COMMON MARKET LAW REVIEW

CONTENTS Vol. 59 No. 2 April 2022

Aims
The Common Market Law Review is designed to function as a medium for the understanding and implementation of European Union Law within the Member States and elsewhere, and for the dissemination of legal thinking on European Union Law matters. It thus aims to meet the needs of both the academic and the practitioner. For practical reasons, English is used as the language of communication.

Common Market Law Review is published bimonthly.
This journal is also available online. Online and individual subscription prices are available upon request. Please contact our sales department for further information at +31(0)172 641562 or at lnternational-sales@wolterskluwer.com.
Periodicals postage paid at Rahway, N.J. USPS no. 663–170.
U.S. Mailing Agent: Mercury Airfreight International Ltd., 365 Blair Road, Avenel, NJ 07001.
Published by Kluwer Law International B.V., P.O. Box 316, 2400 AH Alphen aan den Rijn, The Netherlands

---

Printed on acid-free paper.

COMMON MARKET LAW REVIEW

Managing Editor: Alison McDonnell
Common Market Law Review
Europa Instituut
Steenschuur 25
2311 ES Leiden
The Netherlands
e-mail: a.m.mcdonnell@law.leidenuniv.nl
tel. + 31 71 5277549
fax: + 31 71 5277600

Establishment and Aims

The Common Market Law Review was established in 1963 in cooperation with the British Institute of International and Comparative Law and the Europa Instituut of the University of Leyden.The Common Market Law Review is designed to function as a medium for the understanding and analysis of European Union Law, and for the dissemination of legal thinking on all matters of European Union Law. It aims to meet the needs of both the academic and the practitioner. For practical reasons, English is used as the language of communication.

Editorial policy

The editors will consider for publication manuscripts by contributors from any country. Articles will be subjected to a review procedure. The author should ensure that the significance of the contribution will be apparent also to readers outside the specific expertise. Special terms and abbreviations should be clearly defined in the text or notes. Accepted manuscripts will be edited, if necessary, to improve the general effectiveness of communication. If editing should be extensive, with a consequent danger of altering the meaning, the manuscript will be returned to the author for approval before type is set.

Submission of manuscripts

Manuscripts should be submitted together with a covering letter to the Managing Editor. They must be accompanied by written assurance that the article has not been published, submitted or accepted elsewhere. The author will be notified of acceptance, rejection or need for revision within three to nine weeks. Digital submissions are welcomed. Articles should preferably be no longer than 28 pages (approx. 9,000 words). Annotations should be no longer than 10 pages (approx. 3,000 words). Details concerning submission and the review process can be found on the journal's website http://www.kluwerlawonline.com/toc.php?pubcode=COLA

Common Market Law Review **59**: 473–500, 2022.

THE EUROPEAN RISK-BASED APPROACHES: CONNECTING CONSTITUTIONAL DOTS IN THE DIGITAL AGE

GIOVANNI DE GREGORIO AND PIETRO DUNN*

Abstract

In recent years, risk has become a proxy and a parameter characterizing EU regulation of digital technologies. Nonetheless, EU risk-based regulation in the digital age is multi-faceted in the approaches it takes. This article considers three examples: the General Data Protection Regulation; the proposal for the Digital Services Act; and the proposal for the Artificial Intelligence Act. These three instruments move across a spectrum, from a bottom-up approach (the GDPR) to a top-down architecture (the AI Act), going through an intermediate stage (the DSA). It is argued, however, that despite the different methods, the three instruments share a common objective and project: they all seek to guarantee an optimal balance between innovation and the protection of rights, in line with the developing features of European (digital) constitutionalism. Through this lens, it is thus possible to grasp the "fil rouge" behind the GDPR, the DSA and the AI Act as they express a common constitutional aspiration and direction.

1. Introduction

Technologies have always provided opportunities, while raising challenges requiring regulators to find a balance between fostering innovation and mitigating risks. Throughout history, technologies have been used to achieve and serve various purposes, providing, on the one hand, new phases for societal growth and questioning, on the other hand, the *status quo*.

Digital technologies are no exception. The Union thus faces new regulatory challenges in the algorithmic society, where large multinational social platforms sit between traditional nation States and ordinary individuals, and

* Postdoctoral researcher, Centre for Socio-Legal Studies, University of Oxford, giovanni.degregorio@csls.ox.ac.uk and PhD student, University of Bologna – University of Luxembourg, pietro.dunn2@unibo.it, respectively. This article was awarded the Common Market Law Review 2021 Prize for Young Academics.

where algorithms and AI agents are employed by public and private actors.[1] Although digitized systems and environments have brought with them great societal advantages, they have also given rise to unprecedented communication systems and networks which amplify risk.[2] COVID-19 has greatly accelerated this process, by making the digital environment more necessary than ever.[3] Moreover, 21st century technologies have also reset the terms of a range of individual fundamental rights and liberties (e.g. privacy and data protection, freedom of expression, non-discrimination, etc.), *vis-à-vis* both public institutions and private actors.[4]

In this context, the term "risk" has been defined in many ways.[5] A vernacular interpretation identifies it with a danger which may or may not take place, and which can only be foreseen to a certain extent. More technically, however, risk is a combination of the probability of a defined hazard occurring and the magnitude of the consequences that hazard may entail.[6] Risk can thus serve as a proxy for decision-making, based on the forecasting of future positive and negative events.[7] This assessment is mainly done through the practices of risk analysis (or risk management), that is, through a set of methodologies, templates, and processes meant to help make rational decisions based on potential future opportunities or threats.[8] In other words,

1. Balkin, "Free speech in the algorithmic society: Big data, private governance, and new school speech regulation", 51 *UC Davis Law Review* (2018), 1149–1210.

2. Lupton, "Digital risk society" in Burgess, Alemanno and Zinn (Eds.), *Routledge Handbook of Risk Studies* (Routledge, 2016), pp. 301–309. With respect to the specific challenges posed by digital technologies to competition law, see Sørensen, "Digitalisation: An opportunity or a risk?", 9 JECLAP (2018), 349–350.

3. Buil-Gil et al., "Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK", 23 *European Societies* (2020), S47–S59.

4. Van Dijck, "Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology", 12 *Surveillance & Society* (2014), 197–208; Zuboff, *The Age of Surveillance Capitalism. The Fight for a Future at the New Frontier of Power* (PublicAffairs, 2019); Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press, 2019); Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press, 2018); De Gregorio, "From constitutional freedoms to the power of the platforms: Protecting fundamental rights online in the algorithmic society", 11 *European Journal of Legal Studies* (2019), 65–103; Pollicino, *Judicial Protection of Fundamental Rights on the Internet* (Hart, 2021).

5. Gellert, "Understanding the notion of risk in the General Data Protection Regulation", 34 *Computer Law & Security Review* (2018), 279–288, at 280.

6. Gellert, *The Risk-Based Approach to Data Protection* (OUP, 2020), p. 27.

7. Ibid., at p. 28. On this point, see also Bernstein, *Against the Gods. The Remarkable Story of Risk* (John Wiley & Sons, 1996).

8. Risk analysis encompasses two steps: the first one is risk assessment, i.e. the measurement of risk itself, which represents the scientific and quantitative component; the second one, i.e. risk management (*stricto sensu*), is the policy component and consists of the decisional phase. On this point, see Gellert, op. cit. *supra* note 5, at 280; Hutter, "Risk, regulation, and management" in Taylor-Gooby and Zinn (Eds.), *Risk in Social Science* (OUP,

assessing risk leads to a degree of certainty based on probabilistic logics. Coherently, risk regulation can be perceived as an attempt to face the rise of what has been defined as the "risk society",[9] through a rational and technocratic approach that fosters more efficient, objective, and fair governance,[10] whilst fighting against "over-regulation, legalistic and prescriptive rules, and the high costs of regulation".[11] In fact, risk may be employed differently as a parameter to structure regulation depending on the ultimate goal of the regulator, which could be that of eliminating all risks, of simply reducing them to an acceptable level, of reducing them until costs become unbearable or, finally, of striking a proportionate balance between risks and costs of regulation.[12] As will be argued in the following sections, the latter perspective is the one characterizing precisely the development of the EU's risk-based policies in the digital age.

Within this framework, "risk regulation" is a broad term, often conflated with "risk-based regulation". In this respect, Quelle suggests a categorization based on the actual role played by risk.[13] "Risk regulation", *stricto sensu*, would thus identify more precisely those cases where risk is ultimately the object of regulation itself, and thus functions as the rationale behind governmental intervention. In this sense, "risk regulation" would be identifiable as a "governmental interference with market or social processes to control potential adverse consequences".[14] Conversely, "risk-based regulation" uses risk as a tool to prioritize and target enforcement action in a manner that is proportionate to an actual hazard: in other words, it tends to "calibrate" the enforcement of the law based on concrete risk scores.[15] In this

2006), pp. 202–227. As highlighted by Alemanno, "Regulating the European risk society" in Alemanno et al. (Eds.), *Better Business Regulation in a Risk Society* (Springer, 2013), pp. 37–56, at p. 53, EU law also recognizes risk communication as a third component, which essentially entails "providing information on levels of health, safety, and environmental risks, their significance, and their management".

9. Beck, *Risk Society. Towards a New Modernity* (Ritter tr., Sage Publications, 1992).

10. Hutter, "A risk regulation perspective on regulatory excellence" in Coglianese (Ed.), *Achieving Regulatory Excellence* (Brookings Institution Press, 2017), pp. 101–114.

11. Macenaite, "The 'riskification' of European data protection law through a two-fold shift", 8 EJRR (2017), 506–540, at 509. See also Black, "The emergence of risk-based regulation and the new public risk management in the United Kingdom", (2005) *Public Law*, 510–546, at 512.

12. Coglianese, "The law and economics of risk regulation", *University of Pennsylvania, Institute for Law & Economics Research Paper No. 20-18*, (2020) at p. 9.

13. Quelle, "Enhancing compliance under the General Data Protection Regulation: The risky upshot of the accountability and risk-based approach", 9 EJRR (2018), 502–526, at 509.

14. Hood, Rothstein and Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (OUP, 2001), at p. 3.

15. Quelle, op. cit. *supra* note 13.

context, laws might merge together these two aspects, by governing risk through a risk-based approach.

Different approaches to risk regulation have already been developed in Europe.[16] Indeed, in recent decades, risk as an approach to public governance and regulation has, in general, gathered increasing momentum across all Western countries.[17] In the UK, as highlighted by Black, risk management had already become a key feature in developing regulation during the first decade of the 21st century.[18] The same process has recently affected EU law as well.[19] According to Macenaite,[20] risk regulation initially developed as a response to the risks to the environment and to human health and safety stemming from new technologies or industries. Subsequently, its scope of action grew and came to encompass a wider range of fields.[21]

Since the launch of the Digital Single Market Strategy,[22] the Union has increasingly relied on a risk-based approach. Rather than just setting new rights and safeguards, the Union has tried to regulate risks by increasing the accountability of both public and private actors with respect to the risks and potential collateral effects resulting from their activities. The emergence of the risk-based approach within the EU's digital policies is particularly evident when considering the recent legislative developments concerning the fields of data, online content, and artificial intelligence. Nonetheless, the way such an approach has been articulated varies significantly.

The General Data Protection Regulation (GDPR) follows a bottom-up perspective, in the sense that the evaluation of risk and the choice of mitigating measures are not defined by the law, but are primarily left to the discretion of the targets of regulation themselves, i.e. to data controllers and processors. In this sense, as will be further highlighted below, the principle of accountability is the result of a legislative strategy aiming to greatly reduce the imposition of duties coming from "above".[23] Quite the opposite, the proposed Artificial

16. Macenaite, op. cit. *supra* note 11.

17. Van der Heijden, "Risk as an approach to regulatory governance: An evidence synthesis and research agenda", 11 *Sage Open* (2021), available at <doi.org/10.1177%2F2158244021103202>, (all websites last visited 24 Jan. 2022).

18. Black, op. cit. *supra* note 11.

19. See, among others, Vieweg, "Risk and the regulatory State – various aspects regarding safety and security in the fields of technology and health" in Micklitz and Tridimas (Eds.), *Risk and EU Law* (Edward Elgar, 2015), pp. 19–32.

20. Macenaite, op. cit. *supra* note 11, 508–509.

21. Cf. Alemanno, op. cit. *supra* note 8.

22. COM(2015)192 final, "A Digital Single Market Strategy for Europe".

23. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1.

Intelligence Act (AI Act) takes a very different point of view, in that, although it provides for very different degrees of responsibility and imposes differentiated duties depending on the risk scores of regulated AI systems, it does not leave the task of evaluating such risk scores to the targets of regulation: in fact, it is the AI Act itself that, on a top-down basis, identifies directly the various categories of risk.[24] Finally, in the field of online content, the Digital Services Act (DSA) aims at creating a hybrid system, which mixes the two opposite perspectives of the GDPR and the AI Act by identifying on a top-down basis four risk categories for providers of intermediary services, while leaving them ample leeway to choose which measures to employ to reduce the negative externalities their activities entail. In particular, as will be highlighted in the following sections, the DSA suggests that "very large online platforms" make frequent impact assessments of the systemic risks their services entail, and act accordingly to mitigate them.[25]

This framework suggests that the EU's digital policy is increasingly turning to risk-based regulation strategies. However, the way this regulatory technique is elaborated in practice is far from unitary. While the GDPR features a bottom-up risk-based approach, the AI Act adopts a top-down architecture, and the DSA presents features pertaining to both a top-down and a bottom-up perspective. Such diversified legislative styles may cause a regulatory fragmentation which could deeply affect not only the goals of the internal market but also EU constitutional principles, primarily the rule of law.

Nonetheless, we maintain that a *fil rouge*, though variously elaborated, can be identified as a unifying connector of those three approaches. Such a unifying feature is represented by the common European constitutional values guiding the GDPR, the AI Act, and the DSA. Although they represent very different expressions of the EU's risk-based approach, they share the same constitutional goal, that is the fostering of fundamental rights and democratic values as counter-limits to the predominance of pure market logics in the algorithmic society. In particular, they share a constitutional-driven soul, in that they are all characterized by the goal of balancing appropriately the need to foster fundamental rights and freedoms in the digital environment while, at the same time, protecting economic freedoms, as engines of innovation, which are key to the Digital Single Market. In this sense, from a constitutional standpoint, the three instruments are unified in their aspiration to foster a model of "optimizing constitutionalism" – that is a "mature" approach to risk

24. COM(2021)206 final, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

25. COM(2020)825 final, Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA). See, in particular, Arts. 26–27.

regulation which, rather than simply aiming at minimizing risks at all costs by imposing "maximum" precautions ("precautionary constitutionalism"), seeks to design "optimal" precautions that do not excessively constrain the various actors playing in the market.[26]

Moreover, the suggested characterization of these three different instruments is a direct reflection of the transformation of the EU's approach itself which, in the last twenty years, has shifted from an eminently liberal market-based perspective to a constitutional-driven strategy.[27] Whereas digital policies were initially driven by the purpose of fostering the development of digital services in the internal market, the developing popularity of the concept of risk follows the increasing role of constitutionalism within the European project. We thus argue that the EU's risk-based approach and the rights-based approach have not only come to coexist in the Union's digital policy but have, to a greater extent, become intimately connected.[28]

In this context, Section 2 of this article focuses on analysing the bottom-up risk-based approach of the GDPR. Section 3 analyses the Union's approach to risk related to content moderation, looking at the hybrid model of the DSA. Section 4 highlights the top-down architecture of the AI Act. Section 5 aims to catch the differences and similarities between these sources, underlining how, notwithstanding their profound technical divergence, they are generally moved by a common constitutional spirit, driven by the normative phase of European digital constitutionalism which aims to ensure the protection of fundamental rights and democratic values in the algorithmic society.

2. The General Data Protection Regulation: The bottom-up approach

The first instrument analysed in this article from a risk-based perspective is the GDPR. The GDPR has been a landmark step in the path of the EU's data protection law which, since 1995, had been governed by the Data Protection Directive.[29] In the Explanatory Memorandum to the initial proposal for the GDPR, the Commission stressed how EU law had to be brought up to date to fit the new societal context, where technology has come to allow both private actors and public administrations "to make use of personal data on an

26. See Vermeule, *The Constitution of Risk* (Cambridge University Press, 2014), p. 77.

27. De Gregorio, "The rise of digital constitutionalism in the European Union", 19 *International Journal of Constitutional Law* (2021), 41–70.

28. Cf. Gellert, op. cit. *supra* note 6.

29. Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 1995, L 281/31.

unprecedented scale in order to pursue their activities".[30] The changing strategy of the Union can be examined by comparing the first recitals of the Data Protection Directive with those of the GDPR, which underlines the shift of focus from the central role of data circulation within the internal market to the protection of individual fundamental rights.[31]

It should not come as a surprise if this transition from a market-driven to a constitutional-oriented perspective was translated into law through the adoption of a risk-based approach that, as has already been stressed and will be further shown in the following sections, ultimately represents an attempt to strike an "optimal" balance among conflicting constitutional interests. The principle of accountability,[32] pursuant to which data controllers must be able to prove they comply with the general principles set by the GDPR,[33] is itself strictly intertwined with the rationale of this approach.

There is not one single way to comply with the requirements of the GDPR. In fact, data controllers are entrusted with the responsibility of ensuring that the processing of personal data is aligned with the protection of the general principles it sets. This form of delegation characterizes the bottom-up structure of the GDPR. Although remaining within the context of Union rules, the way such rules and principles are elaborated in practice is mainly up to the targets of regulation. Data controllers are thus required to evaluate which risks their processing activities entail, and actively to shape the measures and techniques necessary to guarantee individual data protection and privacy rights in accordance with such specific risks.

The meaning of the principle of accountability can thus be better understood by focusing on the dynamic definition of data controllers' responsibility, which is based on the nature, scope, context, and purposes of processing, as well as on the risks of varying likelihood and/or severity for the rights and freedoms of natural persons.[34] Therefore, the data controller is required to ascertain concretely the degree of risks to data subjects' fundamental rights when processing personal data, and, based on that assessment, design the appropriate mitigation responses. If a data controller is

30. COM(2012)11 final, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

31. GDPR, cited *supra* note 23, Recitals 1–2.

32. Ibid., Art. 5(2).

33. Thus Castets-Renard, "Accountability of algorithms in the GDPR and beyond: A European legal framework on automated decision-making", 30 *Fordham Intellectual Property, Media & Entertainment Law Journal* (2019), 91–137, at 107: "Accountability starts with an agent and the outcome of its actions; the data holder (controller or processor) is accountable for ensuring compliance with the principles (and rights of the data subject). The data holder is also supposed to have a mechanism in place to ensure compliance".

34. GDPR, cited *supra* note 23, Art. 24.

not able to prove that they have put in place measures sufficient for complying with the general principles of the Regulation, then they will be held liable for damages. The GDPR thus relies directly on the targets of regulation as far as the definition of risk scores is concerned: the law does not establish any risk thresholds itself, but leaves such a sensitive duty to those private and public actors who are in charge of processing individual personal data. In this sense, the risk-based approach of the GDPR may be defined as bottom-up, as opposed to the DSA and, even further, to the AI Act, as will be explained in the next sections.

The duty to evaluate the perils connected to any processing of personal data, and consequently to introduce remedies and safeguards, emerges not only from the rules governing data controllers' responsibilities, but also from the principle of privacy by design and by default.[35] Both provisions require precisely that data controllers "implement appropriate technical and organisational measures" to ensure full compliance with the GDPR, based on the riskiness of their processing activities. As noted by Quelle, such a legal regime requires data controllers and data processors to engage in a form of "compliance 2.0", i.e. "a form of compliance that does not merely 'tick boxes', but is tailored to respect the rights and freedoms of data subjects".[36] Therefore, not all data controllers are required to implement the same risk mitigation systems in order to be compliant with the GDPR.

In fact, this diversity raised concerns during the GDPR adoption process. As highlighted by Gellert,[37] leaving data controllers to define the margin of data protection safeguards could foster the interests of corporations rather than the interests of citizens. The new system implemented by the GDPR would contradict the foundations of the EU data protection regime, which, as underscored by Lynskey, was traditionally "rights-based".[38] Instead, the GDPR's risk-based foundation departs from a different *modus operandi*. Whereas the former follows a binary logic, whereby processing is either legal or illegal, the latter follows the "granular, scalable, logic of risk analysis" and is thus concerned with "how much risk one can take" rather than with "whether the processing is too risky or not".[39] In this sense, the rights-based approach and the risk-based approach can be ascribed respectively to the

35. Ibid., Art. 25(1).

36. Quelle, op. cit. *supra* note 13, at 506.

37. Gellert, op. cit. *supra* note 6, at p. 2 et seq.

38. Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015). According to the author, at pp. 35–36, a data protection regime can be considered as being rights-based if, on the one hand, it is "rights-conferring" (i.e. it grants rights to individuals) and, on the other hand, "if it 'gives expression to' a fundamental right or if its design and interpretation are consistent with its underlying conception as a fundamental right".

39. Gellert, op. cit. *supra* note 6, at p. 2.

"command-and-control" model, which refers "to the command of the law and the legal authority of the State",[40] and to the class of "meta-regulations", a sub-category of principle-based regulations[41] where the purpose becomes that of "encouraging the industry to put in place its own systems of management which are then scrutinized by regulators".[42]

It follows from the above that, whereas the resort to a command-and-control system in the field of data protection implies that rules apply indiscriminately to any controller and data processing, the scalable element of a risk-based approach leads to a multiform protection of data which is inherently diverse depending on the actual target of regulation. Obligations may, therefore, be objectively "uneven", reflecting the interests of the actors called to comply with the GDPR, but this different outcome is justified in that it is the consequence of a specific balancing test operated directly by data controllers based on the principle of accountability.

This last aspect, which is precisely what characterizes the GDPR as a bottom-up risk-based regulation, where the balancing between interests is made directly by the targets of regulation rather than by the law, emerges from a range of different provisions. The GDPR, for instance, introduces the requirement that controllers carry out a data protection impact assessment (DPIA) whenever a specific type of processing is likely to result in a "high" risk to the rights and freedoms of natural persons.[43] In this case, data controllers are called to define when a processing is high risk in order to decide whether or not a DPIA is required in a certain context. Such an obligation represents a typical point of contact between the managerial practices of risk management and regulation, so much so that Alemanno defines risk assessment as a "*Grundnorm*", i.e. as "the privileged methodological tool for regulating risk in Europe".[44] Impact assessment is a "process for simultaneously documenting an undertaking, evaluating the

40. Hutter, op. cit. *supra* note 8, at p. 203. According to Gellert, op. cit. *supra* note 6, at p. 46, "Command and control regulation can best be described as mirroring an 'Austinian' understanding of the law, that is, a set of standards and behaviour issued by the Sovereign, and associated to sanctions in case of non-respect".

41. Gellert, op. cit. *supra* note 6, at p. 20.

42. Gunningham, "Enforcement and Compliance Strategies" in Baldwin, Cave and Lodge (Eds.), *The Oxford Handbook of Regulation* (OUP, 2010), at p. 113.

43. GDPR, cited *supra* note 23, Art. 35(1). Para 3 of the same provision expressly states that a DPIA is always required "in the case of (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale".

44. Alemanno, op. cit. *supra* note 8, at p. 41.

impacts it might cause, and assigning responsibility for those impacts",[45] and its main purpose is indeed to offer guidance to data controllers as to which organizational tools they should adopt in light of its conclusions.

The GDPR thus delegates data controllers the fundamental role of identifying on their own the proper means to comply with legal requirements. Such a "power", however, comes with a price, since it implies that data controllers become truly responsible for any negative impact on the fundamental rights and liberties of data subjects. Through such a model, the targets of the GDPR are granted a broader discretion than would be possible under a binary command-and-control approach, but precisely for this reason they are made accountable for their increased autonomy and their choices. It is no wonder, therefore, that the principle of accountability represents one of the most important and well-known core features characterizing the entire system of EU data protection law.

The risk-based approach of the GDPR is, in other words, inherently grounded upon the "responsibilization of the regulatee".[46] The traditional top-down legislative dialectic shifts towards a more collaborative architecture, where the governed must implement the appropriate risk management strategies to avoid liability.[47] The key word becomes, in this sense, "proportionality", which functions both as a principle and as a guiding standard.[48] Proportionality, on the one hand, guarantees that businesses and organizations are not compelled to adopt excessively costly measures but, on the other hand, obliges them to keenly evaluate and balance all existing risk factors in order to respond to them in a satisfactory way. In other words, the purpose is to find an optimal balance.

The way the EU legislature has elaborated the GDPR's risk-based approach seemingly reflects and is consistent with the general trend, more and more common within EU law and case law, by which the pursuit of desirable outcomes for society is sought also through the horizontal involvement of the targets of regulation and the delegation to them of balancing powers and tasks traditionally vested in public institutions.[49] As will emerge from the following

45. Moss et al., *Assembling Accountability. Algorithmic Impact Assessment for the Public Interest* (Data & Society, 2021), at p. 10. In their work, the authors identify and describe ten constitutive components that must be taken into account when establishing accountability under any impact assessment regime: (a) sources of legitimacy; (b) actors and forum; (c) catalysing event; (d) time frame; (e) public access; (f) public consultation; (g) method; (h) assessors; (i) impacts; (j) harms and redress.

46. Gellert, op. cit. *supra* note 6, at p. 20.

47. Ibid., at p. 23.

48. Ibid.

49. See, among others, Pollicino, op. cit. *supra* note 4; De Gregorio, op. cit. *supra* note 4; Bassini, "Fundamental rights and private enforcement in the digital age", 25 ELJ (2019), 182–197; Durante, *Computational Power. The Impact of ICT on Law, Society and Knowledge*

section, this tendency to rely on private actors for the enforcement of publicly-relevant interests also characterizes the Digital Services Act proposal which aims to regulate online content by imposing on Internet intermediaries due diligence duties to moderate illicit and harmful materials in the online environment. This is mainly done, again, through a risk-based approach which translates into a delegation of public power into the hands of private actors. However, the way such an approach is elaborated differs partly from the technique employed by the GDPR.

3. The Digital Services Act: Mixing the bottom-up and top-down approaches

The second instrument analysed in this work is the DSA which is characterized by what the European Commission itself defined as a "supervised risk management approach, with an important role of the governance system for enforcement".[50] In December 2020, the European Commission presented a package of two draft regulation proposals commonly referred to as the DSA and the Digital Markets Act (DMA),[51] aimed at fostering the twofold goal of creating "a safer digital space in which the fundamental rights of all users of digital services are protected" and establishing "a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally".[52] The DSA explicitly foresees a general and horizontal, rather than sectoral, reform of intermediary liability for third-party content. In the opening of its Explanatory Memorandum to the DSA, the Commission expressly stated that, since the adoption of the e-Commerce Directive,[53] new digital services have

(Routledge, 2021). Moving across the Atlantic, cf. Balkin, "Free speech is a triangle", 118 *Columbia Law Review* (2018), 2011–2056, highlights how contemporary speech regulation generally relies on delegating to private digital actors the evaluation of the illegal or harmful nature of a specific online content. Cf. Klonick, "The new governors: The people, rules and processes governing online speech", 131 *Harvard Law Review* (2018), 1598–1670.

50. DSA, cited *supra* note 25, Explanatory Memorandum, at 1. On the role of risk within the DSA, see also Efroni, "The Digital Services Act: Risk-based regulation of online platforms", *Internet Policy Review* (2021), available at <policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606>.

51. COM(2020)842 final, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

52. European Commission, "The Digital Services Act Package", 31 Aug. 2021, available at <digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. See, on this topic, Eifert et al., "Taming the giants: The DMA/DSA package", 58 CML Rev. (2021), 987–1028.

53. 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 (E-commerce Directive), O.J. 2000, L 178/1.

emerged, revolutionizing our daily lives and our economy but, at the same time, giving rise to new risks and challenges, both for society as a whole and individuals using such services.[54]

Like the GDPR, the DSA also adopts a risk-based approach, in the sense that the targets of regulation, in this case the providers of intermediary (digital) services, are subject to duties and obligations which are proportional and calibrated to the concrete risks potentially resulting from the provision of their services. However, in this case, the European Commission distanced itself from the pure bottom-up structure adopted by the GDPR. Indeed, the DSA sets of its own accord the various categories into which online intermediaries should be divided, based on risk thresholds established from above. In other words, in the case of the DSA, a (preliminary) risk assessment is made directly from the top. Nonetheless, depending on the category they are assigned to, providers have varying degrees of discretion as to how to actively manage the risks arising from their own services. Depending on how they have been classified, they maintain a certain leeway as to the definition of their risk-mitigation strategies. We argue, therefore, that the model envisaged within the DSA is neither purely bottom-up nor purely top-down: rather, it represents a "third way" in between the two.

At first glance, the DSA does not really engage in a revolutionary transformation of the current regime.[55] The new provisions[56] simply transpose into the DSA[57] the e-Commerce Directive's "safe harbour" approach,[58] which is still kept as a background general rule.[59] It does, however, confirm that strand of Court of Justice case law inaugurated with *Google France*[60] and *L'Oréal*,[61] by explicitly stating that such a system is justified only in as much as providers act neutrally "by a merely technical and automatic processing of the information provided by the recipient of the service".[62] Moreover, to

54. DSA, cited *supra* note 25, Explanatory Memorandum, at 1.

55. See Cauffman and Goanta, "A new order: The Digital Services Act and consumer protection", (2021) EJRR, available at <doi.org/10.1017/err.2021.8>, at 6 et seq.

56. DSA, cited *supra* note 25, Arts. 3–5, 7.

57. Edwards, "Articles 12–15 ECD: ISP liability. The problem of intermediary service provider liability" in Edwards (Ed.), *The New Legal Framework for E-Commerce in Europe* (Hart Publishing, 2005), pp. 93–136; Yannopoulos, "The immunity of internet intermediaries reconsidered?" in Taddeo and Floridi (Eds.), *The Responsibilities of Online Service Providers* (Springer, 2017), pp. 43–60.

58. E-Commerce Directive, cited *supra* note 53, Arts. 12–15.

59. The "safe harbour" doctrine was strongly inspired by Section 230 of the US Communication Decency Act 1996. On the topic, see among others Citron and Wittes, "The Internet will not break: Denying Bad Samaritans Sec. 230 immunity", 86 *Fordham Law Review* (2017), 401–424.

60. Case C–236/08, *Google France*, EU:C:2010:159.

61. Case C-324/09, *L'Oréal*, EU:C:2011:474.

62. DSA, cited *supra* note 25, Recital 18.

address the challenges raised by online platforms, the DSA complements the system of exemption of liability by introducing an ample array of new due diligence obligations "for a transparent and safe online environment". These safeguards represent the true expression of the risk-based approach adopted in the DSA at the intersection of the bottom-up and top-down approaches of the GDPR and AI Act.

These new obligations do not apply indiscriminately to all providers, but are scaled based on the services they offer and on their dimensions. A small group of provisions thus applies to all providers of intermediary services,[63] whereas the scope of application of the subsequent Articles becomes progressively narrower, covering in turn: hosting providers;[64] online platforms;[65] and "very large online platforms" (VLOPs).[66] As clarified by the proposal, online platforms represent a subset of the class of hosting providers which are characterized by the fact that they do not only store information provided by the recipients of their services but, on request, they disseminate such information to the public.[67] An online platform, moreover, ought to be considered a VLOP when it provides its services to a number of average monthly recipients in the EU that is equal or higher than 45 million.[68]

The new due diligence obligations move in two main directions. On the one hand, the DSA introduces transparency duties,[69] which are particularly strict and detailed for online platforms[70] and VLOPs.[71] These include the need to publish transparency reports regularly and the duty of online platforms,[72] and VLOPs,[73] to give users information about advertising practices.[74] On the other hand, the DSA requires an active involvement in the fight against illegal content and illegal activities on the Internet, on penalty of a fine.[75] Most notably, all hosting providers must put in place notice-and-action mechanisms to allow individuals or entities to notify them of the presence of supposedly

63. Ibid., Arts. 10–13.
64. Ibid., Arts.14–15.
65. Ibid., Arts. 16–24.
66. Ibid., Arts. 25–33.
67. Ibid., Art. 2(h).
68. Ibid., Art. 25.
69. Ibid., Art. 13.
70. Ibid., Art. 23.
71. Ibid., Arts. 30–33.
72. Ibid., Art. 24.
73. Ibid., Art. 30.
74. The focus on advertising transparency, as a means to fight phenomena such as online disinformation, reflects the agenda proposed by the EC in its European Democracy Action Plan (EDAP). COM(2020)790 final, "On the European democracy action plan".
75. DSA, cited *supra* note 25, Art. 42.

illegal content.[76] Following such notification, the hosting provider is presumed to have actual knowledge or awareness of the specific item of information, and is, therefore, not able to enjoy any liability exemption.[77]

The resulting system envisaged by the DSA translates into what Balkin defined as "new-school speech regulation",[78] and reflects a desire to intervene through positive actions in the regulation of freedom of expression,[79] since it aims at controlling the digital networks themselves by emphasizing *ex ante* prevention through forms of collaborative cooperation between the private and the public. However, the Commission also took into account the risks connected to "collateral censorship",[80] and therefore tried to introduce within the DSA some antibodies to counteract drifts in directions endangering liberties. Most notably, together with the ban on general monitoring,[81] Article 17 introduces an obligatory internal complaint-handling system for online platforms against moderation decisions. Complaints will have to be decided on in a "timely, diligent, and objective manner" and, most interestingly, platforms will have to ensure that they are not solved based uniquely on the use of automated means.[82] In this sense, online platforms are thus required to protect individuals and society from the risk of their services being misused with illegal intent, while, at the same time, carefully balancing their decisions so as to avoid the unwarranted result of violating users' fundamental right to freedom of expression.

76. Ibid., Art. 14.

77. Online platforms are, in addition, required to "suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content" (Art. 20) and to inform authorities of any information suggesting "that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place" (Art. 21).

78. Balkin, "Old-school/new school speech regulation", 127 *Harvard Law Review* (2014), 2296–2342, at 2306.

79. Kuczerawy, "The power of positive thinking", 8 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2017), 226–237; De Gregorio, "Democratising online content moderation: A constitutional framework", 36 *Computer Law & Security Review* (2020), available at <doi.org/10.1016/j.clsr.2019.105374>.

80. Balkin, op. cit. *supra* note 78, at 2298; on the notion of "collateral censorship" see also Balkin, "Free speech and hostile environments", 99 *Columbia Law Review* (1999), 2295–2320, at 2298.

81. DSA, cited *supra* note 25, Art. 7.

82. Ibid., Art. 17(3) and (5). Art. 12(2), moreover, introduces some important substantial parameters for the enforcement of providers' terms and conditions: in particular, intermediaries are required to act with "due regard to the rights and legitimate interests of all parties involved, including the applicable fundamental rights of the recipients of the service as enshrined in the Charter". On Art. 12(2) DSA, see Appelman, Quintais and Fahy, "Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?" (*DSA Observatory*, 13 May 2021), available at <dsa-observatory.eu/2021/05/31/article-12-dsa-will-platforms-be-required-to-apply-eu-fundamental-rights-in-content-moderation-decisions/>.

As mentioned above, through the choice to adopt an asymmetric[83] approach as to the obligations imposed on the targets of regulation, the DSA welcomes the principle of proportionality, which represents a key feature of Union risk-based digital regulation. Besides, the text of the proposal requires that VLOPs make a yearly assessment of "any significant risks stemming from the functioning and use made of their services in the Union",[84] also taking into account the role of their content moderation, recommender, and advertising systems. Based on those risk assessments, VLOPs shall have to "put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified".[85] As a matter of fact, proportionality is explicitly mentioned in the Explanatory Memorandum as a driving principle of the DSA.[86] Nonetheless, at least at a first stage, the calibration of the duties provided for in Chapter III is mainly based on an assessment operated directly by the law. Providers of intermediary services are assigned to a certain category based on objective criteria set by the legislature *a priori* and on a top-down basis.

The structure of the DSA, in this sense, reduces the role of an aspect which is a key feature of the GDPR, i.e. the "responsibilization of the regulatee", which inevitably translates into the principle of accountability investing the targets of regulation. Put in this perspective, a critical difference emerges between the GDPR and the DSA, which is the role granted to the principle of accountability, as a result of the abandonment of a pure bottom-up approach to risk regulation. However, provisions such as those obliging VLOPs to assess the systematic risks connected to their services, and to act accordingly,[87] show that the gap between the DSA and the GDPR is only partial, and not complete. To a certain extent, providers are still autonomous in their risk mitigation duties. The establishment of an internal complaint-handling mechanism is a key example of this. Online platforms, both "very large" and "smaller", have to pay extra attention when proceeding to remove user-generated content or disabling access to recipients of their services, in that they have to respond to the latter if they unjustly limit their freedom of expression. In this sense, VLOPs and other online platforms are in many ways directly responsible and accountable for how they enforce their policies and the law.

83. Barata et al., "Unravelling the Digital Services Act package", *IRIS Special 2021-1* (European Audiovisual Observatory, Strasbourg 2021).

84. DSA, cited *supra* note 25, Art. 26.

85. Ibid., Art. 27. Recital 68 suggests that VLOPs might avail themselves of self- and co-regulatory agreements when adopting the necessary risk mitigation measures and, to this end, Art. 35 encourages the drafting of codes of conduct, also at the initiative of the European Commission or of the future European Board for Digital Services.

86. DSA, cited *supra* note 25, Explanatory Memorandum, at 6–7.

87. Cf. Barata et al., op. cit. *supra* note 83.

Ultimately, the approach followed by the DSA can be defined as hybrid. The overall structure of the DSA can be represented as a spectrum ranging from a predominantly top-down, compliance-based discipline to an increasingly bottom-up approach. Since they carry the most risks and since, due to their dimensions and revenues, VLOPs can put in place the appropriate measures for risk assessment, management, and mitigation,[88] these platforms are in many ways held accountable for their policies and for the harms and dangers arising from their infrastructures. Be that as it may, the DSA represents an essential and intermediate stage in the evolution of the Union's risk-based regulation of the digital landscape. The third stage is represented, as will be shown throughout the following section, by the AI Act.

4. The Artificial Intelligence Act: The top-down approach

With the AI Act, the shift from a bottom-up to a top-down approach to digital risk-based regulation is seemingly complete. The proposal, which was presented by the Commission in April 2021, represents a new critical step in the developing digital strategy of the Union. Also in this case, the choice was to resort to a risk-based approach aiming, on the one hand, to protect and foster "Union values, fundamental rights and principles",[89] and, on the other hand, to provide a set of uniform rules for ensuring the development of these technologies in the internal market.

The Union had long been aware of the need to intervene in this field. The White Paper on Artificial Intelligence underscored that AI, as "a collection of technologies that combine data, algorithms and computing power",[90] will represent a fundamental tool for the improvement of many aspects of our society (e.g. healthcare, farming, climate change mitigation, efficiency of production, security, etc.). Apart from being in many instances a potential hazard for safety, in the sense that a flaw in the design or in the training of an AI product may lead to injuries or other physical damages affecting natural persons,[91] automated systems, especially when they are delegated sensitive decision-making tasks, may also have a critical impact on a range of fundamental rights.[92] AI systems can be especially problematic because of

88. Cf. DSA, cited *supra* note 25, Recitals 54–56.

89. AI Act, cited *supra* note 24, Explanatory Memorandum, at 1.

90. COM(2020)65 final, "White Paper on Artificial Intelligence – A European approach to excellence and trust", at p. 2.

91. Think, for instance, of autonomous cars, or of automated components of planes, toys, and medical devices.

92. European Union Agency for Fundamental Rights (FRA), *Getting the Future Right. Artificial Intelligence and Fundamental Rights* (Publications Office of the EU, 2020);

their inherent opacity and lack of transparency,[93] and, on the other hand, because they can lead (and have often led) to incorrect, biased and discriminatory results.[94]

For this reason, the Union has focused its policy objectives on building an "ecosystem of trust" in order to foster the development of AI technologies while protecting citizens in the algorithmic society.[95] Besides, in 2019, the appointed High-Level Expert Group on AI had identified the seven key requirements for trustworthiness,[96] based on four ethical principles: respect for human autonomy, prevention of harm, fairness, and explicability.[97] Those seven key requirements – one of which is precisely the principle of accountability – represented a fundamental source of inspiration for the drafters of the AI Act.

With the purpose of building a legal framework fostering "trustworthy AI", the European Commission finally adopted a top-down risk-based approach in the AI Act, structured on four levels of risk referring to certain AI systems and their applications.[98] As for the DSA, the choice of such a risk-based model was ascribed to the goal of introducing a proportionate and effective system,

Pasquale, *New Laws of Robotics. Defending Human Expertise in the Age of AI* (Belknap Press, Harvard University Press, 2020).

93. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms", 3 *Big Data & Society* (2016), available at <doi.org/10.1177%2F2053951715622512>; Pasquale, *The Black Box Society. The Secret Algorithms that Control Money and Information* (Harvard University Press, 2015).

94. See, among others, Llansó et al., *Artificial Intelligence, Content Moderation, and Freedom of Expression* (TWG, 2020), available at <www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf>; Oliva, Antonialli and Gomes, "Fighting hate speech, silencing drag queens? Artificial Intelligence in content moderation and risks to LGBTQ voices online", 25 *Sexuality & Culture* (2021), 700–732; Pasquale, op. cit. *supra* note 92; Davidson, Bhattacharya and Weber, "Racial bias in hate speech and abusive language detection datasets", *Third Workshop on Abusive Language Online* (Florence, 2019), available at <dx.doi.org/10.18653/v1/W19-3504>.

95. White Paper on Artificial Intelligence, cited *supra* note 90, at p. 3.

96. Human agency and oversight; robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; accountability.

97. High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (2019), available at <digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. See Floridi, "Establishing the rules for building trustworthy AI", 1 *Nature Machine Intelligence* (2019), 261–262.

98. AI4EU Observatory Team, "The New Frontiers of European AI Regulation: How We Are Moving Toward Trustworthiness" (AI4EU, 2 July 2021) available at <www.ai4europe.eu/news-and-events/news/society/ethics/new-frontiers-european-ai-regulation-how-we-are-moving-toward>; Ebers, "Standardizing AI – The case of the European Commission's proposal for an Artificial Intelligence Act" in Di Matteo, Cannarsa and Poncibò (Eds.), *The Cambridge*

capable of combining both market-related and rights-related interests.[99] In this case, however, providers and users of AI systems are provided with little, if any, discretion as to the concrete and case-by-case assessment of the risks inherently connected to them.

Rather than entrusting providers and users of AI systems with the task of developing their own risk mitigation system, as is the case of the GDPR and, to a large extent, of the DSA, the AI Act restricts the margins of discretion. What truly changes with the AI Act is how the assessment of risk is carried out and by whom: in the GDPR, such a task is in the hands of data controllers; in the DSA, the Union legislature sets a top-down framework applicable to all providers of intermediary services, while still leaving space for a certain margin of discretion as far as enforcement of the law is concerned (especially in the case of VLOPs). With the AI Act, conversely, the shift towards a top-down approach seems significantly more evident, with the creation of a system where the leeway granted to producers and users is much more limited.

First, the AI Act proposal prohibits some practices involving systems whose use is deemed to be "unacceptable".[100] This category includes applications that manipulate human behaviour to circumvent the free will of users (e.g. voice-assisted toys that encourage minors to engage in dangerous behaviour) or that set up, by public authorities or on their behalf, the creation of a personal rating system based on personal behaviour or characteristics. It also includes the use of real-time biometric recognition systems in publicly accessible spaces for the purposes of law enforcement, unless this is necessary for one of a limited number of legitimate aims. All these AI technologies have been held *a priori* as too dangerous for the fundamental rights of people and invasive of their sphere of personal liberty.

Second, the Commission identifies a "high-risk" threshold for AI systems.[101] Technologies are held to be high-risk when they are used as a safety component of a product, or are themselves products, which are covered by the Union harmonization legislation listed in Annex II, or even when they are simply required to undergo a third-party conformity assessment, with a view to the placing on the market or putting into service of that product, pursuant to that same legislation. The Commission also provides in Annex III a list of additional AI systems which are to be considered as high-risk, including tools used for educational or professional training, where the algorithm can be used to assess a candidate's merit to access a scholarship; or,

Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics (Cambridge University Press, forthcoming 2022), available at <papers.ssrn.com/sol3/papers.cfm?abstract_id=3900378>.

99. AI Act, cited *supra* note 24, Recital 14.

100. Ibid., Art. 5; see Explanatory memorandum 5.2.2.

101. Ibid., Art. 6.

in the context of employment and selection of workers, AI software used by human resources offices to automatically categorize CVs. The Commission is empowered to adopt delegated acts to update Annex III, based on a list of criteria.[102] High-risk AI systems have to comply with a long and extensive series of requirements.

Most interestingly, high-risk AI systems seem to represent the only class where the legislature truly adopts a liability system more similar to that set by the DSA and, to a certain extent, that of the GDPR. Providers and users of those systems will have to establish, implement, document, and maintain a risk management system, with a view to adopting suitable measures to face any known or foreseeable hazard.[103] Additionally, providers of high-risk AI systems are required to put in place a quality management system to ensure compliance with the entire Regulation.[104] In this case, therefore, providers and users are given a margin of discretion to adopt necessary risk mitigation measures. However, it should be noted that the draft regulation still provides for a long list of duties and requirements which must be complied with; therefore, the room for manoeuvre granted to the targets of regulation is arguably only residual.

Third, some AI applications are included in a category characterized by "limited risks".[105] These include systems intended to interact with natural persons (such as chatbots), emotion recognition, or biometric categorization systems, as well as systems capable of generating "deep fake" contents. Providers and users of such tools must comply with specific transparency requirements. A person must therefore be informed that they are interacting with a chatbot, that they are being subjected to automated emotion recognition, or to biometric categorization, or that the content they see before them has been created artificially by an AI technology.

Finally, "minimal risk" is associated with AI applications that do not have the same invasiveness as those described above. For example, video games or spam filters applied to e-mail services are placed in this category. From this survey, it is clear that the spectrum embracing the set of AI applications with minimal risk is very broad and offers both the interpreter and the operator an opaque, albeit vast, range of application possibilities. Minimal risk AI applications are not subject to any specific duty or obligation, although the Commission and Member States may encourage and facilitate the drawing up

102. Ibid., Art. 7.
103. Ibid., Art. 9.
104. Ibid., Art. 17.
105. Ibid., Art. 52.

of codes of conduct intended to foster on their part the voluntary application of the requirements set for high-risk systems.[106]

In this case, the shift from a bottom-up to a top-down interpretation of risk-based regulation, already partially emerging from the DSA, reached its apex.[107] The categories of risk are defined directly by the Commission and set in stone within the law. The list of "unacceptable", and therefore prohibited, AI systems is directly set by the law and is independent of any *a posteriori* risk assessment by providers or users of those systems. The definition of high-risk technologies is also already defined by the law: in this case, the category is seemingly less rigid and more open to *ex post* change, since a procedure to amend the Annex III is possible. However, it is once again up to the Commission to make the necessary adjustments. The AI Act sets a range of risk criteria: however, in this case, they are meant as a guide for the Commission itself, and not for the targets of regulation. Moreover, although it is true that a risk management system for high-risk AI systems is introduced, extensive top-down rules specify how to implement it, thus leaving a relatively limited margin of discretion to providers and users. Additionally, high-risk systems have to comply with a far-reaching set of duties and obligations which follow a binary compliance/non-compliance logic.

The choice to adopt such a top-down approach to the risk regulation of AI directly affects the principle of accountability. As demonstrated in the previous sections, accountability is a direct corollary of a regulatory system which, to a certain extent, delegates to its targets the power to decide how to balance their own interests with the need to protect, guarantee and foster the rights and liberties of individuals, as well as the fundamental values characterizing the constitutional heart of the Union. The AI Act, which has been criticized for a range of reasons, including the lack of adequate remedies, has seemingly abandoned the bottom-up structure which characterized the first phase of risk-based digital regulation in the EU.[108]

Nonetheless, notwithstanding the critical aspects of the proposal, the system designed within the AI Act is arguably in line with Union risk-based regulation as a fundamental rights-driven framework. As will be highlighted

106. Ibid., Art. 69.

107. Pollicino et al., "Regolamento AI, la 'terza via' europea lascia troppi nodi irrisolti: ecco quali", *Agenda Digitale*, 21 May 2021, available at <www.agendadigitale.eu/cultura-digitale/regolamento-ai-la-terza-via-europea-lascia-troppi-nodi-irrisolti-ecco-quali/>.

108. Cf. Smuha et al., "How the EU can achieve legally trustworthy AI: A response to the European Commission's proposal for an Artificial Intelligence Act", SSRN, 5 Aug. 2021, available at <papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991>; Veale and Zuiderveen Borgesius, "Demystifying the draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach", 22 *Computer Law Review International* (2021), 97–112.

through the next section, the way risk-based regulation has been articulated is itself a product and a reflection of the general shift of the Union's approach towards the digital environment, characterized by the evolution from a liberal to a gradually more interventionist and constitutional-driven approach.

5. The EU's risk-based approach as a fundamental rights-driven system

The previous sections have underlined how risk has become a central feature of contemporary EU legislation with respect to digital technologies and the challenges characterizing the algorithmic society. At first glance, the development of such diverse approaches to risk regulation as those embodied by the GDPR (bottom-up), the DSA (hybrid), and the AI Act (top-down) might represent a cause for concern and preoccupations, given the apparently magmatic and chaotic character of the legal framework as a whole. The existence of such a wide array of legislative sources, all setting additional and new – and apparently inconsistent and incoherent – duties, could be regarded as potentially ineffective with respect to both ultimate goals of the Digital Single Market Strategy, i.e. the fostering of an innovative internal market and the contextual protection of fundamental rights.

At the outset, it should be clarified that the scope of the three described legislative sources is not unique. The targets of regulation are themselves different (although they can certainly coincide): thus, the GDPR applies to all actors, both public and private, that process individual personal data; the DSA is addressed only to a specific category of entities, i.e. that of providers of intermediary services, which are primarily private; the AI Act regulates the functioning of automated systems and, therefore, influences the activities of both providers and users of those systems, be they private or public actors. However, as has been outlined throughout the previous sections, what truly distinguishes the three instruments is how they each approach risk governance and how they develop a balance between the various interests at stake.

What changes, at a deeper level, is the way risk regulation itself is dealt with, and the relationship between regulator and regulatee. In the GDPR, the regulatee is responsible for balancing their own interests with that of the data subject and, for that choice, may be held accountable. As for the DSA and the AI Act, the decision concerning such balancing of conflicting interests shifts progressively from the regulatee to the regulator. Partly, such a mutation can be ascribed to the fact that the approval procedure of the GDPR was coordinated by a different Directorate-General from that of the DSA and the

AI Act,[109] and under the work of a different European Commission. However, the cause for such a development seems to be, ultimately, a slight change of direction as far as Union digital policies are concerned. The overall legal imprinting, indeed, has seemingly shifted from an eminently liberal (and negative) to a more clearly democratic (and active) approach, as a result of the rise of European digital constitutionalism.[110]

However, on a closer look, although they take different approaches and develop regulatory solutions which in many cases seem to conflict with one another, the three instruments share a common constitutional project. Notwithstanding the fact that they are different as to the means employed, the GDPR, the DSA, and the AI Act thus represent, each and every one of them, a step towards the establishment of a common framework for European digital constitutionalism, characterized by the consolidation of a democratic constitutional approach to address the challenges of the algorithmic society.[111] The purpose of fostering a human rights-driven and democratic-oriented framework for the digital environment is what allows us to bring together and give sense to the apparent inconsistency between the choices made by these three different instruments.

The three instruments, indeed, strive to find a balance between the various constitutional interests at stake. As a matter of fact, within the framework of the digital policies of the Union, the notion of risk itself ends up being a proxy for such a constitutional exercise, precisely the search for an equilibrium between, on the one hand, individual fundamental rights, and, on the other hand, the construction of an internal market where economic initiative can be fully enjoyed. With respect to the digital landscape, the Commission has proved to be aware of how much potential developing technologies have in the context of a globalized economy but, at the same time, is also concerned with the threats brought about by practices such as big data analysis and the spread of online digital services and algorithmic tools.[112] Through the employment of a risk-based approach, the purpose has been that of trying to push for both goals: the "economic" one, i.e. the building of an economically sustainable Digital Single Market, and the "constitutional" one, i.e. the introduction of a human-centric approach to digital policies respectful of individual fundamental rights and democratic values.

The three Acts, in this sense, aim to foster a European Digital Single Market that is not only driven by innovation but that is also respectful of the European

109. Indeed, the GDPR approval procedure was governed by the DG for Justice and Consumers, whereas the DSA and the AI Act have been mainly developed by the DG for Communications Networks, Content and Technology.

110. See De Gregorio, op. cit. *supra* note 27.

111. Ibid.

112. COM(2020)67 final, "Shaping Europe's digital future".

(constitutional) values enshrined in the Treaty on European Union, the EU Charter of Fundamental Rights, and the European Convention on Human Rights.[113] This common goal has its roots in the characteristics of European constitutionalism in which the logic of balancing permeates the entire constitutional architecture. Against this backdrop, no right or liberty, most notably economic freedom, may be invoked as a justification to destroy other individual fundamental rights. The prohibition on abuse of rights, enshrined in the ECHR,[114] and the EU Charter,[115] is part of this constitutional puzzle, which is primarily driven by human dignity.[116] The ultimate goal of European constitutionalism is, in other words, the search for an optimal balance between market interests and fundamental rights.

Such a constitutional architecture gradually invested the digital environment itself, and it is evident when looking at the role of the ECJ which has paved the way towards the rise of European digital constitutionalism. Following the institutionalization and recognition of the EU Charter as primary Union law, the role of the ECJ as a constitutional court has become even more relevant, and this role has been especially evident within the field of data protection law.[117] Through the development of a consistent body of case law, including *Digital Rights Ireland,*[118] *Google Spain*,[119] and *Schrems I*[120] and *II*,[121] the Court helped build the overall constitutional structure of the rights to data protection and privacy.[122]

In *Google Spain*, the ECJ shed light on how the application of fundamental rights such as those protected by the EU Charter should be based on an optimal

113. On the role of proportionality and balancing within modern constitutionalism, at a global and especially at a European level, see Stone Sweet and Mathews, "Proportionality balancing and global constitutionalism", 47 *Columbia Journal of Transnational Law* (2008), 72–164.

114. Art. 17 ECHR.

115. Art. 54 CFR.

116. As stated in *Omega*, even before the Lisbon Treaty, "the Community legal order undeniably strives to ensure respect for human dignity as a general principle of law". Case C-36/02, *Omega Spielhallen und Automatenaufstellungs- GmbH* v. *Oberbürgermeisterin der Bundesstadt Bonn*, EU:C:2004:614, para 34.

117. Pollicino, op. cit. *supra* note 4, at pp. 110 et seq.

118. Joined cases C-293 & 594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources* and *others and Kärntner Landesregierung and others*, EU:C:2014:238.

119. Case C-131/12, *Google Spain SL and Google Inc.* v. *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Google Spain)*, EU:C:2014:317.

120. Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner (Schrems I)*, EU:C:2015:650.

121. Case C-311/18, *Data Protection Commissioner* v. *Facebook Ireland Limited and Maximillian Schrems (Schrems II)*, EU:C:2020:559.

122. Fabbrini, "The EU Charter of Fundamental Rights and the rights to data privacy: The EU Court of Justice as a human rights court", *iCourts Working Paper Series No. 19,* (2015).

assessment of the various interests at stake.[123] In this decision, years before the GDPR, the ECJ ended up entrusting search engines with the duty to evaluate the stances of all actors involved, and to balance them with the potential damages that published content might cause to a data subject's privacy rights. In this sense, the ECJ anticipated the bottom-up risk-based approach characterizing the GDPR, by entrusting search engines, as data controllers, with the responsibility for ensuring individuals' rights as set in the Data Protection Directive.[124] Later case law reveals, instead, a more interventionist approach. Notably, in the *Schrems* decisions, the ECJ autonomously struck down both the Safe Harbour Decision and the Data Privacy Shield on the grounds that they were not fully compliant with the principles of the GDPR and were not sufficient to protect EU citizens from the risks connected to their data being transferred to the United States.[125] In this sense, a slight shift from a bottom-up to a top-down perspective arguably occurred within the case law of the ECJ itself.

This process is directly reflected by the EU's digital risk-based regulation, which is, ultimately, an attempt to regulate the digital market by striking the optimal balance between innovation and protection of constitutional and democratic values, although this is done by adopting various perspectives and points of view. The main example of this is, clearly, the GDPR. This instrument focuses specifically on the right to privacy and data protection, extensively defined at the outset in its contents and elaborations (e.g. lawfulness of processing;[126] transparency;[127] right to information;[128] right of access by data subject;[129] right to rectification;[130] right to be forgotten;[131]

123. As is well known, one of the major concerns in *Google Spain* was the need to ensure a correct balance between the data subject's right to privacy and the public's interest to being informed. See Case C-131/12, *Google Spain*, para 81.

124. Thus Pollicino, op. cit. *supra* note 4, at p. 194: today "Google enjoys broad margins of discretion in deciding whether to delist information": in doing so, it has to engage in the balancing and enforcement of individuals' fundamental rights online.

125. As highlighted by Ojanen, the ECJ, in Case C-362/14, *Schrems I*, expressly specified that the right to privacy has a core which cannot be negotiated nor balanced with other interests. The ECJ thus evaluated that, in the case at hand, the Safe Harbour Decision did not respect the core, i.e. the "essence" of the rights set by Arts. 7 and 8 CFR. Ojanen, "Making the essence of fundamental rights real: The Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter: ECJ 6 October 2015, Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*", 12 EuConst (2016), 318–329.

126. GDPR, cited *supra* note 23, Arts. 6 et seq.

127. Ibid., Art. 12.

128. Ibid., Arts. 13–14.

129. Ibid., Art. 15.

130. Ibid., Art. 16.

131. Ibid., Art. 17.

portability[132]), and represents the first stage of a regulatory trend where fundamental rights are at the forefront. The Regulation's bottom-up approach is, ultimately, an attempt to set the limits to market interests by identifying the core principles that digital technologies should respect. In this sense, this framework fully discloses the constitutional characterization of the GDPR as a meta-regulation founded on a principle-based logic where privacy and data protection are the guiding principles of technological development.

The same goal, although from different perspectives, is also sought by the other two instruments. The DSA and the AI Act are also intended as a response to the negative externalities, in terms of fundamental rights and human dignity, which are inherently connected to digital innovation. However, the techniques these two instruments employ are rather different in that they leave behind the liberal imprint of the GDPR, pursuant to which the targets of regulation are themselves vested with the task of balancing rights and powers, and adopt a progressively more interventionist approach.

The DSA, as an intermediate step, protects fundamental rights by focusing on identifying the risk categories to which providers of intermediary services should be ascribed and establishing, through a "supervised" method, how those actors should address the dangers entailed by their businesses. Like the GDPR, the ultimate goal of the DSA is to find an optimal equilibrium capable of combining digital innovation and the constitutional values of the EU. What changes is the distribution of scaling and balancing duties. Whereas the GDPR wholly delegates such duties to data controllers, the DSA operates a first risk assessment itself, based on which obligations are imposed on Internet service providers. Subsequently, the various legal regimes assigned to regulated actors allow for different degrees of discretion. In other words, balance is sought through a double evaluation, so that responsibility for finding the appropriate equilibrium is shared by the legislature and by the targets of regulation.

The AI Act, on the other hand, directly regulates the use and functioning of AI systems. Throughout the entire Explanatory Memorandum and text of the draft law, the need to protect natural persons from the dangers of these tools is at the forefront, although this purpose is sought directly through vertical regulation. Even in this last case, however, the choice to establish different categories is the direct consequence of the aspiration for an optimal balance. Again, the main difference does not alter the spirit of the law which is, once again, a reflection of the European constitutional spirit. The difference simply concerns the means employed and, more precisely, the distribution of the balancing task itself, which is, in this case, mainly a prerogative of the European Commission.

132. Ibid., Art. 20.

The three legislative instruments analysed thus reflect the general evolution of Union digital policies, moving from a liberal to a more active and constitutional-driven approach, aimed at fostering and guaranteeing fundamental rights and democratic values in the algorithmic society. If such a perspective is taken, the resort to such diverse elaborations of the risk-based approach to the protection of digital fundamental rights can lose its apparent disconnect. Through the lens of digital constitutionalism, it is possible to retrieve a common purpose, that is the balancing of fundamental rights, market, and innovation interests, with a view to ensuring as much as possible a framework of "constitutional optimization".[133]

This approach may represent an essential standpoint to address also future legislative reforms and policy initiatives, considering that the three instruments ultimately reflect a unique goal and aspiration, though the means they use might appear, to a large extent, different. The GDPR, the DSA, and the AI Act are part of a unique constitutionalizing process investing the foundations of the digital age: this way, as part of a unitary (although sometimes not fully clear) picture, the three instruments can offer valuable insights on the direction of European digital constitutionalism itself. Further research in this sense could help predict the outcomes and developments of the EU's digital policies, as well as represent an invaluable asset to suggest new legislative solutions compatible and consistent with that picture.

6. Conclusions

Risk regulation has gathered increasing momentum across Western democracies and has become increasingly popular as a regulatory tool to foster Union policies in a range of operative fields, including, lately, the governance of the Digital Single Market in the context of the algorithmic society.

The legislative (and constitutional) strategy of the EU's digital policy underwent an evolution with respect to its own approach to risk-based regulation, with a progressive but radical shift from a bottom-up (GDPR) to a top-down (AI Act) approach. The GDPR highlights the relevance of fundamental rights becoming the guide for data controllers and processors when assessing the risks for data subjects in the processing of personal data. Rather than introducing a long and extensive set of compliance-based duties and obligations, the GDPR focuses on the accountability and general principles which represent the horizontal translation of the right to privacy and data protection. The designation of the means adopted to comply with general

133. Vermeule, op. cit. *supra* note 26.

principles is, nonetheless, a task left to the discretion of data controllers. Fundamental rights thus become a parameter which organizations need to consider when balancing their own interests with the duty to protect individuals' fundamental rights. An inevitable consequence of this system is that legal accountability for those choices falls entirely on data controllers.

The DSA adopts a different view, in that it provides for a framework where the balancing between the goal of protecting fundamental rights and that of fostering the Digital Single Market is shared between the government and the governed. Risk assessment follows a two-phase procedure. In the first stage, it is a top-down regulation that categorizes providers of intermediary services in groups based on a general and *a priori* evaluation of objective risk criteria. Only at a second stage are private actors called to perform a further balancing operation where more specific risk mitigation measures are defined. The role of intermediaries, therefore, comes into play only at a subsequent moment, and is itself scaled depending on the category they have been assigned to by the law. As a consequence, accountability, rather than being a "monolithic" principle, equally applicable to all targets of regulation, takes the form of a spectrum, at one end of which VLOPs, as actors almost fully responsible for their fundamental rights policies, can be found.

Finally, the AI Act completes the shift from a bottom-up to a top-down approach towards risk regulation. As seen in section 4, the provisions set within the regulation proposal are a result of a risk assessment operated directly by the law, in which four risk categories for AI systems are identified. Again, a preliminary decision is operated directly by the law, and the solution is a pyramidal structure similar to that defined by the DSA. However, a different regulation follows such a categorization. In a way which is rather different from, if not the opposite of, the system introduced by the DSA, the AI Act couples higher levels of risk with relatively little margin of discretion as to the measures to employ for risk mitigation. The risk-based approach, as a technique for fostering a proportionate and calibrated scheme of duties and obligations, takes in the AI Act a top-down turn where providers and users of AI systems must comply with requirements already established by the law, in a manner which draws the prospective regulation nearer to a command-and-control system.

The GDPR, DSA and AI Act all share this common constitutional feature, and resort to risk as a proxy to develop a framework adequately and fairly balancing the various economic and constitutional interests purported by the Union in the regulation of the Digital Single Market. This ultimate role of risk as an optimal balancing technique allows a connection to be made between the provisions contained within the three analysed instruments, which are otherwise characterized by differing, if not opposing, structures and models.

Such differences acquire a deeper meaning if put in the context of the constitutional pattern rapidly developing in the digital framework of the Union. The shift from a bottom-up, liberal perspective to an increasingly top-down, active approach is also apparent from the ECJ case law in recent years. If the EU's constitutional experience is characterized by the endeavour to strike an equal, and proportionate, balance between the various interests of social parties, the *fil rouge* at the heart of the GDPR, DSA, and AI Act is precisely that they strive to create a digital environment which embraces European constitutional values and principles.

Although the means may be different, as has been extensively highlighted throughout the previous sections, the GDPR, the DSA, and the AI Act all share the same purpose. As pointed out above, the major goal of the EU's risk-based digital policies as driven by the characteristics of European constitutionalism is, ultimately, the (optimal) balance between the promotion of economic freedoms to foster the internal market and the protection of fundamental rights and democratic values. Therefore, to connect the dots and make sense of the complex set of legal instruments, the lens of European digital constitutionalism can offer us valuable insights to understand the future developments of the EU's digital strategy and help suggest constitutional solutions to address the challenges of the algorithmic society.

COMMON MARKET LAW REVIEW

Personal subscription prices at a substantially reduced rate as well as online subscription prices are available upon request. Please contact our sales department for further information at +31 172641562 or at International-sales@wolterskluwer.com.

Payments can be made by bank draft, personal cheque, international money order, or UNESCO coupons.

All requests for further information
and specimen copies should be addressed to:

Kluwer Law International
P.O. Box 316
2400 AH Alphen aan den Rijn
The Netherlands
fax: +31 172641515

For Marketing Opportunities please contact International-marketing@wolterskluwer.com

Please visit the Common Market Law Review homepage at http://www.kluwerlawonline.com for up-to-date information, tables of contents and to view a FREE online sample copy.

Microfilm and Microfiche editions of this journal are available from University Microfilms International, 300 North Zeeb Road, Ann Arbor, MI 48106, USA.

The Common Market Law Review is indexed/abstracted in Current Contents/Social & Behavioral Sciences; Current Legal Sociology; Data Juridica; European Access; European Legal Journals Index; IBZ-CD-ROM: IBZ-Online; IBZ-lnternational Bibliography of Periodical literature on the Humanities and Social Sciences; Index to Foreign Legal Periodicals; International Political Science Abstracts; The ISI Alerting Services; Legal Journals Index; RAVE; Social Sciences Citation Index; Social Scisearch.