The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies

Pietro Dunn [1,2] and Giovanni De Gregorio [3]

[1] *Alma Mater Studiorum – Università di Bologna, Via Zamboni 27/29, Bologna, 40126, Italy*
[2] *University of Luxembourg, 4 Rue Alphonse Weicker, Luxembourg, L-2721, Luxembourg*
[3] *Centre for Socio-Legal Studies, University of Oxford, Manor Road, Oxford, OX1 3UQ, United Kingdom*

Abstract

The AI Act regulation proposal adopts a risk-based approach to the regulation of artificial intelligence systems. As a matter of fact, the risk-based approach has become more typical of Union strategies with respect to digital policies. However, the way such an approach has been declined varies greatly: most notably, whereas the GDPR and, to a limited extent, the DSA regulation proposal adopt a bottom-up perspective, the AI Act rather reflects a top-down scheme, where the task of risk assessment is kept within the hands of the legislator. This position paper aims at highlighting the common features, as well as the differences, between the various legal acts discussed: in particular, by considering (optimal) proportionality and due diligence as a characterizing features of the risk-based approach, the goal is to understand whether the AI Act does indeed reflect the typical principles of this developing legal model. Although noting that the role of due diligence is feebler within the regulation proposal, we argue that the central common point is represented by the (constitutionally relevant) goal of proportionality.

Keywords

Risk-Based Regulation, Artificial Intelligence Act, Proportionality

1. Introduction

The advancement of progress and technology always represents a challenge for regulators, who are called upon to strike a fair balance between the need to foster innovation and the often conflicting need to reduce the risk for collateral effects on individuals' lives and fundamental rights and freedoms. Such a tension between progress and risk is also typical of digital technologies [1]: indeed, in the last few years, the Union has had to face the complex task of designing the appropriate regulatory strategy for the development of a digital single market competitive in the international landscape but respectful, at the same time, of human rights and democratic principles.[1] This task has become increasingly important *vis-à-vis* the rise of artificial intelligence and of the algorithmic society [2].

In its 2021 Communication on fostering a European approach to artificial intelligence,[2] accompanying the presentation of its proposal for an Artificial Intelligence Act (AI Act),[3] the Commission underscored the manifold potential benefits of AI: throughout the COVID-19 pandemic, for instance, AI was used to predict the geographical spread of the virus, as well as for diagnostic purposes and for developing new vaccines and drugs against it. However, algorithms and AI can also carry risks. A flaw in the design or in the training of AI, in some instances, could lead for example to personal injuries or physical damages when those systems are used as safety components of a product.

IAIL 2022 – Imagining the AI Landscape after the AI Act, June 13, 2022, Amsterdam, Netherlands.
EMAIL: pietro.dunn2@unibo.it (P. Dunn); giovanni.degregorio@csls.ox.ac.uk (G. De Gregorio).
ORCID: 0000-0002-0248-7049 (P. Dunn); 0000-0001-7236-6149 (G. De Gregorio).

[1] Cf. Commission's Communication on a Digital Single Market Strategy for Europe, COM(2015)192 final.
[2] COM(2021)205 final.
[3] COM(2021)206 final, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts".

Moreover, when used for automated decision-making, algorithms can influence and sometimes affect individuals' exercise of fundamental rights [3]. AI systems are particularly problematic since, in most cases, they lack transparency [4]: this is worrying, for instance, *vis-à-vis* the risk of incorrect, biased and discriminatory results [5–8].

To face the challenges raised by technological progress, Western countries have resorted more and more to regulatory models based on the concept of risk [9], to be intended, technically, as a combination between the probability of a defined hazard occurring and the magnitude of the consequences that hazard may entail [10]. Risk is thus used as a proxy for decision-making. Through the practices of risk analysis [11, 12], it is indeed possible to forecast, on a probabilistic logic, the future developments of a specific conduct or activity: based on this, the necessary mitigation strategies and tools may be identified.

All in all, risk-based regulation represents an attempt to face the new challenges of innovation through a rational and technocratic approach that fosters more efficient, objective, and fair governance, whilst fighting against "over-regulation, legalistic and prescriptive rules, and the high costs of regulation" [13]. In particular, it uses risk as a tool to prioritize and target enforcement action in a manner that is proportionate to an actual hazard: regulation is thus calibrated to the actual needs of society *vis-à-vis* the risks connected to a product, service or activity [14].

The resort to risk-based regulation to face the new digital age is particularly evident when considering at least three fields: that of private and data protection; that of content moderation; and, finally, that of AI. As described elsewhere, indeed, the General Data Protection Regulation (GDPR)[4], as well as the proposal for a Digital Services Act (DSA)[5] and the AI Act all adopt forms of risk-based approaches, although the perspective they take seems to shift progressively from a bottom-up to a top-down model. Because of such a different approach, doubts may arise with respect to the consistency of the legal framework about digital technologies. In particular, as has been already done by some researchers [15], the question which may be posed is whether the AI Act actually entails a risk-based approach. The argument of the present position paper is that the link between the AI Act and previous legislative measure is based on the principle of (optimal) proportionality among conflicting constitutional interests: in this sense, risk-based regulation represents a declination of the developing digital constitutionalism in Europe [16].

Section 2 analyses the relationship of the risk-based regulatory model with the principles of proportionality and due diligence. Section 3 compares the GDPR, the DSA, and the AI Act to outline the progressive shift from a bottom-up to a top-down perspective. Section 4 draws highlights what the roles of proportionality and due diligence are in the AI Act. Finally, Section 6 draws some conclusions.

2. Risk, "optimal" proportionality, and due diligence

Risk-based regulation is characterized by some typical features differentiating it from more traditional models of law. The present subsection focuses on two aspects which appear to be fundamental in the context of contemporary Union risk-based policies: the pursuit of an "optimal" balance of interests and the reliance on due diligence.

First of all, as mentioned above, the characteristic goal of the risk-based approach is that of creating a framework where legal obligations are tailored to the specific risks entailed by a particular activity or service, with a view to avoiding the overburdening of the regulated actors. The scheme of the risk-based approach differs from that of traditional "command-and-control" mechanisms, where the state, as the entity endowed with legal authority, sets the rules on a top-down basis to impose certain duties and obligations applicable indiscriminately to all natural and legal persons subject to its jurisdiction [11]. In fact, risk-based regulation inherently seeks to operate a "discrimination" between the subjects of law, thus differentiating the legal regime governing them based, precisely, on the proxy of risk.

[4] 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.

[5] COM(2020)825 final, "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".

In this sense, risk-based regulation aims at pursuing goals similar to what Adrian Vermeule has defined as "optimizing constitutionalism", or the "mature position" to (constitutional) risk regulation [17]. Vermeule, in fact, operates a distinction between "precautionary constitutionalism" and "optimizing constitutionalism":[6] whereas the former, in synthesis, implies that "new instruments, technologies, and policies should be rejected unless and until they can be shown to be safe", the latter, instead of seeking "maximal" precautions", aims to introduce "optimal precautions" in terms of costs and benefits. In other words, whereas the concern of precautionary constitutionalism is to prevent *in toto* the potential consequences of a risk, optimizing constitutionalism takes a more consequentialist view on the regulation of risk, and, taking into account the potential downsides and collateral effects of a "no-risk" policy, seeks to balance the need to contain risk and the need to avoid over-regulation. In this sense, the EU risk-based approach to digital technologies is somehow consistent with the notion of "optimizing constitutionalism", since its aim is to reduce the potential harms such technologies may entail for individuals and society, while at the same time ensuring the development of industry and the market.

Besides, within risk-based regulation, such a balancing operation is to some extent left directly to the discretion of the "regulatee", who retains some leeway as to the identification of the measures to be implemented to reduce and mitigate the risk of harms. As will be underscored below, this is especially true for the GDPR and, in part, for the DSA, whereas such a margin of discretion is much more limited within the AI Act.

Be it as it may, the reliance on the targets of regulation for the purpose of identifying the exact content of the measures to be put into place inherently implies the need for such actors to operate with due diligence. This should not come as a surprise: indeed, in the field of international law, the notion of "due diligence" has come to play an increasingly central role with respect to the duty of states to manage risks (for the environment, for economy, for human rights, etc.) within their jurisdictions. As highlighted by Peters, Krieger, and Kreuzer, "due diligence is needed when a risk has to be controlled or contained, in order to prevent harm and damage done to another actor or to a public interest"; indeed, "the rise of the concept [of due diligence] is […] tied to the rise of the 'risk society' and the idea of risk management" [18]. Risk-based regulation thus transposes the principle of due diligence from the framework of international law, and thus from the relations between states, to the framework of national law, translating it into a fundamental rule governing the behaviour of natural or legal persons acting within the state.

3. The spectrum of the risk-based approach in EU digital policies

The risk-based approach towards digital policies has been developed through the last decade by EU law [19]. Since the launch of the Digital Single Market Strategy, 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 European 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 declined 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, the principle of accountability is the result of a legislative strategy aiming to greatly reduce the imposition of duties coming from "above". Quite to the opposite, the proposed Artificial 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. Finally, in the field of online content, the Digital Services Act (DSA) aims at creating a hybrid system, which mixes the

[6] In its analysis, Vermeule focuses on "political risks". Nonetheless, such a distinction may ultimately applied to all types of risk.

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

The present section thus briefly describes the shift from a bottom-up perspective, characteristic of the GDPR, to the top-down one, typical of the AI Act.

3.1. The risk-based approach in the GDPR and DSA

The bottom-up perspective of the GDPR emerges from the fact that data controllers are entrusted themselves with the duty to ensure that the processing of personal data is aligned with the general principles of the Regulation. In fact, data controllers must operate a risk assessment with respect to the activities they conduct and develop the appropriate response to reduce any collateral effects affecting individuals' rights to privacy and data protection. It is from these duties that the concept of accountability arises, meaning that data controllers are held responsible for the decisions they make to minimize and mitigate damages: "the data holder […] is accountable for ensuring compliance with the principles (and rights of the data subject)" [20].

Accountability thus takes a dynamic form, since it varies depending 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. In other words, the risk-based approach of the GDPR is inherently grounded upon a form of "responsibilisation of the regulatee" [10] which translates, in turn, into the notion of accountability. It also translates into a model of "compliance 2.0", where the regulatee is not required to simply engage in a form of compliance consisting of "ticking boxes" but has to tailor the measures adopted to the situation at hand, with a view to respecting the rights and freedoms of data subjects [14]. In other words, the binary logic of compliance/non-compliance, typical of the traditional rights-based approach of the European Union [10, 21], is overcome by the scalable logic of risk analysis. As a result, obligations may be "uneven" depending on the actors who are called to comply with the GDPR, but this different outcome is justified by the existence of a preliminary balancing test operated directly by data controllers.

This last aspect, which is precisely what characterizes the GDPR as a bottom-up risk-based regulation, emerges from a range of different provisions. For instance, apart from the provisions regulating in general the responsibility of data controllers[7] and introducing the principle of data protection by design and by the default[8] [10, 13], the Regulation foresees a mandatory 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.[9]

Whereas the GDPR adopted a risk-based approach for the regulation of personal data in the EU, the DSA proposal features, with specific respect to content moderation practices, a "supervised risk management approach".[10] Indeed, presented together with the Digital Markets Act (DMA) in December 2020, the DSA aims *inter alia* at updating the intermediary liability regime established in 2000 by the e-Commerce Directive (ECD).[11] Though maintaining substantially unaltered the "safe harbor" approach developed by the ECD and inherited from the US [22–24], the Regulation proposal envisages a broad array of new duties and obligations for providers of intermediary services, with a view to guaranteeing a transparent and safe online environment [25]. These duties and obligations, moreover, reveal the peculiar traits of the DSA's risk-based approach. In fact, said obligations are not applicable to all providers of intermediary services indiscriminately, but follow a pyramidal structure, based on which they are divided into four tiers. Indeeed, on the basis of specific criteria concerning their dimension and the services they provide, providers are assigned to risk categories variously disciplined.[12]

[7] Art. 24 GDPR.
[8] Art. 25 GDPR.
[9] Art. 35 GDPR.
[10] Explanatory memorandum to the DSA proposal, p. 1.
[11] 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'), O.J. 2020 L 178/1.
[12] A small group of provisions thus applies to all providers of intermediary services, whereas the subsequent Articles have an increasingly narrow scope of application: hosting providers; online platforms; and "very large online platforms" (VLOPs). The obligations set by the DSA mainly move in two directions: first, that of fostering transparency concerning content moderation practices; second, that of making intermediaries, notably hosting providers and online platforms, more responsible for the content they host and contribute to disseminating. In

Therefore, as in the GDPR, the measures to be adopted by providers to face the risks arising from the services they offer are not horizontally equal but are directly calibrated based on varying risk assessment strategies. However, the DSA moves away from the pure bottom-up structure adopted by the GDPR, since decisions concerning the measures to adopt are not left entirely to the discretion of the targets of regulation. Indeed, the four categories for online intermediaries are established directly by the Regulation proposal and are disciplined in a progressively more severe manner depending on a preliminary top-down risk assessment [26]. The "responsibilisation of the regulatee" is thus more feeble in the DSA if compared to the GDPR.

Besides, a certain margin of discretion is still left to the appreciation of the targets of regulation. In particular, in the case of very large online platforms (VLOPs), a significantly important duty is represented by the need to assess any significant risks entailed by their activities (including those concerning the dissemination of unlawful or harmful content and those potentially affecting the fundamental rights and freedoms of individuals) and to put in place the appropriate mitigation measures.[13] Such a provision shows how the gap between the DSA and the GDPR is only partial. Also, the establishment of an internal complaint-handling mechanism,[14] applicable to all online platforms, is another key example showing that these actors still retain a central role in defining which content items may or may not represent an unlawful or harmful content. All in all, the approach followed by the DSA, rather than being strictly top-down, seems to be hybrid. As such, both the GDPR and the DSA must necessarily rely, to a certain degree, on the due diligence of the targets of regulation: failure to develop mitigation strategies in a diligent manner will, inevitably, entail liability.

Moreover, both the GDPR and the DSA ultimately aim to establish an optimal balance between the goal of preventing harms deriving from digital technologies and the goal of guaranteeing an environment where the digital single market can fully flourish. Indeed, both acts incentivise the imposition of duties and obligations that are as much tailored as possible to the single specific cases. The GDPR's choice of delegating to data controllers and processors the decisions concerning the measures to be implemented, as well as the DSA's choice of creating an asymmetric legal regime for providers of intermediary services, are ultimately aimed at fostering a proportionate and optimal framework for actors in the digital market [17, 19]

3.2. The risk-based approach in the Artificial Intelligence Act

Within the AI Act, the trajectory from a bottom-up to a top-down perspective is seemingly complete. In fact, notwithstanding the explicit statement of the Commission, according to which the AI Act is fundamentally based upon a risk-based approach, some commentators have raised serious doubts concerning the possibility of actually recognising it as such [15].

The Commission's intentions to adopt a balanced risk-based approach to the regulation of artificial intelligence already emerged within the 2020 White Paper on Artificial Intelligence.[15] The document highlighted the role that AI should play in the improvement of many aspects of our society, including healthcare, the mitigation of climate change, and efficiency in production. At the same time, it stressed the potential collateral impact of artificial intelligence systems on people's physical integrity as well as on their individual rights and liberties. According to the Union's strategy towards AI, the ultimate goal must be that of building an ecosystem of trust [27] and excellence as a means to strike the correct balance between risk and innovation.[16]

The AI Act proposal aims to build precisely that ecosystem of trust and excellence, thus representing a new critical step in the developing digital strategy of the Union. As is well known, the text of the proposal is structured upon four levels of risk, associated with certain AI systems and their use [28]. This structure recalls, to a certain extent, that of the DSA: however, the AI Act leaves very little, if any, discretion to users and providers of AI. Rather than entrusting them with the task of assessing risks and

particular, all providers of hosting services will need to put in place a "notice and action" procedure: individuals or entities shall thus have the opportunity of flagging the presence of unlawful content, following which intermediaries will have to act expeditiously in order to avoid subsidiary liability for third-party content (Art. 14 DSA).

[13] Artt. 26-27 DSA.

[14] Art. 17 DSA.

[15] COM/2020/65 final, "White Paper on Artificial Intelligence – A European approach to excellence and trust".

[16] ibid., at 3.

developing the appropriate risk mitigation strategies, the choice of the AI Act is to set from above the rules of the game which must be complied with.

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 legislator 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). Within the AI Act, conversely, it is the legislator (together with the Commission) that is vested with the task of assessing risk: the leeway granted to providers and users is, in fact, minimal.

First, the AI Act proposal prohibits some practices involving systems which are deemed to be "unacceptable" and thus prohibited because considered *a priori* too dangerous[17] (these include applications that manipulate human behaviour to circumvent the free will of users; personal credit-based rating systems managed by governments; real-time biometric recognition systems in publicly accessible spaces for the purposes of law enforcement).

Second, the Commission identifies a "high-risk" threshold for AI systems,[18] most of which are identified by the list which is contained within Annex III and can be amended by the Commission based on a range of set criteria.[19] High-risk AI systems shall have to comply with a long and extensive series of requirements. Most interestingly, they seem to represent the only class where the legislator gives some leeway to the targets of regulation. Indeed, 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.[20] Additionally, providers of high-risk AI systems are required to put in place a quality management system to ensure compliance with the entire Regulation.[21] Nonetheless, it must be stressed that the actual margin of discretion for providers and users of high risk systems is still very residual.

Third, some AI applications are included in a category characterized by "limited risks" (systems intended to interact with natural persons; emotion recognition or biometric categorization systems; systems capable of generating "deep fake" contents).[22] Providers and users of such tools shall comply with specific transparency requirements. Finally, a residual category of "minimal risk" is associated with AI applications that do not have the same invasiveness as those described above: since it is constructed as a residual category, it embraces an ample set of AI applications and systems. Minimal risk AI applications are not subject to any specific duty or obligation, although the Commission and Member States should encourage and facilitate the drawing up of codes of conduct intended to foster on their part the voluntary application of the requirements set for high-risk systems.[23]

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. The categories of risk are defined directly by the EU 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 stiff 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 EU 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.

[17] Art. 5 AI Act.
[18] ibid., Art. 6.
[19] ibid., Art. 7.
[20] ibid., Art. 9.
[21] ibid., Art. 17.
[22] ibid., Art. 52.
[23] ibid., Art. 69.

4. (Optimal) proportionality and due diligence in the AI Act

Having outlined the peculiar perspective adopted by the AI Act with respect to the regulation of the risks posed by AI systems, it is important to focus on the role played by the features of proportionality and due diligence within the system created by the Regulation proposal, so as to understand what the link is between the AI Act and previous risk-based regulatory models devised by the Union with respect to matters concerning the digital field.

The goal of (optimal) proportionality within the AI Act emerges explicitly from the Explanatory Memorandum, where the European Commission stated that the proposal "puts in place a proportionate regulatory system centred on a well-defined risk-based regulatory approach that does not create unnecessary restrictions to trade", also adding that "legal intervention is tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future".[24]

These statements, focusing especially on the centrality of proportionality between regulation and risk, seem to resonate with the GDPR and the DSA. It is true, as a matter of fact, that the choice of resorting to a top-down structure makes the law much more rigid: if compared with the GDPR, the AI Act does not allow much space to tailor the measures to the specific risks. Nevertheless, the spirit of the law, as confirmed by the words of the Commission, is still that of implementing a legal framework where proportionality is the ultimate goal to be attained. Although the system is more rigid, nonetheless the envisioning of a differentiated regulatory regime based on risk represents the core essence of the principle of proportionality characterizing the digital policies of the European Union.

Of course, the adoption of a more rigid scheme directly affects the principle of accountability which, within the system developed by the GDPR, is directly related to the freedom given to data controllers and processors with respect to the measures to adopt to protect data subjects' rights to privacy and data protection. 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 [10, 19]. In the AI Act, what changes, at a deeper level, is thus the relationship between regulator and regulatee: whereas in the GDPR, the latter was delegated with the duty of assessing risk by the former, and was thus responsible for such a duty, this delegation is almost absent within the AI Act.

As a result, also the principle of due diligence is much less present within the AI Act than within the GDPR and the DSA. Because they are given less choice as to the means adopted to comply with the law, the principle of due diligence mainly applies at the level of the implementation of the necessary measures, and not so much at the level of their designation. A few provisions, as mentioned above, give leeway for a minor customization in the choice of the mitigation system to adopt: however, such a liberty is quite reduced.

Table 1

The bottom-up, hybrid, and top-down approaches to risk-based regulation

Bottom-up (GDPR)	Hybrid (DSA)	Top-down (AI Act)
Risk assessment made by the targets of regulation	Risk assessment shared between the law maker and the targets of regulation	Risk assessment made by the law maker
Wide margin of discretion	Moderate margin of discretion	Limited margin of discretion
Goal: optimal balancing (proportionality)	Goal: optimal balancing (proportionality)	Goal: optimal balancing (proportionality)

[24] Explanatory memorandum to the AI Act proposal, at 3.

5. 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.

Ultimately, the *fil rouge* connecting the AI Act with the GDPR and the DSA, and with the risk-based approach in general, is the goal of developing a legal framework for digital technologies that promotes an "optimal" balancing between the interests involved. If the European constitutional experience, is characterized by the strive to strike an equal, and proportionate, balance between the various interests of social parties, the common feature at the heart of the GDPR, DSA, and AI Act is precisely their aspiration to create a digital environment which embraces European constitutional values and principles.

Although due diligence still represents an important aspect of the AI Act, it appears that proportionality is, ultimately, the common and central aspect unifying the strategies of the EU in such a field. To this extent, the risk-based approach ultimately represents an instrument to develop a constitutionally sound environment. It is one of the expression of European digital constitutionalism [29], where the interests of the market and the protection of societal, democratic, and fundamental rights interests, must be equally protected.

6. References

[1] D. Lupton, Digital risk society, in: A. Burgess, A. Alemanno, J.O. Zinn (Eds.), Routledge Handbook of Risk Studies, Routledge, London, 2016, pp. 301–309.

[2] J.M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, U.C.D. L. Rev. 51 (2018) 1149–1210.

[3] European Union Agency for Fundamental Rights (FRA), Getting the Future Right. Artificial Intelligence and Fundamental Rights, Publications Office of the European Union, Luxembourg, 2020.

[4] J. Burrell, How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data & Society 3 (2016). doi:10.1177/2053951715622512.

[5] S.U. Noble, Algorithms of oppression: how search engines reinforce racism, New York University Press, New York, NY, 2018.

[6] F. Pasquale, New laws of robotics: defending human expertise in the age of AI, The Belknap Press of Harvard University Press, Cambridge, MA, 2020.

[7] European Commission, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law, Publications Office of the European Union, Luxembourg, 2021.

[8] S. Wachter, B. Mittelstadt, C. Russell, Bias Preservation in Machine Learning: The Legality of Fairness Metrics under EU Non-Discrimination Law, W. Va. L. Rev. 123 (2020) 735–790.

[9] J. van der Heijden, Risk as an Approach to Regulatory Governance: An Evidence Synthesis and Research Agenda, SAGE Open 11 (2021). doi:10.1177/21582440211032202.

[10] R. Gellert, The Risk-Based Approach to Data Protection, Oxford University Press, Oxford, 2020.

[11] B.M. Hutter, Risk, Regulation, and Management, in: P. Taylor-Gooby, J.O. and Zinn (Eds.), Risk in Social Science, Oxford University Press, Oxford, 2006, pp. 202–227.

[12] A. Alemanno, Regulating the European Risk Society, in: A. Alemanno, F. den Butter, A. Nijsen, J. Torriti (Eds.), Better Business Regulation in a Risk Society, Springer, New York, NY, 2013, pp. 37–56. doi:10.1007/978-1-4614-4406-0_3.

[13] M. Macenaite, The "Riskification" of European Data Protection Law through a two-fold Shift, European Journal of Risk Regulation 8 (2017) 506–540. doi:10.1017/err.2017.40.

[14] C. Quelle, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach, European Journal of Risk Regulation 9 (2018) 502–526. https://doi.org/10.1017/err.2018.47.

[15] L. Edwards, Regulating AI in Europe: four problems and four solutions, Ada Lovelace Institute, 2022. URL: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf.
[16] G. De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, Cambridge University Press, Cambridge, 2022.
[17] A. Vermeule, The Constitution of Risk, Cambridge University Press, Cambridge, 2013.
[18] A. Peters, H. Krieger, L. Kreuzer, Due Diligence in the International Legal Order: Dissecting the Leitmotif of Current Accountability Debates, in: H. Krieger, A. Peters, L. Kreuzer (Eds.), Due Diligence in the International Legal Order, Oxford University Press, Oxford, 2020, pp. 1-19. doi: 10.1093/oso/9780198869900.003.0001.
[19] G. De Gregorio, P. Dunn, The European risk-based approaches: Connecting constitutional dots in the digital age, CMLR 59 (2022) 473–500.
[20] C. Castets-Renard, Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making, Fordham Intellectual Property, Media and Entertainment Law Journal 30 (2019) 91-137.
[21] O. Lynskey, The Foundations of EU Data Protection Law, Oxford University Press, Oxford, 2015.
[22] L. Edwards, Articles 12-15 ECD: ISP liability. The problem of intermediary service provider liability, in: L. Edwards (Ed.), The new legal framework for e-commerce in Europe, Hart, Oxford, 2005, pp. 93–136.
[23] G.N. Yannopoulos, The Immunity of Internet Intermediaries Reconsidered?, in: M. Taddeo, L. Floridi (Eds.), The Responsibilities of Online Service Providers, Springer, Cham, 2017, pp. 43–59. doi:10.1007/978-3-319-47852-4_3.
[24] D. Citron, B. Wittes, The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity, Fordham Law Review 86 (2017) 401-424.
[25] C. Cauffman, C. Goanta, A New Order: The Digital Services Act and Consumer Protection, European Journal of Risk Regulation 12 (2021) 758–774. doi:10.1017/err.2021.8.
[26] Z. Efroni, The Digital Services Act: risk-based regulation of online platforms, Internet Policy Review, 2021. URL: https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606.
[27] L. Floridi, Establishing the rules for building trustworthy AI, Nat Mach Intell. 1 (2019) 261–262. doi:10.1038/s42256-019-0055-y.
[28] M. Ebers, Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: L. Di Matteo, C. Poncibò, M. Cannarsa (Eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, Cambridge University Press, Cambridge (2022, forthcoming).
[29] G. De Gregorio, The rise of digital constitutionalism in the European Union, International Journal of Constitutional Law 19 (2021) 41–70. doi:10.1093/icon/moab001.