Profiling under Risk-based Regulation: Bringing together the GDPR and the DSA

Giovanni De Gregorio[*] and Pietro Dunn[°]

Abstract

In the last years, risk has become a proxy and a parameter characterising the Union regulation of digital technologies, with a view to serving the twofold goal of fostering the Digital Single Market while protecting individuals' fundamental rights. Data processing based on the profiling of individuals represents an innovative tool increasingly used by businesses playing in the internal market. The processing of vast amount of data allows obtaining information about the behaviours, preferences, and lifestyles of data subjects. Such possibilities represent an invaluable asset for marketing strategies, but raises in turn many concerns with regard to individuals' fundamental rights to data protection, privacy, dignity, non-discrimination and self-determination. We argue that the regulatory strategy adopted by the Union with respect to profiling is largely based on a risk-based approach, and that this emerges especially from the text of the General Data Protection Regulation (GDPR) and from the recent proposal for a Digital Services Act (DSA). We acknowledge that these two instruments resort themselves to different architecture: most notably, whereas the structure of the GDPR reflects a bottom-up perspective, this character is less evident within the DSA. While acknowledging that such diverse approach may raise concerns with regard to the principles of the rule of law and, especially of legal certainty, we argue nonetheless that the resulting framework is, ultimately, coherent and characterised by the fil rouge of risk as a proxy for the balancing of the various interests at stake. Moreover, we hold that such an approach is consistent with the constitutional human rights framework of the Union and may be fully understood through the lens of digital constitutionalism.

Keywords: Risk-based regulation – Profiling – Artificial Intelligence – Fundamental Rights – Digital Constitutionalism

I. Introduction

Digital technologies have become more and more essential within the contemporary societal and economic landscape, allowing for unprecedented developments in a range of areas and fields such as healthcare, communication, and e-commerce. The "algorithmic society", where large multinational social platforms sit between traditional nation states and ordinary individuals and where algorithms and AI agents are employed by public and private actors,[1] has nonetheless also amplified the risks concerning a range of fundamental human rights of the individual,[2] such as,

[*] Post-doctoral researcher, Centre for Socio-Legal Studies, University of Oxford, giovanni.degregorio@csls.ox.ac.uk.
[°] PhD student, University of Bologna – University of Luxembourg, pietro.dunn2@unibo.it.
[1] Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 University of California Davis Law Review 1149.
[2] Deborah Lupton, 'Digital Risk Society' in Burgess, Alemanno and Zinn (eds), *Routledge Handbook of Risk Studies* (Routledge 2016).

most notably, the right to privacy and data protection.[3] COVID-19, on the one hand, has greatly accelerated this process, by making the digital environment more necessary than ever, and, on the other hand, gave an impulse to the development of new tools, including contract-tracing apps and COVID-19 "green" certificates, which have in turn caused concerns for the protection of persons' interests.[4]

The processing of vast amount of data allows obtaining information about the behaviours, preferences, and lifestyles of data subjects.[5] The implementation of automated decision-making, especially based on machine-learning techniques, raises challenges not only for privacy and data protection but also for the potential discriminatory and biased results coming from inferential analytics.[6]

Though the resort to such techniques may at first glance be perceived as less problematic when considering the statistical or research field, the same processing acquires nonetheless a different value when the categorisation of the individual in a group rather than in another one leads to a decision affecting individuals' rights.[7] Profiling and automated decisions are processes whose implicit goal is to divide groups of individuals into different categories based on common characteristics and make decisions based on the person's belonging to a specific group.[8] Profiling and automated decision-making do not focus on individuals as such, but considers them as part of clusters or groups based on common characteristics.[9] This automatic classification can lead to discrimination and serious effects on individuals' fundamental rights and freedoms.[10]

The practice of profiling citizens and consumers, in particular, has been increasingly addressed by the Union, as it is potentially detrimental not of individuals' privacy rights, as well as of their rights to self-determination, to non-discrimination, to freedom of expression, and, in general, to

[3] See, among others, José Van Dijck, 'Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology' (2014) 12(2) Surveillance & Society 197; Shoshana Zuboff, *The Age of Surveillance Capitalism. The Fight for a Future at the New Frontier of Power* (PublicAffairs 2019).

[4] See, for instance, Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet* (Hart 2021), at 181; Oskar J Gstrein, 'The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment' (2021) 12(2) European Journal of Risk Regulation (2021) 370.

[5] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1*;* Tal Zarsky, 'Understanding Discrimination in the Scored Society' (2014) 89 Washington Law Review 1375; Frederike Kaltheuner and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) 2(2) Journal of Information Rights, Policy and Practice.

[6] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

[7] Brent Mittelstadt and Luciano Floridi, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22 Science and Engineering Ethics 303.

[8] Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a "Right To Explanation"' (2016) 38 AI magazine 50.

[9] Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor and others (eds), *Group Privacy* (Springer 2017).

[10] Maddalena Favaretto, Eva De Clercq and Bernice Simone Elger, 'Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review' (2019) 6 Journal of Big Data 12; Talia B Gillis and Jann L Spiess, 'Big Data and Discrimination' (2019) 86 The University of Chicago Law Review 459; Monique Mann and Tobias Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6(2) Big Data & Society < https://journals.sagepub.com/doi/pdf/10.1177/2053951719895805> accessed 12 October 2020; Safiya U Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018).

human dignity.[11] Profiling, defined "as the construction or inference of patterns by means of data mining and as the application of the ensuing profiles to people whose data match with them",[12] has been variously dealt with by a range of legislative Union sources, especially in the field of data protection.

In recent years, the policy practices of Union regulation, with respect to the protection of fundamental human rights in a digital context, have increasingly turned towards a "risk-based" approach. Since the launch of the Digital Single Market Strategy,[13] the Union has increasingly relied on risk-based approach in the field of digital policy. Rather than just setting new rights and safeguards, the Union has tried to regulate risks by increasing the accountability of the public and private sector. Technically speaking, "risk" is a combination between the probability of a defined hazard occurring and the magnitude of its consequences, and can thus serve as a proxy for decision-making, based on the forecasting of positive or negative future events.[14] This is mainly done through the practices of risk analysis, which consists of a set of methodologies, templates and processes.[15] Risk regulation can thus be perceived as an attempt to face the rise of what has been defined as the "risk society"[16] through a rational and technocratic approach which fosters more efficient, objective, and fair governance,[17] whilst fighting against "over-regulation, legalistic and prescriptive rules, and the high costs of regulation".[18]

Within this framework, this paper proposes a way to find a legal coherence among the different risk-based approaches influencing profiling. We argue that, despite different approaches to risk which could affect the principle of the rule of law and legal certainty in the internal market, we the resulting framework is consistent in creating an overall coherent regulation of the phenomenon. The resort to a risk-based approach, indeed, can be linked to the transformation of

[11] Brent Mittelstadt et al, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data & Society (2016) <https://doi.org/10.1177%2F2053951716679679> accessed 28 September 2021; Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer 2008).

[12] Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) Modern Law Review 428, at 431

[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe (COM/2015/192 final).

[14] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press, 2020), at 27-28. See also Raphaël Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279; Bernstein, *Against the Gods. The Remarkable Story of Risk* (John Wiley & Sons, 1996).

[15] 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 Bridget M Hutter, 'Risk, Regulation, and Management' in Peter Taylor-Gooby and Jens Zinn (eds), *Risk in Social Science* (Oxford University Press 2006). As highlighted by Alberto Alemanno, 'Regulating the European Risk Society' in Alberto Alemanno et al. (eds), *Better Business Regulation in a Risk Society* (Springer 2013), at 53, EU law also recognises risk communication as a third component, which essentially entails "providing information on levels of health, safety, and environmental risks, their significance, and their management".

[16] Ulrich Beck, *Risk Society. Towards a New Modernity* (Mark Ritter tr, Sage Publications 1992).

[17] Bridget M Hutter, 'A Risk Regulation Perspective on Regulatory Excellence' in Cary Coglianese (ed.), *Achieving Regulatory Excellence* (Brookings Institution Press 2017).

[18] Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-fold Shift' (2017) 8 European Journal of Risk Regulation 506, at 509. See also Julia Black, 'The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom' (2005) Public Law 510, at 512.

the European approach which in the last twenty years has moved from a market-based approach to a constitutional strategy.[19]

The focus of this contribution will be set, in particular, upon the General Data Protection Regulation (GDPR)[20], and upon the Digital Services Act (DSA) proposal, presented by the Commission in December 2020.[21] These two instruments adopt different perspectives with respect to the issue of profiling but find a common ground in the choice to follow a risk-based approach to confront it. Section II focuses on analysing the GDPR's risk-based approach to profiling. Section III analyses how the developing legal framework of content moderation, enshrined within the DSA, addresses such a topic. Section IV aims to catch the differences and similarities between the two instruments, which ultimately represent two expressions of the same, unitary Union constitutional framework.

II. Profiling and the Risk-based Approach in the GDPR

In the Explanatory Memorandum to the initial proposal for the GDPR, the Commission stressed how EU law had to be updated to the new societal context, where technology allows both private actors and public administrations "to make use of personal data on an unprecedented scale in order to pursue their activities".[22] In the face of the changing landscape, the GDPR re-set the focus of data protection law, stressing the central role of individual fundamental rights within the framework of European data protection law.[23] In this context, profiling, defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person",[24] represents a source of particular concern because of the impact it might have directly on human dignity. Moreover, the use of profiling techniques for the purposes of automated decision-making is explicitly recognised as potentially leading to discriminatory results.[25]

The regulatory solution employed by the GDPR, as a means to protect such fundamental rights while avoiding constraining excessively and suffocating data analytics developing practices, has been that of resorting to a risk-based approach which is grounded specifically in the principle of accountability.[26] This principle implies that the data controller should be able to prove they are compliant with the general principles and provisions set by the Regulation.[27] It is up to the data

[19] Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19(1) International Journal of Constitutional Law 41.
[20] 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) [2016] OJ L119/1.
[21] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM/2020/825 final).
[22] 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) (COM/2012/11 final).
[23] GDPR, supra, note 20, Recitals 1-2.
[24] Ibid, Art. 4(4).
[25] Ibid, Recital 71.
[26] Ibid, Art. 5(2).
[27] Thus Céline Castets-Renard, 'Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making' (2019) 30(1) Fordham Intellectual Property, Media & Entertainment Law Journal 91, at 107: "Accountability starts with an agent and the outcome of its actions;

controller to ascertain how much a specific data processing activity might impact on an individual's fundamental rights: based on that assessment, data controllers will have to design the appropriate responses to reduce and mitigate such risks. If a data controller is not able to prove that they have put in place measures sufficient for complying with the GDPR, they will be held directly accountable.

The GDPR relies directly on the targets of regulation as far as the definition of risk scores is concerned: the law does not directly establish any risk thresholds but leaves such a sensitive duty to regulated actors. In this sense, the risk-based approach of the GDPR may be defined as bottom-up. 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".[28] In this sense the GDPR overcomes the traditionally "rights-based",[29] approach of European data protection law, intended as a "command-and-control" form of regulation.[30] Instead, the GDPR follows the "granular, scalable, logic of risk analysis",[31] and constitutes a form of principle-based regulation founded on the principles of proportionality and accountability. Obligations may, therefore, be objectively "uneven" based on the actor called to comply with the GDPR, but this different outcome is justified in that it is the consequence of a specific balancing test based on the principles of accountability and proportionality.[32]

Aware of the fundamental rights risks connected to decision-making based on automated processing, including profiling, the GDPR sets specific safeguards. Against such processing, the data subject has the right to object at any time, for reasons connected with their particular situation. However, this right is not absolute since it can be exercised only when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,[33] or for the purposes of the legitimate interests pursued by the controller or by a third party (except where such interests are overridden by the interests

---

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".

[28] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 European Journal of Risk Regulation 502, at 506.

[29] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015). According to the Author, at 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".

[30] Bridget M Hutter, supra, note 15, at 203. According to Gellert, *The Risk-Based Approach to Data Protection*, supra, note 14, at 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".

[31] Gellert, Ibid, at 2.

[32] Besides, GDPR, supra, note 20, Art. 35(1) 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. Such an obligation represents a typical point of contact between the managerial practices of risk management and risk regulation, so much so that Alberto Alemanno, supra, note 15, at 41, defines it as a "*Grundnorm*", i.e. as "the privileged methodological tool for regulating risk in Europe"

[33] Ibid, Art. 6(1)(e).

or fundamental rights and freedoms of the data subject which require protection of personal data, primarily where the data subject is a child).[34] Therefore, the scope of such right is narrow and it cannot find a legal basis when profiling occurs based on the consent of the data subject or any other legal basis provided for by the GDPR.

Even more importantly, Article 22 sets a general right of individuals not to be subject to such practices, unless this is necessary for entering into or performing a contract, unless the data controller is explicitly authorised to do so by Union or Member State law setting suitable measures and safeguards for persons' rights, or unless the data subject has expressly given their consent. However, whenever a data controller resorts to automated decision-making and profiling, they must nonetheless "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests", including the right to obtain human intervention, the right to intervention in the decisional process and the right to contest the decision itself. Automated decision-making and profiling may also be based on the collection and processing of the special categories of personal data included within Article 9, if the data subjects give their explicit consent or if it is necessary for reasons of substantial public interests: in this case, however, data controllers shall have to put in place additional safeguards to ensure the full respect of individual rights.

The GDPR thus delegates data controllers the fundamental role of identifying on their own the proper means to comply with the requirements it sets. Most notably, data controllers are not prohibited from the deploying profiling techniques and automated decision-making processing potentially affecting natural persons' fundamental privacy rights. Indeed, as highlighted above, the right to object is very limited as to its scope of action, and Article 22 as well keeps the doors open for the profiling of individuals. However, when fundamental rights are at stake, data controllers may well be held accountable for the negative impact their processing activities have produced. The targets of the GDPR are thus granted a broader discretion than that which would be possible under a binary command-and-control approach, but precisely for this reason they are potentially liable for their choices. The GDPR, in other words, inherently points towards a "responsibilisation of the regulatee".[35] The key-word is, in this sense, "proportionality": higher risks connected to a specific profiling activity will generally be acceptable as long as they are coupled with *ad hoc* measures.

III. Profiling and the Risk-based Approach in the DSA

The DSA was presented in December 2020 as part of a package 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 of establishing "a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally".[36] The DSA explicitly foresees a general and horizontal reform of intermediary liability. The Explanatory Memorandum explains

[34] Ibid, Art. 6(1)(f).
[35] Gellert, *The Risk-Based Approach to Data Protection*, supra, note 14, 20.
[36] European Commission, 'The Digital Services Act Package' (*European Commission*, 31 August 2021) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 31 August 2021. See, on this topic, Martin Eifert and others, "Taming the Giants: The DMA/DSA Package", 58(4) *Common Market Law Review* (2021), 987-1028.

that, since the adoption of the e-Commerce Directive (ECD),[37] new digital services have emerged, revolutionising 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.[38]

Like the GDPR, the DSA also adopts a risk-based approach, in the sense that the targets of regulation, i.e. the providers of intermediary (digital) services, are subject to duties and obligations which are proportional and calibrated to the concrete risks, to society and to individuals' rights and liberties, their services entail. However, in stark contrast with the bottom-up structure of the GDPR, the DSA sets a series of risk thresholds, based on which intermediaries are assigned to different categories and are subject to different regulation. In other words, a preliminary risk assessment is made directly by the legislator. Providers of intermediary services are assigned to a certain category based on objective criteria set by the legislator *a priori* and on a top-down basis. Thus, a small group of provisions applies to all providers of intermediary services,[39] whereas the subsequent Articles have an increasingly narrow scope of application: hosting providers;[40] online platforms;[41] and "very large online platforms" ("VLOPs").[42] 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 "responsibilisation of the regulatee", which inevitably translates into a reduction of the space granted to the principle of accountability. The Explanatory Memorandum to the proposal, in this sense, speaks of a "supervised risk management approach, with an important role of the governance system for enforcement".[43]

The new asymmetric due diligence obligations, though keeping intact, in the background, the general structure of the "safe harbour" approach designed by Articles 12-15 ECD,[44]aim at guaranteeing "a transparent and safe online environment". In this sense, they move in two main directions: the fostering of transparency;[45] the involvement of intermediaries in the fight against illegal content and illegal activities on the Internet, including content violating the fundamental rights of individuals (for instance, all hosting providers must put in place notice-and-action mechanisms against illegal content).[46] The resulting discipline translates into what Balkin defined as "new-school speech regulation",[47] since it aims at controlling the digital networks themselves

[37] 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') [2000] OJ L178/1.
[38] DSA, supra, note 21, Explanatory Memorandum, at 1.
[39] Ibid, Artt. 10-13.
[40] Ibid, Artt.14-15.
[41] Ibid, Artt. 16-24. Pursuant to Art. 2(h), online platforms are a subset of hosting providers which, upon request, disseminate user-generated content to the public
[42] Ibid, Artt. 25-33. An online platform is considered "very large" if when it provides its services to a number of average monthly recipients in the EU which is equal or higher than 45 million.
[43] Ibid, Explanatory Memorandum, at 11.
[44] Ibid, Artt. 3-5 and 7. See Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) European Journal of Risk Regulation, <https://doi.org/10.1017/err.2021.8> accessed 1 September 2021, at 6 ff.
[45] DSA, supra, note 21, Art. 13. Additional duties apply to online platforms (Art. 23) and to VLOPs (Artt. 30-33).
[46] Ibid, Art. 14.
[47] Jack M Balkin, 'Old-School/New School Speech Regulation' (2014) 127 Harvard Law Review 2296, at 2306.

by emphasising *ex ante* prevention through forms of collaborative cooperation between the private and the public.

As highlighted by Barata,[48] this may well push online providers to resort to automated systems of content moderation. This may well be a problematic from various perspectives. First, automated content moderation is more than often subject to errors, including false positives,[49] which could thus affect freedom of expression. Second, and more interestingly for the purpose of the present contribution, research has shown how these AI systems often censor content from minorities more frequently than content from majority groups: thus, for instance, users speaking African-American English[50] or employing LGBTQIA+ slang[51] are more targeted than others. To a certain extent, minority groups are thus clustered together, and thus profiled, based on the language they use and subsequently suffer from discriminatory consequences. Aware of these risks, inherently connected to "collateral censorship",[52] the Commission tried to introduce within the DSA some antibodies. Most notably, Article 17 introduces an obligatory internal complaint-handling system for online platforms against moderation decisions which will have to be decided upon in a "timely, diligent, and objective manner" and, most interestingly, not based uniquely on the use of automated means.[53] Online platforms are therefore required, when applying the rules set out in the DSA, to keenly balance the various interests at stake, including individuals' fundamental rights to privacy, data protection, non-discrimination, dignity, and freedom of expression.

In addition to this, VLOPs, pursuant to Articles 26 and 27, are required to make a yearly assessment of "any significant risks stemming from the functioning and use made of their services in the Union", also taking into account the role of their content moderation, recommender, and advertising systems.[54] Based on those risk assessments, VLOPs shall "put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks

[48] Joan Barata, 'The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations' (*DSA Observatory*, 27 July 2021) <https://dsa-observatory.eu/2021/07/27/the-digital-services-act-and-its-impact-on-the-right-to-freedom-of-expression-special-focus-on-risk-mitigation-obligations/> accessed 4 September 2021.

[49] See, for instance, Evelyn Douek, 'Governing Online Speech: From "Post-as-Trumps" to Proportionality and Probability' (2021) 121(3) Columbia Law Review 759.

[50] Thomas Davidson, Debasmita Bhattacharya and Ingmar Weber, 'Racial Bias in Hate Speech and Abusive Language Detection Datasets' (2019) Proceedings of the Third Workshop on Abusive Language Online (Florence, Italy) 25.

[51] Thiago Dias Oliva, Dennys Marcelo Antionially and Alessandra Gomes, 'Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online' (2021) 25 Sexuality & Culture 700.

[52] Balkin, supra, note 47, at 2298; on the notion of "collateral censorship" see also Jack M Balkin, 'Free Speech and Hostile Environments' (1999) 99(8) Columbia Law Review 2295, at 2298.

[53] DSA, supra, note 21, 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 Naomi Appelman, João Pedro Quintais and Ronan Fahy, 'Article 12 DSA: Will Platforms Be Required to Apply EU Fundamental Rights in Content Moderation Decisions?' (*DSA Observatory*, 13 May 2021) <https://dsa-observatory.eu/2021/05/31/article-12-dsa-will-platforms-be-required-to-apply-eu-fundamental-rights-in-content-moderation-decisions/> accessed 4 September 2021.

[54] DSA, supra, note 21, Art. 26.

identified".[55] On the one hand, these Articles show that the accountability gap between the GDPR and the DSA is only partial: to a certain extent, providers are still autonomous in their risk mitigation duties, and are thus held accountable of the decisions they may take and of the efficiency of the measures they adopt. In this sense, the approach followed by the DSA is a hybrid one, where online platforms, and especially VLOPs, are held accountable for their mitigation systems since they carry the most risks.[56] On the other hand, such provisions confirm the Commission's specific concerns towards profiling of individuals and consumers. The recommender and advertising systems described within Articles 26-27, as a matter of fact, rely on the algorithmic profiling of users and can thus disrupt the individual experience of personal identity.[57] VLOPs can resort to these systems for marketing purposes, but are required to implement adequate measures to avoid the impairment of users' fundamental rights and liberties.

Besides, recommender and advertising systems are also subject to extra transparency requirements. VLOPs must set out clearly in their terms and conditions the parameters used by their recommender systems, and must also ensure that users are granted at least one option "which is not based on profiling within the meaning of Article 4(4) of Regulation (EU) 2016/679".[58] Additionally, they must provide information concerning the display of online advertising, including "whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose".[59]

Overall, the DSA sets out a regulatory framework pursuant to which digital services providers, most notably VLOPs, are held accountable and responsible for the governance of the risks connected to the implementation of profiling systems and automated decision-making. Once again, these systems are not prohibited, but actors employing them must couple them with adequate and proportionate measures safeguarding natural persons' interests. In this sense, they will be, again, accountable for failing to protect the rights to privacy, data protection, dignity and non-discrimination.

IV. Digital Risk-Based Regulation: A Unitary Approach to Profiling?

Risk has become a central feature of contemporary European legislation with respect to digital technologies and the challenges characterising the algorithmic society. The GDPR and the DSA are only two examples of the many legislative instruments which the Union has enacted, or foresees to enact, using risk as a proxy and a balancing criterion essential to foster digital human rights while ensuring, at the same time, the full development of the Digital Single Market. Risk-based regulation, however, can take different forms. Thus, for instance, the GDPR takes an eminently bottom-up approach, whereas such a character is much less visible within the DSA.

[55] 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 purpose, 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

[56] Cf. Ibid, Recitals 54-56.

[57] Silvia Milano, Mariarosaria Taddeo and Luciano Floridi, 'Recommender Systems and their Ethical Challenges' (2020) 35 AI & Society 957.

[58] DSA, supra, note 21, Art. 29.

[59] Ibid, Art. 30.

The main goal of the GDPR is that of shedding a light on the characters of privacy and data protection, as well as of their corollaries, within the context of Union digital policies. Rather than just providing for a long and extensive set of compliance-based duties and obligations, the GDPR points at the contents and purposes of the fundamental rights it enshrines and, subsequently, adopts accountability as a model to guarantee such principles. In this context, profiling, since it is coupled with higher levels of risk with respect to those fundamental rights, requires extra attention and the adoption of additional mitigation measures.

The DSA provides for a framework where the necessary balancing between the various interests at stake is shared between the government and the governed. The role and discretion of intermediaries is subsidiary and is scaled depending on the category they have been assigned to in the first place: as a consequence, the principle of accountability, rather than being "monolithic" and equally relevant to all targets of regulation, takes the form of a spectrum. Profiling, nonetheless, is given special consideration, especially with respect to those players who are at the end of the accountability spectrum. Pursuant to the DSA, VLOPs should be aware of the higher privacy and data protection concerns which accompany the deployment of such tools and have, therefore, to take additional care to ensure satisfactory remedies and mitigation instruments. Besides, the shift towards a top-down approach to risk-based regulation within Union digital policies is even more evident within the 2021 proposal for an Artificial Intelligence Act (AI Act),[60] which establishes directly four categories of risk connected to AI systems and provides a different regime for each of them.

At first glance, the development of such diverse approaches might appear worrisome. The apparently magmatic and chaotic character of the resulting legal framework, as a whole, may appear inconsistent both with fundamental values such as the rule of law and legal certainty. This could, on the one hand, have a direct impact on the efficacy of digital human rights policies and, at the same time, freeze important economic actors, such as online platforms, thus damaging the entire Digital Single Market Strategy. The existence of such a wide array of legislative sources, all setting additional and new, and seemingly inconsistent and incoherent, duties, could be looked upon 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.

However, at a closer look, the picture may become less chaotic and unstructured than expected. Although they are different as to the means employed, these instruments share a common project and a common direction, in that they all represent a tile of the new phase of European digital constitutionalism.[61] This is particularly evident if one considers the policies adopted with respect to profiling activities, where risk is, ultimately, the tool used by the Union to govern such a phenomenon. The notion of risk represents a proxy for a balancing operation between the various interests at stake.[62] The resulting framework is thus much less chaotic than what it may seem at first glance. Both within the DSA and the GDPR, profiling is allowed as a fundamental component of the developing Digital Single Market, but risk is chosen as a key instrument to establish how

[60] 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 (COM/2021/206 final).
[61] De Gregorio, supra, note 19.
[62] Cf. Gellert, 'Understanding the notion of risk in the General Data Protection Regulation', supra, note 14.

to deploy such kinds of processing without impairing excessively the constitutional values of the Union. The concerns with respect to the employment of such techniques are, by the way, also confirmed by the AI Act proposal, which explicitly prohibits those AI systems which, either through "subliminal techniques" or by exploiting "any of the vulnerabilities of a specific group of persons based on their age, physical or mental disability", "materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm".[63] Risk is, in other words, directly proportional to the degree of accountability of an actor employing profiling systems.

Besides, the rationale behind the different approaches to risk regulation, and therefore to the balancing of the fundamental values of the Union, are, to a certain extent, fully comprehensible in light of the different perspectives from which each of them addresses the matter of fundamental rights protection. As mentioned above, the GDPR focuses specifically on the right to privacy and data protection, which is extensively defined at the outset in its contents and declinations (e.g. lawfulness of processing;[64] transparency;[65] right to information;[66] right of access by data subject;[67] right to rectification;[68] right to be forgotten;[69] portability;[70] etc.). Fundamental rights are the starting point of the entire Regulation. The bottom-up approach is, therefore, the result of a regulatory structure focusing first and foremost on defining the nature and content of the rights at stake. A different perspective is the one taken by the DSA, which approaches the topic of fundamental rights only indirectly, and focuses rather upon the actors which are to be involved in the balancing and protection of users' fundamental rights. The AI Act itself considers a third different perspective, in that its purpose is to regulate directly not a specific fundamental right, nor the conduct of the actors playing in the Digital Single Market, but, rather, directly the technical tools which may be employed by them.

If one takes such a perspective, the resulting framework, far from being chaotic or magmatic, proves in fact to be coherent and consistent in creating a unitary regulation of profiling systems, and of digital technologies more in general, by choosing risk as the main governance tool and parameter.

V. 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. In the last few years, especially since the second half of the 2010s, risk has become increasingly central to the digital policies of the Union.

Both the GDPR and the DSA show how risk has ultimately been adopted as a technique to balance the various interests at stake and to create a legal framework free of burdensome over-regulation while at the same time safeguarding and protecting individuals' fundamental rights,

[63] AI Act, supra, note 60.
[64] GDPR, supra, note 20, Artt. 6 ff.
[65] Ibid, Art. 12.
[66] Ibid, Artt. 13-14.
[67] Ibid, Art. 15.
[68] Ibid, Art. 16.
[69] Ibid, Art. 17.
[70] Ibid, Art. 20.

including the rights to privacy, data protection, human dignity and non-discrimination. This is particularly evident with respect to the regulation of profiling activities which, although being generally allowed, require additional risk-mitigation measures because of the inherent threat they represent to users and consumers. The ultimate role of risk as a balancing technique allows to draw a connection between such provisions and the contents of traditional rights-based regulation. The European constitutional experience is characterised by the strive to strike an equal, and proportionate, balance between the various interests embodied by the Union. In this sense, the *fil rouge* at the heart of the various declinations of profiling regulation in Union policies is precisely the goal of contributing to creating a digital environment which embraces the constitutional values and principles enshrined by the Charter of Fundamental Rights. This reflection, moreover, may well be applicable to a range of other aspects and matters confronted by and regulated by the described Union legislative instruments.

The lens of digital constitutionalism can thus represent a tool for connecting the dots and make sense of the Union's current digital strategy. Although the concept of risk, and the consequent role of accountability, may be variously declined, such lenses can give us a key to fully understand the developments of the Union's digital policies, with respect especially (but not only) to privacy rights.