The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?

Raphaël Gellert

Radboud Business Law Institute , Interdisciplinary Hub for Digitalization and Society (iHub), Radboud University

This contribution is based upon a keynote speech of the same title, which was given at the Jon Bing Memorial Seminar 2021. I would like to thank the Norwegian Research Center for Computers and Law, and in particular Lee Bygrave for their kind invitation.

Abstract: In April 2021 the European Commission unveiled a proposal for a Regulation on Artificial Intelligence (AI), the so-called AI Act (AIA). The regulatory architecture of the proposed AIA is explicitly predicated upon a risk-based approach. This begs the question as to whether the risk-based approach in the proposed AIA is the same as the one featured in the EU's General Data Protection Regulation (GDPR), or whether there are differences. And in this case, which ones and how can they be framed? This contribution contrasts the two risk-based approaches by framing them as two different iterations of risk-based models of regulation. One concerned with better compliance (GDPR), and one concerned with the determination of which AI systems should be regulated (AIA). Framing things in terms of regulation models allows to shift the focus upon key components of risk-based models of regulation. Namely, the concept of risk at stake, and the type of obligations for regulatees. In both cases, there seem to be some sharp contrasts at first sight. Upon better look however, these are not as acute as it first seemed. The contribution ends by reflecting upon the proposed AIA's limited scope (i.e., limited to high risk AI systems). Can the recourse to regulatory theory help shed some light on this issue and be instrumental in devising more encompassing and protective alternatives?

Keywords: risk-based approach, GDPR, proposed AI Act, risk, regulation theory

Introduction

In recent years the EU's General Data Protection Regulation (GDPR) has imposed itself as one of the most important instruments for the regulation of information and communication technology (or digital technology)[1]. It features a so-called risk-based approach, which has been framed as a scalable approach to compliance with existing data protection obligations and requirements (see, Art. 29 WP 2014, 2).

In April 2021, the European Commission unveiled a proposal for a Regulation on Artificial Intelligence (AI), the so-called AI Act (AIA)[2]. The goal of this proposed Regulation is to regulate artificial intelligence technology (what it refers to 'AI systems')[3]. Given the increasing importance of AI, it can be seen as the next most important EU instrument for digital technology regulation. Just like the GDPR, the AIA is also underpinned by a risk-based approach. The Explanatory memorandum of the proposal refers to this risk-based approach as a regulatory approach that tailors legal intervention to 'those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future' (European Commission 2021, 3).

The proposed AIA is indeed predicated upon a three-pronged system. The latter distinguishes between prohibited AI systems[4], high-risk AI systems[5], and AI system that interact with natural persons (for which a number of transparency requirements apply)[6]. It would therefore appear that the risk-based approach of the proposed AIA is a regulatory mechanism that focuses on high-risk scenarios (hence this paper's focus on high risk AI systems)[7], and consists in determining which AI systems should be regulated, and which AI systems shouldn't (European Commission 2021, 3).

Building upon this initial distinction, the present contribution goes on to analyse both risk-based approaches as pertaining to different types of risk-

[1] Regulation 2016/679/EU 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 [2016] OJ L119/1. For an overview of the successes and points of improvement of the GDPR, see (European Commission 2020).

[2] European Commission, 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 Act (2021) 167, 84, 85 final.

[3] See, (European Commission 2021, 3), where the European Commission refers to the proposal as a 'horizontal regulatory approach to AI'.

[4] Proposed AIA, Title II.

[5] Proposed AIA, Title III.

[6] See, proposed AIA, art. 52(1), (European Commission 2021, 7).

[7] Leaving aside AI systems that are safety components of products or products themselves. See, proposed AIA, art. 6(1).

based regulation models. In the first case (GDPR), the point is to use risk and risk management tools as a means to better comply. In the second (proposed AIA), the point is to determine which AI systems should be regulated.

It then goes on to analyse two key elements of risk-based regulation models: the concept of risk at stake and the obligations for the duty bearers (regulatees). In both cases, there seems to be some sharp contrasts at first sight. Upon better look however, these are not as acute as it first seemed.

The contribution ends by reflecting upon the proposed AIA's limited scope (i.e., limited to high risk AI systems). Can the recourse to regulatory theory help shed some light on this issue and be instrumental in devising more encompassing and protective alternatives?

Different regulatory models

The first way in which the two risk-based approaches can be contrasted is by paying attention to the regulatory models they embody, since both risk-based approaches can indeed be understood as pertaining to a model of regulation[8].

Although a contested concept, regulation has been classically defined as 'the sustained and focused control (…) over activities that are generally regarded as desirable for society' (Selznick 1985, 363–64). In other words, the point of regulation is to influence -through governmental action but also beyond- the behaviour of social actors in order to achieve beneficial goals for society (or conversely to avoid harmful activities) (see, Morgan and Yeung 2007, 16–17)[9].

In this case a risk-based model of regulation is at stake. However, as Black warns, the concept of risk-based regulation encompasses various types of regulation models that are not identical (Black 2010a, 187). One type of risk-based regulation addresses risks to society such as in the field of health, safety, or the environment. It is risk-based because risk is used as way to determine whether certain activities should be regulated and how (Black 2010a, 187). This type of risk-based regulation echoes what the proposed AIA is about. Another type of risk-based regulation has been used in the financial sector. Organisations use risk management instruments in order to determine whether they have set enough capital aside (Black 2010a, 187), and in so-doing one might add, whether they are compliant with the regulatory

[8] See the relevant references in each sub-section.

[9] Of course, law is a primary vehicle for regulation, but far from the only one. On the links and overlaps between law and regulation, see (Black 2002).

framework. This type of risk-based regulation evokes more what the risk-based approach to the GDPR is about[10].

AIA model of regulation

The risk-based approach in the AIA can be described as pertaining to what has been qualified as risk regulation (see, Demortain 2011, 6).

Whereas the traditional notion of regulation (otherwise known as command and control) has been linked to the avoidance of broadly defined harms stemming from all sorts of activities (see, e.g., Yeung 2004, 258), one can distinguish a specific iteration thereof known as risk regulation. The goal in this case is to address health (and safety) harms (Demortain 2011, 6). Whereas risk regulation can't be qualified as a sub-field of regulatory activity as such, it is usually prevalent in the areas of relevance for health and safety because of its reliance upon scientific expertise and scientific (i.e., quantitative) tools for risk analysis and risk management, which are characteristic of risk regulation (see, Demortain 2011, 1). The point of risk regulation is therefore to determine what levels of health and safety risks are acceptable (see, Weimer 2019, 23). The emergence of risk regulation has been linked to the increasing role played by science and technology in our societies (see, Weimer 2019, 24). As the role of industrialisation, and hence of science and technology, becomes preponderant, many objects of regulatory intervention are framed as scientific risks, with a particular emphasis on health and safety (Weimer 2019, 24)[11]. This requires in turn regulatory responses that also make use of scientific and quantitative concepts of risk assessment and management (see, Black 2010b, 302). Furthermore, and given the importance of health and safety for well-functioning markets, one can argue that the EU internal market and the issue of risk regulation (with a focus on health and safety risks) have been both intertwined in a decades-long process of co-evolution (see, Weimer 2019, chap. 2, in particular pp. 50-62). In other words, risk regulation has become an inherent feature of the EU internal market[12].

[10] Black refers to a third meaning of risk-based regulation, which has to do with the way regulators prioritise their own actions. This issue falls beyond the scope of this contribution. See, (Black 2010a, 187–88).

[11] Not to mention that some authors have also argued that some issues are explicitly transformed into scientific risks in order to make them more easily regulated through risk regulation, (see, e.g., Borraz 2008).

[12] Which is why its legal basis is Article 114 of the Treaty on the functioning of the EU (TFEU) (Weimer 2019, 54). This is the same basis as that of the proposed AIA, except for certain rules concerning AI systems for so-called real-time remote biometric identification, which are based on TFEU, art. 16. See (European Commission 2021, 6).

Such a framing is consistent with the Proposed AIA's explicit kinship with the EU's new legislative framework for product legislation (European Commission 2021, 13), and the latter's concern for risks to health and safety. It is also consistent with its *modus operandi* and the very way the proposed Act itself defines the risk-based approach. Namely, 'a balanced and proportionate horizontal regulatory approach to AI' (European Commission 2021, 3) that tailors legal intervention to 'those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future' (European Commission 2021, 3). In other words, the point of the risk-based approach in the AIA is to determine thresholds of (high) risks above which AI systems are presenting a high risk to individuals' health, safety, and fundamental rights, and regulatory (or legislative) intervention is therefore required (European Commission 2021, 3). Such regulatory intervention is encapsulated in Title III of the proposed Act, which contains among others the horizontal requirements for AI (which the Explanatory memorandum refers to as 'principle-based requirements that AI systems should comply with'), as well as the prior authorisation system for being put on the market (i.e., the conformity assessment procedures) (European Commission 2021, 3).

In other words, the risk-based approach seems to be a way to determine when AI systems create high risks to individuals' health and safety and fundamental rights (European Commission 2021, 7). In which case, these systems will be subject to the horizontal 'principle-based requirements' (which include such things as requirements concerning the quality of data, documentation and traceability, human oversight, accuracy and robustness, etc.) and to the prior market authorisation system (European Commission 2021, 7).

The risk-based approach relies upon a centralised system since it is up to the European Commission to determine what constitutes a high risk and what does not.[13] Annex III of the proposed Regulation contains the AI systems that are considered high risk. These include, among others, systems for the management and operation of critical infrastructure (Annex III, art. 2); systems for education and vocational training (art. 3); systems for employment and workers management (art. 4). On top of that the European Commission can amend the high risk list of Annex III in case it considers that another -not yet considered- AI system poses a risk to harm and safety or fundamental rights, which is sufficiently high so as to be considered high risk and to be included in the Annex (proposed AIA, art. 7(1)(b)). Article 7(2) of the proposed Act specifies a number of parameters that should be taken

[13] See, proposed AIA, art. 6(2).

into consideration into the risk assessment leading to the classification of a system as being high risk.

The GDPR model of regulation

In contrast, one can argue that the risk-based approach to the GDPR does not espouse the logic of risk regulation. The risk-based approach is part of the GDPR (Art. 29 WP 2014), but is not officially defined therein (see, e.g., Quelle 2017, 34).

It has been argued that the risk-based approach to data protection partakes of a model of regulation known as meta regulation, itself part of a broader regulation model known as principles-based regulation (Gellert 2020, 20). Rather than a specific way of regulating activities (through tools stemming from risk analysis and management), these models of regulation can best be understood as a way to address some of the issues plaguing the traditional model of command and control regulation, and in particular those pertaining to rules (see, Gellert 2020, 19–20). In a nutshell, these models of regulation are known to be collaborative models of regulation. The point of which is to lead to better compliance with the GDPR's requirements by endowing duty bearers (or regulatees, in this case data controllers) with an increased responsibility -and hence discretion- for complying (see, Gellert 2020, 20; in a similar sense, see also Quelle 2017, 42–43). Data controllers become more responsible by resorting to risk management tools, which they precisely use to the ends of -better- complying with data protection mandates (Gellert 2020, 20–21; see also, Demetzou 2018, 143).[14] Such an analysis is confirmed by the now-defunct Article 29 Working Party (Art. 29 WP), which has stated that the risk-based approach to data protection is 'a scalable and proportionate approach to "compliance obligations"' (Art. 29 WP 2014, 2).

The heart of the risk-based approach can therefore be situated in the accountability principle (Article 24 GDPR, see Gellert 2020, 149; Demetzou 2018, 143)[15], which says that:

'Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'

[14] Using risk management tools also allows to find the purportedly best way to comply and as such can therefore entail a calibration of compliance measures, hence the discretion (see, Gellert 2020, 20–22).

[15] Contrast with Quelle, who also considers GDPR, art. 25 as core to the risk-based approach. See, (Quelle 2017).

This general provision concerning the use of risk management tools as a means to comply is completed by a number of risk-based obligations in chapter IV GDPR (see, Art. 29 WP 2014, 3). The latter entails that the regulatees use their risk management tools as a means to replace the former regulatory systems that existed in the now defunct data protection Directive (see, Gellert 2020, 164 et s.). A classic example is the data protection impact assessment (DPIA) obligation of Article 35 GDPR, which now replaces the former notification obligation (see, GDPR, Recital 89).

In other words, the point here is not to regulate specific harms to health and safety, which because of their nature require the use of risk analysis and management tools (hence resorting to risk regulation). Rather, the point is to use risk management tools as a way to address some of the shortcomings plaguing traditional models of regulation, and thus, to better comply with legal obligations and requirements. That is, to better comply with data protection law and thus, to uphold the fundamental right to personal data protection. This also entails that the scope of the risk-based approach to data protection is not concerned with substantive issues, namely what it is exactly that has to be complied with (i.e., the content of data protection requirements) (Gellert 2020, 157). The point is simply to better comply with the requirements and obligations (see, Demetzou 2018, 143; Quelle 2017, 35). This is also in sharp contrast with the risk-based approach in the proposed AIA since the latter's scope is concerned with substance. It does indeed determine what AI systems need to be regulated. So, contrary to the GDPR where the risk-based approach serves mainly to determine the intensity of compliance measures, the risk-based approach in the AIA has a much more substantive scope since it determines what gets regulated in the first place, with the risk that some AI systems are unduly categorised as non-high risk (more on that in the conclusion).

So, in spite of the key role of risk management and the risk-based moniker in both cases, one can see that these are two very distinctive regulatory logics and models at play. Nonetheless, the fact that we are confronted with two regulatory models underpinned by risks also allows to compare them on the account of the following factors. First, what are the type of obligations for the regulatees (regulation models)[16]. Second, what concept of risk is at play (regulatory models based upon risk)?

[16] Since regulation is at its heart about the control of actors' behaviour, see Black's seminal definition of regulation as the 'process involving the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly defined outcome or outcomes', (Black 2001, 142).

The concept of risk

As a reminder, a commonly accepted definition of risk is that of a combination of the probability or likelihood of an event (i.e., the risk) and the severity or magnitude of its consequences (i.e., the harms it leads to) (Warner 1992, 4).

At first sight the concept of risk in the GDPR and in the proposed AIA seem to be quite different. These differences can be traced back to the diverging underpinning regulatory models (i.e., concept of risk based on the logic of better complying with legal obligations *versus* concept of risk stemming from scientifically calculated risks to health and safety).

However, on closer inspection it might appear that the concepts of risk are not that diverging. This has probably to do with how the fact that even though the proposed AIA is predicated upon the logic of the EU New Legislative Framework and the risks to health and safety, it also looks at risks to fundamental rights, which lend themselves less easily to scientific risk calculations.

The GDPR risk

Even though the notion of risk is as such not defined in the GDPR (see, e.g., Demetzou 2019, 6), the GDPR does contain various indications as to how a risk should be measured. There is also additional guidance from the Art. 29 WP, and the high risk lists from the national supervisory authorities (SAs)[17].

When looking at these indications one can observe that the GDPR (and the additional guidance instruments) leave the issues of harms to the side. Rather, they focus on the event as such (i.e., the risk likely to happen), and more particularly they look at the properties of the processing (see, Demetzou 2019, 6), which they consider as proxies for such risk (see, Gellert 2020, 215–17). In other words, the properties of the processing are taken as an indication concerning the extent of the risk.

This is clearly the case in Article 35 GDPR. Article 35(1) GDPR refers to the 'nature, scope, context and purposes of the processing'. Article 35(3) GDPR refers for instance to the large scale processing of special categories of data (art. 35(3)(b)); the systematic monitoring of publicly accessible areas on a large scale (art. 35(3)(c)); or to certain forms of profiling (art. 35(3)(a)). This is also the case for the Art. 29 WP's guidelines on data protection impact assessments (DPIAs). The latter look among others at specific types of processing operations such as evaluation or scoring (e.g., creation of a credit

[17] See for instance, the list of the French data protection authority (CNIL 2018).

rating database) (Art. 29 WP 2017, 9, 11); or matching and/or combining of data sets (Art. 29 WP 2017, 10), just to name a few.

This does not mean to say that no attention whatsoever is dedicated to the harms incurred by the data subject. One can obviously point the fact that Article 35(3)(a) GDPR refers specifically to those profiling operations contemplated by Article 22 GDPR (namely those that have legal effects or that similarly significantly affect the data subject). Similarly, Recital 75 GDPR refers to vulnerable data subjects as well as to a series of harms (e.g., physical, material, non-material damage; discrimination, identity theft, etc.).

However, and the former being said, the overwhelming way in which the GDPR calculates a risk is by paying attention to the properties of the processing, which it considers as a proxy for the extent of the risk. One can only speculate as to why this is the case. On the one hand, it probably has to do with the compliance logic of the risk-based approach to the GDPR (i.e., to comply with legal obligations). On the other hand, it might also be the case that calculating risks when fundamental rights are at stake does not lend itself easily to quantitative and scientific calculations.

The proposed AIA risk

Different AIA risk

The proposed AIA does not seem to define what it means by risk either. That being said, it does contain some quite explicit indications as to how the risks should be measured.

Contrary to the GDPR, these seem to put the emphasis on the harms experienced -or to be experienced- by the individuals. This is particularly visible in Article 7(2) of the proposed Act, which contains the criteria according to which the European Commission can determine whether additional AI systems should be considered as high risk. Article 7(2) itself talks about a (risk of) harm to the health and safety (and/or adverse impact) and on fundamental rights[18]. Article 7(2)(c) of the proposed Act refers to the likelihood of the harm since it mentions harms that have already materialised or harms for which there are significant concerns that they will materialise. Article 7(2)(d) of the proposed Act refers to the severity of the harm (i.e., its 'intensity'), including its capacity to affect a plurality of persons. Articles

[18] One can assume that the reason why it makes the distinction between harms to health and safety and impacts on fundamental rights has to do with the vocabulary of the GDPR, which refers to impacts instead of harms, even though the two terms most likely cover the same reality. See for instance Black who shows that some fields like food regulation talk about hazards, while other fields such as financial regulation talk about impact, (Black 2010a, 190).

7(2)(e)-(g) contain indications as how to measure severity of the harm, in particular by looking at the way in which individuals have been harmed. Such harms include individuals being dependent upon the outcome of an AI system without any opt-out possibility (art. 7(2)(e) proposed AIA); the individual's vulnerability (e.g., imbalance of power, socio-economic imbalance, age - art. 7(2)(f) proposed AIA); or the irreversible nature of the harm on individuals (art. 7(2)(g) proposed AIA).

From this perspective both instruments seem to be diverging in the way they measure risk. Whereas the GDPR looks mostly at the properties of the processing as proxies for measuring the risk, the proposed AIA -underpinned by the logic of risk regulation and risks to health and safety- mostly looks at the harms for the individuals' health, safety, and fundamental rights[19].

Similar AIA risk?

However, this theoretical strong divergence between these two different ways of measuring risks could also be mitigated in practice. Even though the actuals Articles of the proposed AIA proclaim to look at the harms caused by AI systems, this claim can be toned down if we look at the proposed Act's Recitals. Rather than looking at harm, they seem to adopt the same technique as the GPDR. That is, to look at the properties of the processing (in this case the AI system), which are then used as a proxy in order to measure the severity of the risk.

This stems very clearly from a number of Recitals. Recital 33 looks at the discrimination harm (with a particular focus on discrimination on the basis of disabilities, age, sex, or ethnicity) linked to remote biometric identification systems. Instead of looking at the way in which such harms could take place at the level of individuals as Article 7 of the proposed Act seems to suggest, Recital 33 simply look at the properties of the AI system: if there are technical inaccuracies, then this indicates that the harm might take place. This is exactly the way the GDPR operates. A similar remark can be made in the context of Recital 38, which concerns actions by law enforcement. This Recital directly links harms to the rights to an effective remedy, to a fair trial, and to the presumption of innocence to the properties of the AI system being used. Namely, whether it is insufficiently designed and tested, trained on data of insufficient quality, or isn't sufficiently robust and accurate.

As one can see the purported distinction between the two ways of calculating risks might not be as strong as the different regulation models might suggest. Beyond issues of compliance with legal obligations (which can directly be linked to the GDPR's regulation model), this probably has to

[19] On the use of proxies, see (Black 2010a, 197).

do with the fact that in both cases the types of risks at stake here are risks to fundamental rights. The latter lend themselves much less easily to scientific and quantitative analyses of risk.

The regulatees' obligations

As previously mentioned, the fact that both risk-based approaches are rooted in different regulation models also allows us to compare them on the basis of the type of obligations they foresee for the regulatees. Whereas the very nature of the risk-based approach to the GDPR allows for some measure of flexibility in complying with data protection mandates, the same cannot be said for the proposed AIA. Risk is indeed only used to determine which AI systems should be regulated, and the latter are subject to so-called 'principle-based' obligations. However, as in the previous section this distinction can be mitigated on the account that the proposed AIA relies upon so-called quality management systems, which are in fact risk management instruments for compliance purposes.

GDPR obligations: compliance flexibility

As seen, the risk-based approach to data protection entails greater compliance responsibility for data controllers. This is done through the use of risk management tools, which are used in order to determine what the best way to comply is. This also entails that data controllers have more discretion in how to comply with the GDPR (see section 2.2.). Increased discretion can indeed be seen as a direct consequence of their increased responsibilisation (see section 2.2.) and is epitomised by the fact that risk is a contextual tool (i.e., allowing to find the most adequate safeguards for each specific situation) (see section 2.2.).

Of course, this discretion is not limitless. First, and as already discussed, this discretion is limited to matters of compliance with pre-existing legal obligations (cf., section 2.2). Second, whereas Article 24 GDPR grants data controllers quite some discretion in managing risks, this is less the case as far as high risks and Article 35 GPDR are concerned (account must be taken among others of the criteria from Article 35, from the high risk lists from supervisory authorities, and from the general criteria designed by the former Article 29 WP in its guidance on data protection impact assessments)[20]. Third, as also seen in section 2.2 the GDPR contains a number of mandatory risk

[20] This is confirmed for instance by the Belgian data protection authority, see, https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/analyse-d-impact-relative-a-la-protection-des-donnees, last consulted 01 October 2021.

management-based obligations that are contained in Chapter IV GDPR. This means that these various obligations must be an integral feature of the data controllers' risk management process (Gellert 2020, 20–21), thereby curbing their discretion.

Proposed AIA obligations: compliance inflexibility?

This section focuses on providers since they are the main duty bearers under the proposed AIA.[21] Whereas the GDPR's risk-based approach explicitly focuses on the regulatees' obligations, with a view of making them more flexible and efficient, the same cannot be said of the proposed AIA. As seen, the core of this approach consists in determining *ex ante*, which AI systems should be the object of regulatory intervention. As such it therefore does not say much about the nature of the regulatees' obligations. The proposed Act's Explanatory memorandum clarifies that when an AI system is considered high risk, it should be subject to the so-called 'principle-based requirements' that can be found in Chapter 2 of Title III (European Commission 2021, 3). The European Commission clarifies that these principle-based requirements are 'a set of horizontal mandatory requirements' that must be complied with (European Commission 2021, 3)[22]. These requirements include for instance Article 10, which contains requirements for the training, validation and testing data sets when the latter are used to the ends of training AI models. One can also mention Article 13, which contains transparency obligations with regards to the users of AI systems.

In other words, and compared to the flexible risk-based system of compliance featured in the GDPR, it would seem that the proposed AIA features a much more 'rigid' system of compliance. Rather than a (risk-based) partially flexible and discretionary system of compliance, the proposed AIA seems to feature the logic of rules abidance that is characteristic of command and control regulation (see, Morgan and Yeung 2007, chap. 4.2).

However, here too it is possible to mitigate this contrast between the two risk-based approaches. It would indeed seem that -very much like the GDPR- the proposed AIA also builds upon a risk-based system compliance. Namely, the so-called quality management system, which is enshrined in Article 17. Quality management systems are indeed recognised as being risk management tools that can be used for purposes of complying with legal

[21] See, proposed AIA, art. 16(a) following which the providers of high-risk AI systems shall 'ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2'.

[22] See also, proposed AIA, art. 8(1).

obligations[23]. If one is to interpret the proposed AIA correctly, the quality management system can be considered as the device through which all (of the provider's) compliance duties are internalised. This holds true for substantive obligations such as those enshrined in Article 10 of the proposed Act (on 'data and data governance') (see Articles 10(2)(c), and 17(f))[24]. But it also holds true for the proposed Act's prior market authorisation system (i.e., the conformity assessment procedure), which will only be granted in case of satisfactory quality management system[25].

The fact that the whole compliance system of the proposed AIA rests upon quality management system shows that the purported opposition between a system of flexible compliance (GDPR) and rigid compliance (proposed AIA) is not as sharp as it first appeared. If anything, it looks like the proposed AIA has, so to say, actually incorporated both approaches. Mahler has further explored this issue of the various meanings that can be given to the risk-based approach in the AIA, but this is beyond the scope of the present contribution (Mahler 2022). Suffices here to say that as far as risk regulation is concerned, Demortain had already observed the increasing role of risk management tools as an interface for compliance purposes, and the changes to risk regulation this has brought along (see, Demortain 2011, chap. 6).

Conclusions: beyond the differences, looking at the similarities in order to address the Type I versus Type II errors debate in the proposed AIA?

This contribution has endeavoured to compare the risk-based approaches in the GDPR and in the proposed AIA.

Even though both the GDPR and the proposed AIA rely upon the same moniker, the latter refers to different regulatory models. In the first case, the point is to use risk and risk management tools as a means to better comply. In the second, the point is to determine which AI systems should be regulated.

Understanding the risk-based approach as pertaining to risk-based models of regulation then allows to shift the focus of the comparison on key components of risk-based regulation models. Namely, the concept of risk at stake, and the type of obligations for regulatees. In both cases, there seems

[23] See, e.g., (Bazinet, Nissan, and Reilhac 2015, 32, 48–50, 60).

[24] See also proposed AIA, art. 17(a), which states that quality management systems should include a 'strategy for regulatory compliance'.

[25] In most cases the conformity assessment will consist in a self-assessment of the quality management system (and other legal requirements) pursuant to Annex VI of the proposed Act. See, proposed AIA, art. 43(1),(2). Confirming this interpretation, see (Veale and Zuiderveen Borgesius 2021, 106).

to be some sharp contrasts at first sight. Upon better look however, these are not as acute as it first seemed. Whereas the proposed AIA seems to measure a risk by looking at the harms created (as opposed to the GDPR which mainly looks at the properties of the processing) a closer look shows that the properties of the AI system are also key in measuring the risks. Similarly, whereas the proposed AIA seems to rely upon a number of principle-based requirements for high-risk AI systems, it appears that very much like the GPDR, risk management (in the form of quality management systems) is key to complying therewith.

As a way to end this contribution, the present conclusion would like to briefly discuss one important criticism that has been voiced against the risk-based approach in the proposed AIA. Namely, what is the normative justification for only regulating high risk AI systems instead of all of them (Hidvegi, Leufer, and Massé 2021; see also, Veale and Zuiderveen Borgesius 2021, 112)? Or alternatively, who gets to decide what a high-risk AI system is, and what if an AI system is considered non-high risk where in fact it should be considered high risk (Hidvegi, Leufer, and Massé 2021; BEUC 2021, 17–18)? This is a particularly salient point given that AI systems impact fundamental rights (High-Level Expert Group on Artificial Intelligence 2019a; Hidvegi, Leufer, and Massé 2021).

Admittedly this issue is not novel in the literature on regulation. Building upon Black, one can argue that regulators must determine the objectives of regulatory intervention *ex ante* (see, Black 2010a, 193). That is, the whole point of regulatory action is to determine what actions should be regulated (or what counts as safe or unsafe and thus should be authorised or not and under what conditions)[26]. As Black argues, whereas these choices are made somewhat implicitly in non-risk based models of regulations, they are rendered more explicit in risk-based models of regulation (Black 2010a, 193). A key issue therefore in determining the objects of regulatory intervention has been encapsulated in the debate between so-called Type I and Type II errors (Black 2010a, 188; Shrader-Frechette 1991). Following Black, in determining what counts as a high risk, should the regulator lean on the side of individuals with the risk of including non-high risk AI systems in the high risk category (cf., Type I error), or should they lean on the side of AI system providers and fail to consider an AI system as being high risk when that should have been the case (cf., Type II error) (Black

[26] See Hood et al.'s definition of risk regulation as: 'governmental interference with market or social processes to control potential adverse consequences to health' (Hood, Rothstein, and Baldwin 2001, 3). See also their discussion on the varying extents of risk tolerance that influence risk regulatory responses, (Hood, Rothstein, and Baldwin 2001, 5–6).

2010a, 188)? This is exactly the issue at stake with regard to the notion of high risk AI system: in determining what counts as a high risk AI system, should the European Commission be more risk averse (with the chance of wrongly including non-high risk systems) or should it be more risk friendly (with the chance of omitting some high risk AI systems)? Of course, in the Explanatory memorandum to its proposal the Commission assures us that the methodology used for defining high risks is 'a solid one' (European Commission 2021, 3). However, Black warns us that what is deemed to count as a high risk is also determined by the regulator's risk appetite; meaning that it is context-dependent and therefore susceptible to change through time (Black 2010a, 186). One should thus not be too sure of the purported 'solidity' of the European Commission's method[27]. In other words, if the use of a risk methodology helps make the choices of the regulator explicit (in terms of what qualifies as high risk), this does not change the fact that what ends up constituting a high risk is also dependent upon the regulator's risk appetite (see, Black 2010a, 186). Beyond that, isn't the very choice of limiting the regulatory intervention to high risk AI systems itself a 'Type I error versus Type II error' issue, given that focusing on high risks appears as quite risk friendly?

The choice to focus the regulatory attention on high risks can also be surprising given the already mentioned kinship of the proposed Act with the EU's New Legislative Framework, which seems to put the emphasis upon an adequate general level of health and safety.

One can take the example of the toys safety Directive[28], which is one of the New Legislative Framework instruments referred to by the proposed AIA in cases AI is also a safety component of the product[29]. Contrary to the proposed AIA it contains obligations for all toys and not only for high risk toys[30]. In other words, contrary to the proposed AIA, which only regulates high risk AI systems, all toys must satisfy essential safety requirements[31]. On top of that, high risk toys must conform to specific safety requirements that are laid out in Annex II of the Directive[32].

Interestingly, the use of risk management tools is also central in the toys safety Directive. Instead of relying upon a quality management system, the

[27] As seen, it is possible to add new systems but only within the existing predefined categories. Further, it remains to be seen how this mechanism will work in practice.

[28] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] OJ L170/1.

[29] See, proposed AIA, recital 30. See also proposed AIA, Annex II, Section A (containing the list of relevant EU harmonisation legislation based on the New Legislative Framework).

[30] See, toys safety Directive, art. 4(1).

[31] Toys safety Directive, art. 10, and in particular art. 10(3).

[32] The Directive does not explicitly use the expression high risk but this is what is at stake.

toys safety Directive relies upon so-called safety assessments. The latter are used for the conformity assessment procedure (Article 19), and also used to determine whether the non-high risk toys conform with essential safety requirements (Article 18).

On this basis, one can wonder why the European Commission did not adopt a similar approach for the proposed AIA. It could have been perfectly possible to require that all AI systems comply with a minimum or essential level of health, safety, and fundamental rights protection, which in this case would be undertaken through the quality management system (instead of the safety assessment). Furthermore, high risk AI systems would have been subject to the specific substantive requirements that are now enshrined in Chapter II of Title III of the proposed Act. Of course, such a proposal should not be seen as a silver-bullet solution as it means that the assessment as to whether an AI system satisfies these minimal requirements would be at the discretion of the provider in the context of the quality management system. However, this is just an initial idea that can be improved with stronger regulatory mechanisms. And the point is in any case to show that at a different regulatory approach to AI is possible; one that concerns all AI systems, and which is thus much less risk friendly than the existing proposal. In doing so it would also be more aligned with the precautionary principle, which is at the heart of many instruments of the New Legislative Framework,[33] and which has also been hailed as extremely important in harnessing the way AI technology is being deployed unto the European Union[34].

Bibliography

Legislation

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, PB L11/4

Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] OJ L170/1

European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence

[33] This is the case for the general product safety Directive. See Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, PB L11/4, Recital 1. This is also the case of the toys safety Directive (see art. 39).

[34] For instance, the European Commission appointed High-Level Expert Group on Artificial Intelligence had itself recommended that the future AI Act be based on the logic of the precautionary principle. See, (High-Level Expert Group on Artificial Intelligence 2019b, 37).

(Artificial Intelligence Act) and Amending Certain Union Legislative Act (2021) 167, 84, 85 final

Regulation 2016/679/EU 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 [2016] OJ L119/1

Literature

Art. 29 WP. 2014. "Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks."

———. 2017. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679."

Bazinet, Marc, Dori Nissan, and Jean-Marie Reilhac. 2015. *Au Coeur de l'ISO 9001:2015: Une Passerelle Vers l'excellence.* Paris: Afnor Éditions.

BEUC. 2021. "Regulating AI to Protect the Consumer: Position Paper on the AI Act." Brussels.

Black, Julia. 2001. "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World." *Current Legal Problems* 54 (1): 103–46. https://doi.org/10.1093/clp/54.1.103.

———. 2002. "Critical Reflections on Regulation." *Australian Journal of Legal Philosophy* 27 (1): 1–35.

———. 2010a. "Risk-Based Regulation: Choices, Practices and Lessons Being Learnt." In *Risk and Regulatory Policy: Improving the Governance of Risk*, edited by OECD, 185–224. Paris: OECD publishing.

———. 2010b. "The Role of Risk in Regulatory Processes." In *The Oxford Handbook of Regulation*, edited by Robert Baldwin, Martin Cave, and Martin Lodge, 302–48. Oxford: Oxford University Press.

Borraz, Olivier. 2008. *Les Politiques Du Risque.* Paris: Presses de Sciences Po.

CNIL. 2018. Délibération No 2018-327 Du 11 Octobre 2018 Portant Adoption de La Liste Des Types d'opérations de Traitement Pour Lesquelles Une Analyse d'impact Relative à La Protection Des Données Est Requise.

Demetzou, Katerina. 2018. "GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved." In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, edited by Eleni Kosta, Jo Pierson, Daniel Slamanig, Simone Fischer-hübner, and Stephan Krenn, 137–54. Cham: Springer.

———. 2019. “Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of ‘High Risk’ in the General Data Protection Regulation.” *Computer Law and Security Review* 35 (6). https://doi.org/10.1016/j.clsr.2019.105342.

Demortain, David. 2011. “Scientists and the Regulation of Risk. Standardizing Control.” Cheltenham UK, Northampton, MA, USA: Edward Elgar Publishing.

European Commission. 2020. “Communication From the Commission to the European Parliament and the Council Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation.”

———. 2021. “Explanatory Memorandum to the 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.”

Gellert, Raphaël. 2020. *The Risk-Based Approach to Data Protection.* Oxford: Oxford University Press.

Hidvegi, Fanny, Daniel Leufer, and Estelle Massé. 2021. “The EU Should Regulate AI on the Basis of Rights, Not Risks.” 2021. https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

High-Level Expert Group on Artificial Intelligence. 2019a. “High Level Expert Group on AI: Ethics Guidelines for Trustworthy AI.”

———. 2019b. “Policy and Investment Recommendations for Trustworthy AI.” Brussels.

Hood, Christopher, Henry Rothstein, and Robert Baldwin. 2001. *The Government of Risk - Understanding Risk Regulation Regimes.* Oxford, UK: Oxford University Press.

Mahler, Tobias. 2022. “Between Risk Management and Proportionality: The Risk-Based Approach in the EU’s Artificial Intelligence Act Proposal.” In *Nordic Yearbook for ICT Law*, edited by Stanley Greenstein and Liane Colonna.

Morgan, Brownen, and Karen Yeung. 2007. *An Introduction to Law and Regulation: Text and Materials.* Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781107415324.004.

Quelle, Claudia. 2017. “The ‘Risk Revolution’ in EU Data Protection Law: We Can’t Have Our Cake and Eat It, Too.” In *Data Protection and Privacy: The Age of Intelligent Machines*, edited by Ronald Leenes, Rosamunde van

Brakel, Serge Gutwirth, and Paul De Hert, 33–62. Oxford and Portland, Oregon: Hart Publishing.

Selznick, Philip. 1985. "Focusing Organizational Research on Regulation." In *Regulatory Policy and the Social Sciences*, edited by Roger G. Noll. Berkeley and Los Angeles: The University of California Press.

Shrader-Frechette, Kristin. 1991. *Risk and Rationality: Philosophical Foundations for Populist Reforms*. Berkeley: University of California Press.

Veale, Michael, and Frederik Zuiderveen Borgesius. 2021. "Demystifying the Draft EU Artificial Intelligence Act: Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach." *Computer Law Review International* 22 (4): 97–112.

Warner, Frederick. 1992. "Introduction." In *Risk: Analysis, Perception and Management - A Report of a Royal Society Study Group*, edited by The Royal Society, 1–12. London: The Royal Society.

Weimer, Maria. 2019. Risk Regulation in the Internal Market: Lessons from Agricultural Biotechnology. Oxford: Oxford University Press.

Yeung, Karen. 2004. *Securing Compliance: A Principled Approach*. Oxford and Portland, Oregon: Hart Publishing.