reasoning of the ECJ, it was not clear the mutual influence of the two regimes at that time.

Likewise, in *LSG*,[25] the ECJ recognised that the rules of the Enforcement Directive,[26] as well as those of the e-Privacy Directive,[27] 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 has 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*,[28] where it was stated that EU law does not prevent the application of national legislation which, in order to identify an internet subscriber or user, allow in civil proceedings to order an ISP 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 in an infringement. Although these cases could provide a first overview of a primordial overlap between the two regimes, both systems remained formally far from each other.

3. The Link Between Data Controller-Active Provider in the Algorithmic Society

The above-mentioned cases have provided the first clues regarding how the gap between the two regimes has started to converge. In order to move forward, it is necessary to step back and focus on how ISPs and data controller have originally been defined.

---

[24] Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU [2008].

[25] Case C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH [2009].

[26] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

[27] 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.

[28] Case C-461/10 Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB [2012].

A brief look at the definitions reveals the original gap. ISPs are defined as entities offering access, caching or hosting services whose activity is of passive nature.[29] More specifically, their passive nature is reflected in their liability system. Firstly, access providers (or *mere conduit*) which offer services consisting of the transmission in a communication network of information provided by a recipient of the service are not responsible provided that '(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission'.[30] Secondly, caching providers are not liable if '(a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement'.[31]

Thirdly, hosting providers are not liable for the information stored in their digital spaces provided that '(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information'.[32]

Moving to the field of data protection, the data controller is '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'.[33]

These definitions reflect the lack of a starting common point between the two regimes. Indeed, ISPs are depicted as passive entity 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.

However, the data controller is not the only relevant figure defined by the Data Protection Directive. This Directive also provides the definition of 'processor', which is the 'natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'.[34] This definition fits with purely passive hosting providers, that neither determine the means nor the purpose of the data processing.[35] According to the Opinion 1/2010 of WP29: 'An 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'. Put another way, when online intermediaries only process data of third-party services such as hosting a

---

[29] E-Commerce Directive, 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'.

[30] E-Commerce Directive, Article 12.

[31] Ibid, Article 13.

[32] Ibid, Article 14.

[33] Data Protection Directive, Article 2(d).

[34] Ibid, Article 2(e).

[35] Working Party 29, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010).

specific website, they operate as mere passive providers and data processor. Whereas, when the data is processed for the purposes and according to the modalities defined by online intermediaries, this actor plays the role of active providers and data controller.

Online intermediaries such as social networks and search engines represent the second relationship (active providers/data controllers). The activities of these actors are usually performed for profit from advertising revenues based on profiling users' data. In order to manage their online space and profile users, platforms rely on automated decision technologies to organise online contents and processing data. Regarding online contents, the increasing involvement of platforms' in the organisations of contents and profiling of users' preferences by using artificial intelligence technologies has transformed the role of online platforms as passive providers. Indeed, whilst the exemption of liability for ISPs was introduced to protect entities by virtue of their passive role, today, the use of automated systems of filtering and processing preferences have led these entities to perform activities whose passive nature is hard to support. As a result, 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 ISPs' liability could not fit in the algorithmic society since such provisions are based on the passive role of online intermediaries.

Furthermore, modern hosting providers do not only perform a more active role with regard to online contents but also with regard to data. Passive hosting providers such as web service application does not process large amount of data, but they limit to offer hosting services for digital services playing the role of data processor. This model also changed with new online platforms which need to decide how to process large amount of data in order to run their business. Even in this case, this business model is based on the implementation of deterministic algorithms or machine learning technologies processing large amounts of information.[36] The benefit of this process consists not only in increasing the possibilities to gather as much as possible information about people and their activities.

The following subsections will address two decisions where online intermediaries have been involved in their double role of hosting providers and data controller in order to show how the two regimes have slowly converged in the algorithmic society.

3.1 A European Case

The case *Google Spain* is a clear example of convergence.[37] In this case, the reference for preliminary ruling was submitted in the course of some proceedings where Google was ordered by the Spanish Data Protection Authority ('AEPD') to remove links to two pages of the online version of a newspaper published in 1998.

It is interesting to look first at the conclusion of the Advocate General Jääskinen observing that 'the internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party web pages. The service provider is not aware of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling,

---

[36] Solon Barocas et al., 'Governing Algorithms: A Provocation Piece' (2013) available online at <https://ssrn.com/abstract=2245322>; Caryn Devins et al., 'The Law and Big Data' (2017) 27 Cornell Journal of Law and Public Policy 357.

[37] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014]. See 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; Frank Pasquale, 'Reforming the Law of Reputation' (2015) 47 Loyola University of Chicago Law Journal 515Aleksandra Kuczerawy and Jef Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 *Columbia Technology Law Journal* 219; Stefan Kulk and Frederik Zuiderveen Borgesius, 'Google Spain v. González: Did the Court Forget About Freedom of Expression?' (2014) 5(3) *European Journal of Risk Regulation* 389.

analysing and indexing, personal data does not manifest itself as such in any particular way'.[38] The Advocate General did not exclude that upon certain conditions even an Internet search engine service provider does exercise a 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. In fact, the owner of a search engine has control over the index and can filter or block certain contents.[39] This is confirmed by the fact that a provider can be requested to apply exclusion codes on source pages in order to prevent the retrieval of specific contents. Even with respect to the cache copy of the content of websites, in case of request of updating the same by the owner, the search engine has actual control of personal data.[40] The assumption behind this finding, in the Advocate General's view, is that the Internet search engine providers bear liability under the same conditions established by the e-Commerce Directive, i.e. when they are actively operating on contents. In light of that, the opinion reached the conclusion that Google could not be considered a data controller.[41]

Focusing on the ECJ's decision, even though the Court has found – following the opinion of the Advocate General – that the indexing of information retrieved from third parties' websites amounts to a processing of personal data, this point has remained the only common finding between the opinion of Mr. Jääskinen and the decision of the Court. As far 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 decision of the Court is focused only on certain nuances – i.e. the right to be forgotten – and does not take into account the consequence on the other system of liability. A very critical point lies with the Court'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. The assumption behind the reasoning of the Court in this respect seems to be that higher protection of data subjects requires taking a broader definition of data controller. Maybe, the Court has not fully realised the scope of such a statement. The ruling of the ECJ brought serious implications on the legal regime of search engines providers. Put another way, the Court seems to indirectly review the provisions enshrined in the e-Commerce Directive. From the safe harbour standpoint, the main question is how it is possible that a search engine like Google is not aware of information by virtue of its role of data controller. Depending on which type of processing of personal data is considered to occur in the case, in fact, the relevant search engine operator may – hypothetically – be obliged to provide a notice to any of the concerned data subjects and obtain the consent of the same. In this case, the Data Protection Directive applies. Indeed, the Court chose to apply the regime of data protection putting aside the e-Commerce Directive regime.

This consideration is also explained by the interest of the ECJ to ensure effective protection of the right to privacy.[42] The finding of the Court in *Google Spain* does not seem to be supported by the actual manner search engines act when indexing third parties webpages, but rather by the crucial implications that said activity produces with regard to the protection of personal data of individuals. The argument advanced by the Advocate General (according to which an ISP does qualify 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

---

38 Conclusion of the Advocate General Jääskinen in the case Google Spain C-131/12, 25 June 2013, para. 84.

39 Ibid, para. 92.

40 Ibid, para. 93.

41 Ibid, para. 100.

42 This ruling should be read together with other decisions in the field of 'digital privacy' where the Court has ensured a high protection of such fundamental rights against potential interferences. See Joined cases C-293/12 and C-594/12 D*igital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014]; Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015]; Case C-203/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016].

website does not indicate so, 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.

The decision, while burdening search engines with the obligation to remove search results when certain conditions are fulfilled, seems to go against the business model of online intermediaries. The fact that engines have control on the contents retrieved from third parties' websites and, particularly, on the personal data therein, seems to be in contrast with the absence of a general monitoring obligation. Despite the high level of protection to fundamental rights, the ECJ has also delegated to search engines the task of balancing fundamental rights when assessing users' request to deindex online content.

3.2 An Italian Case

Moving to the Italian framework, the *Google v Vivi Down* saga provides similar clues. The case raised from a video showing an autistic boy being bullied by his classmates uploaded to the Google video platform. [43] The Court of first instance condemned three executives from Google sentencing them to a six-month suspended conviction for not having prevented the crime of defamation against the minor and the association according to Articles 40 and 595 of the Italian criminal code and for having unlawfully processed personal data according to Article 167 of Legislative Decree 196/2003. The Court of Milan acquitted the defendants from the crime of defamation, excluding that Google, as hosting provider, had an obligation to prevent crimes committed by its users. Indeed, Legislative Decree 70/2003, implementing the e-Commerce Directive in the Italian legal order, excludes the obligation to monitor the content of the materials disseminated by users. Whereas, the Court of first instance condemned the defendants for the crime of unlawful processing of personal data. Therefore, Google should have warned the uploaders about the obligations to respect when uploading online contents as well as the consequences of potential violations.

The Milan Court of Appeals overturned the 2010 first instance ruling by finding the Google executives not guilty for unlawful data processing. At first glance, this decision is based on data protection grounds. However, it is interesting to observe how the Court of Appeal used in its reasoning the general principle that ISPs have no general duty to monitor user-uploaded content on their systems. The Court observed that service providers were wholly extraneous in relation to the information stored when the e-Commerce Directive was introduced. In today's world, the services that online providers offer are not limited to the technical process that simply sets up and provides access to the network. According to the Court, these actors cannot escape the duty to comply with the standard regulations governing liability for data processing due to these characteristics. This observation reflects the gap between the two systems. On the one hand, the matter involves data protection and, as a result, Google could not rely on the safe harbour provided for by the e-Commerce Directive. On the other hand, even more importantly, this observation underlines a critical evolution of the role of ISP moving from their neutral role to a more active role qualifiying them as data controller.

Moving to the Supreme Court decision in 2013,[44] the approach of the Court of Appeals has been clarified in relation to the qualification of the hosting providers as data controller. 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 on its digital rooms. According to the Court, although an illegal processing of personal data occurred, as the video actually contained health data of the minor, this criminal conduct is attributable only to the uploader. The hosting provider was not aware of the

---

[43] Court of Appeals of Milan, decision no. 8611/2012. See Oreste Pollicino and Ernesto Apa, *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective*, (Egea, 2013); Giovanni Sartor & Mario 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.

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

illicit content of the video and, as soon as the authority notified the provider, the content was promptly removed from the online platform.

In this case, the Supreme Court has expressly addressed the topic of the coordination between the regime of the ISP liability and data protection, as implemented in the Italian legal order respectively by Legislative Decree 70/2003 and 196/2003. The Court observed that the exclusion of data protection from the scope of application of the Legislative Decree 70/2003 clarifies that the protection of personal data is governed by rules other than those on ISP liability. The former also applies in the electronic field even after the adoption of the e-Commerce Directive. Therefore, the two regimes should be interpreted together meaning that the ISP liability regime helps to clarify and confirm the scope of the data protection regime.

Indeed, the role of the data controller implies the existence of a decision-making power with regard to the purposes, the methods of processing personal data and the tools used. Put another way, the data controller is the only subject who can determine its aims, methods and means. In the view of the Supreme Court, this role is compatible with the system of the e-Commerce Directive. More specifically, the Supreme 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.

4. GDPR and e-Commerce Directive: Overlapping Layers?

In light of these considerations, the two regimes have already demonstrated to converge in the algorithmic society. Although the relationship data processor/passive provider continues to exist in the digital environment such as in the case of web hosting, the second model (data controller/active provider) has questioned the separation of the two regimes underlining the point of contacts.

The GDPR has codified this scenario by opening new perspectives in the application of the safe harbour rule even in the field of data protection. Indeed, as already stressed, the GDPR has clarified that the application of the new Regulation should not affect the rules provided for by the e-Commerce Directive, in particular those regarding ISP's liability.[45]

However, it is necessary to underline that the provision limiting the scope of the e-Commerce Directive is still in force. As a result, at this moment, there is a potential clash between the two legislative instruments, and it is not possible to know how the ECJ will deal with the relationship between Article 2(4) GDPR and Article 1(5)(b) of the e-Commerce Directive.

In the past, scholars addressed this question supporting the abolition of the 'data protection exceptionalism'.[46] In particular this outcome could be achieved through a restrictive interpretation of Article 1(5) by limiting its scope only to 'questions relating to information society services covered by Directives 95/46/EC' without covering the issue of user-generated data. Indeed, the e-Commerce Directive 'defers 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)'.[47]

This perspective is confirmed by the potential application of the safe harbour regime only to third-party content. The extension of this regime should not be considered as an exemption of liability from

---

[45] 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.

[46] Giovanni Sartor, '"Providers" liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?' (2013) 3(1) International Data Privacy Law 3.

[47] Ibid., 5.

unlawful processing of personal data performed directly by the online intermediary. Whereas, in relation to content provided for by users violating data protection rules, in this case, online intermediaries could rely on the liability regime established by the e-Commerce Directive.

Secondly, other limitations to the application of the e-Commerce Directive can also be found from the GDPR itself such as the exclusion of the application of the data protection rules for 'purely personal or household activity'.[48] However, in this last case, it is necessary to mention Recital 18 which excludes these activities from the scope of the Regulation except for the case in which the data controllers or processors provide the means for processing personal data for such personal or household activities.[49] As a result, according to this interpretative provision, even in this case, online intermediaries could be subject to the application of GDPR.

Thirdly, the lack of any reference to the e-Commerce Directive when the GDPR addresses the liability of data controller and processor does not help to clarify the relationship between the two regimes. Regarding the liability of the data controller, Article 82(3) GDPR provides that a controller or processor shall be exempt from liability if it proves that it is 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 function as data controller or processor should not be considered liable for third-party conducts. It is necessary to observe that, unlike the Data Protection Directive, the GDPR does not provide a Recital providing two examples of how a controller might prove the lack of any liability: *force majeure* or error on the part of the data subject.[50] Although it could be reasonable thinking that 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.

Fourthly, a systematic interpretation could lead to support an extension of ISP liability also in relation to third-party contents infringing data protection rights. It is possible to observe that the extension of the scope of the e-Commerce Directive would increase uniformity in online content management.[51] If online intermediaries would be able to rely on the safe harbour against illicit data processing perpetrated by third-party, their process of content management could benefit from a general extension also to these online contents with the result that this approach would foster the freedom to conduct business of online intermediaries. However, it is necessary to stress that since the e-Commerce Directive allows Member States to impose injunction and filtering systems to online intermediaries at certain conditions, it would be possible to understand how the positive effects of such a system would be mitigated by the possibility to proactively monitor also personal data when they are disseminated through their platform in order to tackle third-party violations. Since the algorithmic society has led online intermediaries to play a more active role processing data and performing online content management activities, this safe harbour extension could risk encouraging platforms to increase their monitoring activities with potential chilling effects for freedom of expression.

As a result, it would be possible to wonder how *Google Spain* and *Google Vivi Down* would have been adjudicated if the GDPR was in force at that time? Lacking any interpretation of the relationship between the e-Commerce Directive and the GDPR, it is not possible to foresee how the ECJ and the Italian courts would have interpreted the two cases. According to this system, even where the ECJ would

---

48 GDPR, Article 2(2)(c).

49 Ibid., Recital 18.

50 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'.

51 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.

recognise online intermediaries as data controller, it could decide which regime applies by putting aside one of them. One of the main consequences of this approach is to blur the boundaries between the two regimes and, more specifically, between the notion of 'data controller' and 'active provider' affecting the application of the rules in the field of data processing and ISP's liability.

5. Conclusion

At this time, the only certain starting point is that the GDPR has repealed the previous system established by the Data Protection Directive. Whereas, concerning the two regimes analysed in this work, it can be observed that their parallel tracks have already started to overlap before the adoption of the GDPR although both systems were conceived from two different perspectives. Nevertheless, it is possible to foresee that the evolution of artificial intelligence technologies will increasingly lead the two systems to collide where data controllers and hosting providers decide how to use and organise data and online contents.

The cases analysed in this work have shown how the two systems have started to 'talk' each other. From the first dialogue in *Promusicae*, such a relationship has become more complex with the advent of new intermediaries. This convergence has been mostly the result of the rise of new online intermediaries whose business was based on data-driven models. In *Google Spain* and *Google Vivi Down*, the interpretation of the ECJ and the Italian Courts has highlighted the complexities in applying a rigid separation between the two systems. Both layers have started to overlap when focusing on online intermediaries such as search engines and social networks which do not perform the activity of data processor or passive provider any longer. Indeed, considering modern ISPs active providers is strongly linked to their role in establishing how data is processed. Such a mix of active provider and data controller implies that the rigid distinction in the application of the two regimes is no longer generally justified by the passive role of online intermediaries. In other words, if it is no coincidence whether the e-Commerce Directive has excluded the privacy and data protection matters from its scope of application in 2000, today, the same political choice would appear unreasonable when it is applied to some intermediaries such as social networks and search engines.

In light of these considerations, the adoption of the GDPR will likely contribute to the beginning of a new season for online intermediaries by potentially extending their liability even for third-party content violating data protection rules. However, whereas the European Commission adopted a new legal instrument in the field of privacy and data protection, the same path has not been followed for ISP liability. In the framework of the Digital Single Market strategy, the Commission has decided not to amend the e-Commerce Directive with the result that the system of liability of online intermediaries will maintain its old-style structure. As a result, lacking any amendment in the field of ISP liability, the scope of application of the GDPR could be another milestone in the process of convergence between the two regimes.

Author contacts:

Giovanni De Gregorio
Università Milano-Bicocca
Email: g.degregorio@campus.unimib.it