

# From the AI White Paper of the European Commission to the Draft ‘AI-Act’— Contours of a Legal Framework for AI in *Statu Nascendi*



Belen Olmos-Giupponi und Hannes Hofmeister

## 1 Introduction

Artificial intelligence<sup>1</sup> has become an integral part of our everyday lives: assistance systems in cars, facial recognition on mobile phones and smart home applications in the kitchen—they all function on the basis of AI. In response to this emerging trend and to address the challenges posed by AI, the European Union<sup>2</sup> has also consistently devoted more attention to this topic.

Against this backdrop, this article analyses the development from the White Paper to the current Draft AI Regulation.<sup>3</sup> For this purpose, this article first (Sect. 2) provides an overview of the Commission’s ‘AI White Paper’. Having done so, the need for a comprehensive AI legal framework will be discussed in more detail (Sect. 3) and then (Sect. 4) the contours of such a framework pursuant

---

<sup>1</sup> Hereinafter referred to as ‘AI’.

<sup>2</sup> Hereinafter referred to as ‘EU’.

<sup>3</sup> Hereinafter referred to as ‘D-AI Regulation’.

---

The authors would like to thank Prof. Dr Arnold for his comments on earlier drafts of this article. This paper constitutes an updated, expanded and translated version of a paper published by the author initially in DVBI (2022).

---

B. Olmos-Giupponi  
Middlesex University, London, UK  
E-Mail: [b.olmosgiupponi@mdx.ac.uk](mailto:b.olmosgiupponi@mdx.ac.uk)

H. Hofmeister (✉)  
Freie Universität Bozen, Bozen, Italy  
E-Mail: [hannes.hofmeister@eui.eu](mailto:hannes.hofmeister@eui.eu)

to the White Paper will be outlined. This article (Sect. 5) then focuses on the implementation of the White Paper by the draft ‘AI Act’ of April 2021. This draft is a legal novelty as it constitutes the first concrete approach to regulating AI worldwide. The main features of this ‘Act’ are briefly presented and then subjected to a critical analysis.

## 2 The White Paper

The Commission’s White Paper of 19 February 2020<sup>4</sup> is a statement of intent outlining the Commission’s ambitious vision for the development and regulation of AI in the EU.

From the outset, the Commission indicates the advantages and drawbacks of AI. Clearly, the White Paper underlines the importance the Commission attaches to AI, especially in improving healthcare, climate protection, security and the efficiency of production and transport. In the Commission’s view, AI is not only one of the most important applications of the ‘data economy’, but also a crucial tool for achieving the Union’s objectives—namely to improve the lives of individuals and to advance society as a whole.<sup>5</sup> On the other hand, the Commission is also aware of the risks of the increased use of AI: especially with regard to data protection and the prohibition of discrimination new conflicts might arise.<sup>6</sup> Further conflicts might arise with regard to liability issues and the use of AI in critical infrastructures.<sup>7</sup>

Looking at the conflicts to be resolved, the Commission asserts that the current legal framework is not sufficient to address AI inherent risks. While the *acquis unionaire* may deal with some of these risks, the Commission emphasises the necessity of a detailed review of them to ascertain whether AI systems create additional risks that require normative regulation. Taking into consideration the specific characteristics of AI systems (such as unpredictability, complexity, autonomy), the Commission then concludes in its White Paper that an adaptation of the current legal framework to the changed circumstances is necessary; in addition, new legislation specifically on AI is also needed.<sup>8</sup> However, in order to regulate AI in a coherent and comprehensive manner, the Commission believes that a new legal framework for AI is sorely needed, rather than just introducing singular modifications and tweaks.<sup>9</sup>

---

<sup>4</sup>White Paper on Artificial Intelligence—A European approach to excellence and trust, COM (2020) 65 final, 19.02.2020.

<sup>5</sup>See *ibid.*, 2.

<sup>6</sup>See *ibid.*, 10 ff.

<sup>7</sup>See *ibid.*, 12.

<sup>8</sup>See *ibid.*, 18–19.

<sup>9</sup>See *ibid.*, 18–19.

### 3 The Need for an ‘AI Legal Framework’

But is the codification of an AI legal framework at EU level really necessary? It is rightly pointed out that a comprehensive AI legal framework could lead to overregulation. Moreover, it is questionable, whether it is not too early for such comprehensive regulation, especially since not all problems inherent in the new technology are yet known. *Prima facie*, these arguments seem convincing; a closer look, however, shows that they are not really persuasive: For example, the danger of overregulation can be avoided by a risk-based design.<sup>10</sup> Prompt implementation at EU level is also necessary, as otherwise there is a risk of unilateral regulatory measures adopted at national level. This could lead to a fragmentation of the internal market. In addition, as concerns the risks inherent in a horizontal regulatory approach, it can be argued that fundamental requirements for AI can first be formulated across sectors and later specified on a sector-specific basis.<sup>11</sup> Finally, the symbolic effect of adopting a European legal framework for AI must also be considered as this legislation lays down the groundwork for developing appropriate legislation on the international level.<sup>12</sup> As a result, the better arguments militate in favour of codifying a new AI legal framework at EU level.

The main contours of such a European legal framework for AI will be outlined in more detail below.

## 4 The Contours of a European AI Legal Framework According to the White Paper

### 4.1 *The Regulatory Scope of the New Legal Framework*

#### 4.1.1 The Definition of AI

According to the Commission, the proposed legal framework should apply to AI-based products and services. The White Paper describes AI in broad terms simply as ‘a collection of technologies that combine data, algorithms and computing power’.<sup>13</sup> At the same time, it concedes that the definition of AI in the new legal framework must be flexible enough to keep abreast of new technological developments and, at the same time, precise enough to guarantee the necessary degree of

---

<sup>10</sup>O. Unger, Grundfragen eines neuen europäischen Rechtsrahmens für KI, ZRP 2020, 235.

<sup>11</sup>Ibid., 235.

<sup>12</sup>Ibid., 235.

<sup>13</sup>White Paper on Artificial Intelligence—A European approach to excellence and trust, COM (2020) 65 final, 19.02.2020, 2.

legal certainty.<sup>14</sup> Based on these premises, one would therefore expect a specification of the above-mentioned laconic definition; this is all the more so as the White Paper explicitly emphasises the importance of a clear definition.<sup>15</sup> However, such a definition is not provided. The White Paper merely refers to the first approach of a defining AI by the Commission in its 2018 Communication, which states:

‘Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions—with some degree of autonomy—to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).’<sup>16</sup>

This is followed by a reference to the specification of this definition by the ‘High Level Expert Group’ set up by the Commission. According to this, AI systems are ‘software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.’<sup>17</sup>

Based on these two conceptualisations, it is therefore necessary to develop a subsumable definition of AI for the future legal framework. The Commission’s statements in the White Paper imply a broad understanding of AI that also includes so-called symbolic, i.e. rule-based systems.

#### 4.1.2 AI ‘with High Risk’ (So-Called Risk-Based Approach)

In line with the principle of proportionality, the new legal framework is not intended to apply to each and every form of AI.<sup>18</sup> Rather, the Commission envisages a risk-based approach—as is already the case under the GDPR. Only AI applications with a high risk should therefore be subject to the new legal framework. Whether such a high risk exists is to be determined on the basis of two criteria: One has to examine whether (a) the sector and (b) ‘the intended use pose significant risks, in particular from the point of view of security, consumer rights and fundamental

---

<sup>14</sup> See *ibid.*, 16 et seq.

<sup>15</sup> See *ibid.*, 17 et seq.

<sup>16</sup> Communication of the Commission, AI for Europe, COM (2018) 237 final, 1.

<sup>17</sup> High Level Expert Group, A Definition of AI (2018), 36, available online at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

<sup>18</sup> White Paper on Artificial Intelligence—A European approach to excellence and trust, COM (2020) 65 final, 19.02.2020, 17.

rights'.<sup>19</sup> The sector-specific and use-specific risks of the AI application are therefore decisive.

As far as the *sector* in question is concerned, it is necessary to examine whether it involves significant socio-economic risks due to the nature of the typical activity. Specifically, '[t]his first criterion ensures that the regulatory intervention is targeted on the areas where, generally speaking, risks are deemed most likely to occur. The sectors covered should be specifically and exhaustively listed in the new regulatory framework. For instance, healthcare; transport; energy and parts of the public sector'.<sup>20</sup>

As regards the *use* in question, it is worth examining whether the way in which the AI application is employed entails particular risks. 'This second criterion reflects the acknowledgment that not every use of AI in the selected sectors necessarily involves significant risks. For example, whilst healthcare generally may well be a relevant sector, a flaw in the appointment scheduling system in a hospital will normally not pose risks of such significance as to justify legislative intervention'.<sup>21</sup>

From the Commission's standpoint, only if both conditions are met can a 'high risk' AI application be assumed. The cumulative application of the criteria thus serves two purposes: On the one hand, it is intended to ensure that the scope of application remains targeted and on the other hand to increase legal certainty.<sup>22</sup>

However, there should also be exceptions to this basic rule. Hence, the use of AI applications should always be considered 'high-risk' (regardless of the respective sector) if so-called inherent risks are associated with it, for example, if AI applications are used for recruitment processes or for biometric remote identification.<sup>23</sup>

## **4.2 Mandatory Requirements for 'High-Risk AI' Applications**

In substantive terms, the Commission is considering making the use of 'high-risk AI' applications subject to a number of conditions: for example, introducing the obligation to train AI applications with datasets that have appropriate validity and representativeness to ensure that AI applications are safe, non-discriminatory and appropriately respect privacy and personal data.<sup>24</sup>

---

<sup>19</sup> Ibid., 17.

<sup>20</sup> Ibid., 17.

<sup>21</sup> Ibid., 17.

<sup>22</sup> Ibid., 17.

<sup>23</sup> Ibid., 18.

<sup>24</sup> Ibid., 18 et seq.

Furthermore, it must be ensured that AI applications—at all stages—are robust, accurate and able to deal adequately with errors or inconsistencies. In addition, they must be resistant to attacks and their results must be reproducible.<sup>25</sup>

Last but not least, the legal framework should also stipulate binding requirements regarding the following aspects: Appropriate requirements that ensure transparency and alert stakeholders to the existence of AI applications. Requirements that ensure that human oversight remains in place and that human autonomy is not undermined by AI. Specific requirements for systems using remote biometric identification that ensure respect for fundamental rights.<sup>26</sup>

## 5 The Implementation of a European Legal Framework for AI—The Draft Regulation

The proposals of the White Paper on AI were specified in spring 2021 by the European Commission. On 21 April 2021, the Commission presented its proposal for a ‘Regulation laying down harmonised rules on Artificial Intelligence’<sup>27</sup> (‘AI Act’).<sup>28</sup> This proposal is a legal novelty—it is the first specific approach to regulate AI worldwide. In the following sections, the key features of the draft regulation will be presented and then subjected to a critical analysis.

### 5.1 *The Key Features of the Draft Regulation*

#### 5.1.1 Subject Matter

Pursuant to Article 1, the D-AI Regulation lays down rules for placing on the market, putting into service and using AI systems in the EU; the prohibition of certain practices in the field of artificial intelligence; as well as special requirements for high-risk AI systems and obligations for the operators of such systems.<sup>29</sup>

---

<sup>25</sup> Ibid., 19 et seq.

<sup>26</sup> M. Lachenmann, EU-Kommission veröffentlicht Weißbuch für die Regulierung von Künstlicher Intelligenz, ZD-Aktuell 2020, 07021.

<sup>27</sup> EU Commission, ‘Proposal of the European Parliament and of the Council for a Regulation laying down harmonised rules on Artificial Intelligence’ (AI Act) and amending certain Union legislative acts, Brussels, 21 April 2021, COM (2021) 206 final.

<sup>28</sup> For reasons of simplicity the following abbreviation will be used hereinafter ‘D-AI Regulation’.

<sup>29</sup> Article 1 a-c D-AI Regulation.

In addition, the Regulation also contains provisions for market surveillance and market monitoring.<sup>30</sup>

### 5.1.2 Scope of Application

The scope of application of the D-AI Regulation is based on the model of the General Data Protection Regulation. Accordingly, it covers almost everyone who uses AI in the EU or in relation to EU citizens.<sup>31</sup> In this respect, Article 2 I D-AI Regulation stipulates the following:

‘This Regulation applies to:

- a. providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;
- b. users of AI systems located within the Union;
- c. providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union’.<sup>32</sup>

In order to ensure a comprehensive degree of protection, the scope of application of the D-AI Regulation is broad.

For instance, the territorial scope of application is given (a) when an AI system is placed on the market or put into service in the EU or (b) when the result produced by the AI system is used within the EU.<sup>33</sup>

As far as the addressees of the D-AI Regulation are concerned, the providers<sup>34</sup> are covered— i.e. those who develop an AI system and place it on the market. In addition, the D-AI Regulation also covers users<sup>35</sup>— i.e. those who purchase a corresponding system and use it for their own purposes, see Article 2 I b, 3 No. 4 D-AI Regulation. Purely private use, on the other hand, is not regulated.<sup>36</sup>

In terms of the *ratione materiae*, the D-AI Regulation regulates the placing on the market, the putting into service and the use of AI systems. The draft is based

<sup>30</sup> Article 1 e D-AI Regulation.

<sup>31</sup> S. Zimprich, Insight: Die EU-KI Verordnung, 24.08.2021, available online at <https://www.fieldfisher.com/de-de/insights/die-eu-ki-verordnung-teil-1>.

<sup>32</sup> Article 2 I D-AI Regulation.

<sup>33</sup> Article 1(c) D-AI Regulation.

<sup>34</sup> Pursuant to Article 3 No. 2 AI Regulation, a ‘provider’ is defined as a ‘a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge’.

<sup>35</sup> Pursuant to Article 3 No. 2 D-AI Regulation a ‘user’ is defined as ‘any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity’.

<sup>36</sup> S. Zimprich, Insight: Die EU-KI Verordnung, 24.08.2021, available online at <https://www.fieldfisher.com/de-de/insights/die-eu-ki-verordnung-teil-1>.

on the following understanding of the term ‘AI system’: An artificial intelligence system (AI system) is ‘software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with’.<sup>37</sup> The techniques listed in Annex I include, (1) machine learning concepts, (2) knowledge-based techniques, and (3) statistical methods.<sup>38</sup> The list of techniques in Annex I is not exhaustive. In order to be able to react quickly to new technical developments, Article 4 of the D-AI Regulation<sup>39</sup> authorizes the Commission to amend the list by way of delegated legislation.<sup>40</sup>

If a software constitutes an ‘AI system’, then it falls within the ‘scope of the D-AI Regulation—and triggers more or less extensive compliance and documentation obligations depending on the risk level’.<sup>41</sup> These risk levels and the associated obligations will be discussed in more detail below.

### 5.1.3 Risk-Based Approach

While the White Paper only envisaged a single category, i.e. ‘high-risk AI’, the approach of the draft regulation is more nuanced. It provides for a differentiation between four different categories of AI:

- AI systems with unacceptable risks.
- AI systems with high risks
- AI systems with low risks, and
- AI systems with minimal risks

These categories will be examined in more detail below.

#### 5.1.3.1 AI Systems with Unacceptable Risks

AI systems with unacceptable risks are generally prohibited under Article 5 of the D-AI Regulation. These are AI systems that are generally considered to have a particularly harmful effect. Pursuant to Article 5 of the D-AI Regulation, these prohibited practices in the field of AI include:

---

<sup>37</sup> Article 3 No. 1 AI Regulation.

<sup>38</sup> See Annex I of the AI Regulation, available online at [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF).

<sup>39</sup> In conjunction with Article 73 D-AI Regulation.

<sup>40</sup> In conjunction with Article 73 D-AI Regulation.

<sup>41</sup> S. Zimprich, Insight: Die EU-KI Verordnung, 24.08.2021, available online at <https://www.fieldfisher.com/de-de/insights/die-eu-ki-verordnung-teil-2-das-ki-system>.

AI systems that deploy ‘subliminal techniques beyond a person’s consciousness in order to materially distort a person’s behaviour in a manner that causes or is likely to cause that person ... physical or psychological harm’.<sup>42</sup>

Furthermore, AI systems that manipulate the behaviour of vulnerable groups of people (e.g. minors) and thereby cause them physical or psychological harm.<sup>43</sup> An example would be children’s toys with voice assistants that encourage minors to behave dangerously.<sup>44</sup>

In addition, Article 5 I c of the D-AI Regulation prohibits ‘social scoring applications’ to assess the trustworthiness of natural persons on the basis of their social behaviour. Addressees of this prohibition are state agencies only.

The use of real-time remote biometric identification systems in public spaces for law enforcement purposes is also prohibited, although certain exceptions apply in this context, see Article 5 I d of the D-AI Regulation. These exceptions, however, only apply if real-time remote biometric identification is absolutely necessary with regard to one of the following objectives:

- a. ‘the targeted search for specific potential victims of crime, including missing children;
- b. the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
- c. the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State’.<sup>45</sup>

In these cases—which can be subsumed under the heading of ‘public security’—the use of real-time biometric remote identification systems is thus permissible by way of exception. Exceptions other than those explicitly mentioned in Article 5 I d (i)–(iii) of the D-AI Regulation are—arguing *e contrario*—not envisaged.<sup>46</sup>

<sup>42</sup> Article 5 I a D-AI Regulation.

<sup>43</sup> Or are likely to cause them harm, see Article 5 I b D-AI Regulation.

<sup>44</sup> European Commission, New Rules for AI, Q&A, available online at [https://ec.europa.eu/commission/presscorner/detail/de/QANDA\\_21\\_1683](https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683).

<sup>45</sup> Article 5 I d (i)–(iii) AI Regulation.

<sup>46</sup> Pursuant to Article 5 II of the D-AI Regulation a balancing of interest has to be conducted. Said Article stipulates:

‘(2) The use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

- (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;
- (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations’.

In view of the high threshold set by Article 5 of the Regulation, this risk category is likely to play only a minor role in practice.

### 5.1.3.2 High-Risk AI Systems

The focus of the draft is on so-called ‘high-risk AI systems’ as codified in Title III. It is expected that these systems will play a key role in practice. For this reason, the draft regulation contains detailed provisions for high-risk systems. In the following, we will first (1) clarify what is meant by a high-risk AI system and then (2) set out the requirements for such systems.

The D-AI Regulation envisages two main categories of ‘high-risk AI systems’ in Article 6:

1. ‘AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;
2. other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III’.<sup>47</sup>

According to Annex III of the draft regulation, AI systems are considered ‘high-risk’ if they affect one of the following areas: (1) the remote identification of natural persons; (2) the operation of critical infrastructures (e.g. power supply); (3) education and training with regard to access decisions and assessments of natural persons; (4) employment and human resource management, in particular hiring decisions; (5) access to and use of fundamental private and public services and benefits; (6) law enforcement; (7) migration, asylum and border control; and (8) the judiciary.<sup>48</sup> In order to be able to react quickly to new technical developments, Article 7<sup>49</sup> of the D-AI Regulation empowers the Commission to make amendments to the list by means of delegated legislation.

For high-risk AI systems, the Regulation stipulates a number of specific requirements. These are intended to strengthen confidence in AI systems and ensure a high standard of protection.<sup>50</sup> According to Article 9 of the D-AI Regulation, high-risk AI systems are therefore subject to a risk management system, the details of which are specified in Article 9 II of the D-AI Regulation. According to this provision, the risk management system includes:

<sup>47</sup> EU Commission, ‘Proposal of the European Parliament and of the Council for a Regulation laying down harmonised rules on Artificial Intelligence’ (AI Act) and amending certain Union legislative acts, Brussels, 21 April 2021, COM (2021) 206 final., 15.

<sup>48</sup> EU Commission, Annexes to the ‘Proposal of the European Parliament and of the Council for a Regulation laying down harmonised rules on Artificial Intelligence’ (AI Act) and amending certain Union legislative acts, Brussels, 21 April 2021, COM (2021) 206 final., 5 et seq.

<sup>49</sup> In conjunction with Article 73 D-AI Regulation.

<sup>50</sup> EU Kommission, Neue Vorschriften für künstliche Intelligenz, available online at [https://ec.europa.eu/commission/presscorner/detail/de/QANDA\\_21\\_1683](https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683).

- ‘(a) [the] identification and analysis of the known and foreseeable risks associated with each high-risk AI system;
- (b) [the] estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;
- (c) [the] evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;
- (d) [the] adoption of suitable risk management measures in accordance with the provisions of the following paragraphs’.<sup>51</sup>

In addition, ‘high-risk AI systems’ are subject to more specified data governance requirements (Article 10 D-AI Regulation). According to Article 10 II of the D-AI Regulation, these include, for example, the selection of data sets. Furthermore, the D-AI Regulation subjects high-risk AI systems to a series of documentation obligations (Article 11 D-AI Regulation), record keeping obligations, (Article 12 D-AI Regulation) and transparency requirements (Article 13 D-AI Regulation). These comprehensive requirements are intended to facilitate, inter alia, product monitoring obligations, see Article 12 III D-AI Regulation. In addition, high-risk AI systems must be designed in such a way that they can be effectively monitored by human beings, Article 14 D-AI Regulation. This is again based on the idea of confidence-building, in that humans should be able to react immediately to malfunctions and also prevent them.

#### 5.1.3.3 AI Systems with Low or Minimal Risk

The proposal classifies as low risk AI systems systems that are prone to specific manipulation risks, for example, because they are designed for interaction with natural persons or because they generate so-called ‘deep fakes’.<sup>52</sup> For these systems, special transparency obligations apply according to Article 52 of the D-AI Regulation. In particular, the use of AI must be disclosed to users. All other AI systems, and thus the vast majority of systems in use today that cannot be assigned to one of the above groups, are classified as minimal risk AI systems. These can be used in compliance with the generally applicable rules.<sup>53</sup>

## 5.2 Critical Analysis

A critical analysis of the D-AI Regulation is far from easy, given the novel and ambitious nature of this legislative project.

---

<sup>51</sup> Article 9 II D-AI Regulation.

<sup>52</sup> Article 52 I-III D-AI Regulation.

<sup>53</sup> S. Zimprich, Insight: Die EU-KI Verordnung, 24.08.2021, abrufbar online unter <https://www.fieldfisher.com/de-de/insights/die-eu-ki-verordnung-teil-1>.

One strength of the draft is undoubtedly its **broad geographical scope of application**.<sup>54</sup> Article 2 of the D-AI Regulation applies to all providers who place AI systems on the market or put them into operation in the Union, irrespective of whether they are established in the EU or in a third country.<sup>55</sup> In this respect, the D-AI Regulation clearly goes beyond the traditional approach of product safety law.

On the other hand, the D-AI Regulation also contains a number of **restrictive elements** that limit the Regulation's scope of application considerably. For example, the D-AI Regulation is not supposed to apply without restrictions to civil aviation or to motor vehicles that contain AI based safety components.<sup>56</sup> In addition, AI for exclusively military purposes is also excluded from the scope of the Regulation. The reason for this exception is to be found in the principle of conferral, Article 5(1) and (II) TEU. According to this principle, the EU may only legislate if the Treaties confer on it a corresponding competence. However, this is not the case with regard to military matters.

The D-AI Regulation is also ridden with numerous **drafting deficits**, which create a considerable degree of legal uncertainty. Article 5(1)(c) of the D-AI Regulation is a case in point. It prohibits so-called 'social scoring applications' to assess the trustworthiness of natural persons on the basis of their social behaviour. However, this prohibition is not as absolute as it appears *prima facie*: According to Article 5(1)(c) (i)–(ii) of the D-AI Regulation, the prohibition is to be limited to impairments of these persons in social contexts that have no connection to the circumstances under which the data was originally generated or collected, or to impairments that are unjustified or disproportionate with regard to the social behaviour.<sup>57</sup> In this way, the D-AI Regulation indirectly restricts the prohibition of social scoring again *via the reference* to the balancing of interests and thereby generates a considerable degree of legal uncertainty.<sup>58</sup>

The draft also **lacks effective legal remedies** for the individuals concerned.<sup>59</sup> This is surprising, given that one of the key objectives of the D-AI Regulation is to foster individual trust in AI. In case of algorithm-based assessments, malfunctions cannot be ruled out. Such malfunctions can cause serious damage to consumers and hence the latter need adequate legal protection. For this reason, some suggest that the draft should be supplemented—in analogy to the GDPR<sup>60</sup>—by

<sup>54</sup> G. Spindler, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz, CR 2021, 373.

<sup>55</sup> Article 2 I a D-AI Regulation

<sup>56</sup> See Article 2 II D-AI Regulation.

<sup>57</sup> G. Spindler, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz, CR 2021, 365.

<sup>58</sup> *Ibid.*, 365.

<sup>59</sup> Bomhard/Merkl, Europäische KI-Verordnung RD i (2021), 283 et seq.

<sup>60</sup> See Article 13 et seq. of the GDPR.

corresponding rights of those affected to rectification and deletion of unjustified evaluations.<sup>61</sup>

The **design of the conformity assessment procedure** is also deficient—especially the failure to make assessment by an *independent* body mandatory. Pursuant to Article 43(2) of the D-AI Regulation<sup>62</sup>, high-risk AI systems listed in Annex

<sup>61</sup> Bomhard/Merkl, Europäische KI-Verordnung RD (2021), 283 et seq.

<sup>62</sup> Article 43 D-AI Regulation provides:

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chap. 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:
  - (a) the conformity assessment procedure based on internal control referred to in Annex VI;
  - (b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chap. 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

2. For high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to 101 of that Directive.
3. For high-risk AI systems, to which legal acts listed in Annex II, section A, apply, the provider shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chap. 2 of this Title shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.

For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chap. 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been assessed in the context of the notification procedure under those legal acts.

Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in Chap. 2 of this Title.

III<sup>63</sup> are ‘certified’ by a ‘self-declaration’ of the provider after an internal control has been carried out.<sup>64</sup> This is not convincing. Rather, (stand-alone) AI systems should be subject to a conformity assessment by independent bodies, as is the case for ‘embedded’ AI systems.<sup>65</sup> A mere self-certification by the providers as to whether they meet the requirements does not seem appropriate in view of the considerable risks inherent in such systems. Also, the objectives of the regulation—namely the creation of trustworthy AI and (concomitantly) social acceptance—can hardly be achieved without mandatory certification by independent institutions.

The Commission has opted for a **horizontal regulatory approach**. This means that the scope of application of the D-AI Regulation is not limited to individual sectors. Rather, the D-AI Regulation has a cross-sectoral or cross-application effect. It is sometimes argued that such a horizontal regulatory approach risks that the specifics of individual sectors are neglected.<sup>66</sup> However, it can be countered that the fundamental requirements for AI systems can indeed be ‘formulated in cross-sectoral terms and yet further specified in sector-specific terms’.<sup>67</sup> This also applies to the D-AI Regulation. In principle, the horizontal regulatory approach is therefore to be welcomed, as it overcomes the sectoral limits of product safety law.<sup>68</sup>

- 
4. High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user.

For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.

5. The Commission is empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating Annexes VI and Annex VII in order to introduce elements of the conformity assessment procedures that become necessary in light of technical progress.
6. The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies.

<sup>63</sup> Specifically speaking Annex III Nr.2–8.

<sup>64</sup> See G. Spindler, *Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz*, CR 2021, 370.

<sup>65</sup> See Article 43 III D-AI Regulation.

<sup>66</sup> O. Unger, *Grundfragen eines neuen europäischen Rechtsrahmens für KI*, ZRP 2020, 235.

<sup>67</sup> *Ibid.*, 235.

<sup>68</sup> G. Spindler, *Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz*, CR 2021, 373.

In addition, the issue was raised whether it is too early for such a comprehensive regulation of AI, since not all problems inherent in this technology are known yet. *Prima facie*, this argument seems convincing; however, on closer inspection, it is not that persuasive at all. For instance, prompt implementation at EU level is called for, as there would otherwise be the risk that each Member State would adopt national regulatory measures. This, in turn, would lead to a fragmentation of the internal market. Finally, the ‘symbolic effect’ that the adoption of a European AI act would have, should not be neglected.<sup>69</sup>

## 6 Conclusion

With the publication of the AI White Paper in February 2020, the first foray was made into a field of regulation that will continue to occupy lawyers, politicians and IT experts in the future.<sup>70</sup> Only one year later, the White Paper found its first specification in the draft of an AI Regulation (‘AI Act’). In sum, this draft is to be welcomed for the reasons outlined above, although it must be conceded that there is still a need for improvement in several respects, in particular with respect to the design of the conformity assessment procedure and the effective legal protection of Individuals.

---

<sup>69</sup> O. Unger, Grundfragen eines neuen europäischen Rechtsrahmens für KI, ZRP 2020, 235.

<sup>70</sup> Ibid., 234.

**Open Access** Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

