DATA AND DATA GOVERNANCE AND CONNECTIONS TO DATA PROTECTION PRINCIPLES IN ARTICLE 10 OF THE ARTIFICIAL INTELLIGENCE ACT

María Loza Corera

PhD in Law. Lead Advisor at Govertis part of Telefónica Tech.
Lecturer at the International University of La Rioja

I. Introduction

In today's world, nothing can be understood without data, not even the past. Data is an essential asset. In the context of the so-called digital economy, data play a role of paramount importance, to the point of talking about the data economy or data-driven economy[1]. In this context, Artificial Intelligence has even been mentioned as one of the most valuable intangible assets of any company as a driver of organisational value[2]. However, technology is not neutral[3], nor is the approach to risk regulation used[4], so design and data are absolutely relevant and the AI Act (hereafter AIA) is proof of this. The consequences of not having the right type of data, nor the required quality, could be disastrous, as they condition the results of the specific AI solution adopted from the design stage, and are therefore invalid and, more importantly, could affect the security and/or fundamental rights of individuals. The relationship between the data and the AI system is therefore directly proportional to the quality of the results obtained. However, not only will it be necessary to have adequate data sets and quality, but it is also essential to relate these data to the appropriate technology, specific internal procedures and for certain purposes determined by the organisation, not forgetting compliance with the different applicable regulatory frameworks, in other words, to establish a system of governance. At a time when we are already talking about the transition to the

[1] Loza Corera, M., De los microdatos a los datos masivos. Cuestiones legales, University of Valencia, 2017, p. 259.

[2] Witzel M. and Bhargava N., "AI-Related Risk The Merits of an ESG-Based Approach to Oversight", CIGI Papers No. 279, August 2023. https://www.cigionline.org/static/documents/no.279.pdf

[3] Floridi, L., "On Good and Evil, the Mistaken Idea That Technology is Ever Neutral, and the Importance of the Double-charge Thesis". Philosophy & Technology, September 2023, available SSRN: https://ssrn.com/abstract=4551487

[4] Kaminski M., "Regulating the risk of AI", 2022, Boston University Law Review, Vol. 103:1347, 2023, U of Colorado Law Legal Studies Research Paper No. 22-21, available SSRN: https://ssrn.com/abstract=4195066 p. 1351.

quantum economy[5], it is a *conditio sine qua non* to establish an adequate governance system to enable this transition.

The term Governance could well be one of those "*suitcase words*" that Marvin Minsky defined as words with multiple meanings. For this reason, it is necessary to clarify the different meanings of this term, although, as we will see, they are fully related, especially in the field of Artificial Intelligence. First, the concept of data governance will be addressed, taking into account the vital importance of data for an Artificial Intelligence system. Subsequently, the importance of data governance in the current European regulatory context and its meaning in this context will be analysed. Finally, it will analyse the concept of data governance in AIA, which is closer to the concept of *data equity*.

The AIA devotes an entire article (Article 10) in Chapter III, dedicated to high-risk AI systems, to *Data and data governance*, aware of the vital importance of data and data governance in an AI system. We can state without any doubt that this is one of the core articles of the Regulation, as not having adequate data sets will prevent the implementation of an AI system from the outset, not only because of the possible biases inherent in the underlying data, but also because AI also *learns* from data. The evolution, processing and final content of Article 10 will be studied in detail, including all the changes and modifications that have occurred since the European Commission's Proposal for a Regulation in April 2021, through the text proposed by the Council and the amendments approved by the European Parliament in June 2023, to its final version. It should be noted that the issues of accuracy, robustness and bias are not dealt with in this chapter, as they are specifically addressed in the chapter headed by Ana Aba Catoira. The above detailed study of the data governance obligations established by the Regulation will allow us to critically approach the final version contained therein.

Finally, we will briefly analyse the relationship between data governance and the principles of data protection, without prejudice to the more extensive general analysis of data protection in the chapter headed by Jesús Jiménez López.

II. Data governance

1. Concept of data governance

The concept of governance is not exclusive to data management, but

[5] World Economic Forum, "Quantum Economy Blueprint", January 2024, available at https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf.

rather has its origins in other areas, such as Information Technology Governance (IT Governance). However, given the increasing prominence that data has acquired in organisations, both public and private, the concept of data governance, proportionally to this prominence, has acquired its own substance and has become a real necessity.

Data is a core element in the digital economy, to the point of talking about the "data economy", so that properly managing this business asset is a necessary budget in order to be a *data-driven* company. Extracting value from data in order to make more conscious and effective decisions is a possibility that cannot be ignored in the current economic and technological context. This is where the concept of data governance takes on its full importance.

There is no unambiguous or normative definition for the concept of "Data Governance". Initially, data governance was understood to refer to the internal context of an organisation, only in relation to the control and management of its data, and has subsequently evolved into a broader and more elaborate concept. Thus, the *Data Governance Institute* defines it[6] as "the exercise of decision-making and authority in data-related matters", and more broadly, as "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods".

For its part, the *Data Management Association (*DAMA) has created a reference framework for data management, *Data Management Body of Knowledge* (DMBOK[7]), in which data governance occupies an essential place within data management, making it clear that these are not overlapping concepts. That is why data governance or data governance is conceived as the "exercise of authority and control (planning, monitoring and enforcement) over the management of data assets".

The Spanish Data Protection Agency (AEPD) defines[8] data governance as "the strategy for the correct administration and management of data policy in the organisation". The AEPD stresses that the data protection policies to be adopted by the controller in compliance with Recital 78 and Article 24 of

[6] https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/

[7] The DMBOK focuses on eleven main themes: Data Governance; Data Architecture; Data Modelling and Design; Data Storage and Operations; Data Security; Data Integration and Interoperability; Documents and Content; Master and Reference Data; Data Warehousing and Business Intelligence; Metadata and Data Quality.

[8] AEPD, "Governance and Data Protection Policy", 2020 https://www.aepd.es/prensa-y-comunicacion/blog/gobernanza-y-politica-de-proteccion-de-datos

the General Data Protection Regulation[9] (GDPR) are an important part of the organisation's data policy.

It also indicates that, where personal data are processed, they should be added to the data governance objectives:

- Comply with data protection principles.

- To ensure that data subjects are able to exercise their rights.

- Ensure protection of personal data protection by design and by default, through risk management for rights and freedoms.

- Comply with the remaining legal obligations derived from data protection regulations.

Salvador Serna[10] highlights that, despite the multiple approaches to the concept of data governance, "there is a certain consensus in associating data governance with the ideas of: (1) valuing data as an asset of the organisation that must be managed (2) establishing responsibilities in decision-making (rights) and associated tasks (duties) and (3) establishing guidelines and standards to ensure the quality of data and its proper use". To these characteristics, we add a fourth, the need for strategic leadership from management for the establishment of a data governance system, not depending on an exclusive department or area of the company, so that, as a transversal system, it is coherent with the objectives and culture of the organisation and, of course, with the regulations in force.

It is therefore essential to have a data governance system in place, as it enables the comprehensive management of data throughout its life cycle, both in terms of quality, protection, security and maintenance, as well as regulatory compliance. In addition to obtaining the maximum value from the data to help in making more efficient decisions, proper data governance minimises risks, saves costs by centralising information management, eliminates silos, improves data quality and processes thanks to the monitoring and continuous improvement system and, very importantly, establishes the conditions to allow the scalability of different AI solutions that can be adopted. Therefore, we move from the concept of data governance to AI governance, but the former being a necessary presupposition to be able to talk about the latter.

[9] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals 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).

[10] Salvador Serna, M., (2021), Inteligencia artificial y gobernanza de datos en la Administración Pública: sentando las bases para su integración a nivel corporativo, in *Repensando la administración pública: administración digital e innovación pública,* (pp. 126-148), INAP, 2021.

Industry is well aware of the imperative need for an AI governance system, not only to comply with regulations, but to drive business value.[11]

2. European context

The above concept of data governance, which can be referred to as 'micro', must necessarily be put in relation to the current EU political and regulatory context, in particular, to the data governance mechanisms or regulatory requirements at the 'macro' level necessary to enable the single market for data.

In 2018 the European Commission launched its *Artificial Intelligence Strategy*[12] where it laid the foundations to ensure that the potential of AI serves human progress by enhancing the Union's technological and industrial capacity, by preparing for the socio-economic transformations that AI will bring about, and by establishing an appropriate ethical and legal framework, based on the Union's values and in line with the EU Charter of Fundamental Rights. In this way forward, a clear and essential objective is to increase the volume of data available and to facilitate access to it. Thus, the European Commission, aware of the value of data for both the economy and society and, without renouncing the protection of personal data, has promoted the *EU Data Strategy*[13], in the framework of the policy priorities set for the period 2019-2024 (*A Europe fit for the digital age*)[14] and of the *Digital Compass 2030: Europe's approach for the Digital Decade.*[15]

In the *European Data Strategy* the Commission states that "The aim is to create a single European data space, a true single data market, open to data from all over the world, where personal and non-personal data, including sensitive business data, is secure and where businesses also have easy access to an almost infinite amount of high quality industrial data, in a way that drives growth and creates value, while minimising the human environmental and carbon footprint".

To achieve such a single European data space that ensures Europe's glob-

[11] IBM, The urgency of AI governance, 2023. https://www.ibm.com/downloads/cas/MV9EXNV8

[12] COM(2018) 237 final, *Artificial Intelligence for Europe.*

[13] COM(2020) 66 final, *A European Data Strategy,* European Commission https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066

[14] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit--digital-age_es

[15] COM(2021) 118 final https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021DC0118

al competitiveness[16] and data sovereignty[17], as stated in the European Data Strategy, EU legislation must be effectively implemented so that all data-based products and services comply with the rules of the single data market. Alongside appropriate legislation, 'clear and reliable' governance mechanisms to enable access to and use of data must be adopted to ensure that the objectives of the European data space are met.

The European regulatory framework designed to enable the realisation of the European Data Strategy consists, among others, of the Data Governance Regulation 2022/868[18] and Regulation 2023/2854 on harmonised rules for fair access to and use of data (Data Regulation)[19], not forgetting the Regulation on a framework for the free flow of non-personal data in the European Union[20], consistent with the meaning given to the concept of 'data' by the above-mentioned Regulations, whose meaning is much broader than the concept of 'personal data'.

It should be emphasised that the European single data market is not unaware that international data flows are indispensable in today's markets and competitive environments, and therefore has an open approach, but without renouncing European protection and values.

We see, therefore, how we have progressively evolved from a regulation focused on the protection of personal data and the rights and freedoms of individuals, to a strategy focused on data (not necessarily personal) as a business asset, the centre of the data economy, which needs regulations that guarantee its availability, sharing and secure reuse, but always preserving European values. This is why, in order to guarantee the single market for data (governance at the "macro" level), it is essential for organisations to have solid data governance at the internal level (micro level), which will also make it possible to move towards the governance of Artificial Intelligence.

[16] COM(2020) 66 final "However, the sources of competitiveness for the coming decades in the data economy are determined now. This is why the EU must act now".

[17] The functioning of the European data space will depend on the EU's ability to invest in the next generation of technologies and infrastructures, as well as in digital skills such as data literacy. This, in turn, will increase Europe's technological sovereignty in terms of key enabling technologies and related infrastructures for the data economy.

[18] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation).

[19] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Regulation).

[20] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32018R1807&qid=1696786250350

3. Concept of governance in the field of Artificial Intelligence

The AIA does not provide a definition of governance applied to the field of AI. Nor is there a definition in ISO *Information technology-Artificial Intelligence - Artificial Intelligence concepts and terminology ISO/IEC 22989*. The IAPP[21] defines "*AI Governance*" as "*A system of policies, practices and processes organisations implement to manage and oversee their use of AI technology and associated risks to ensure the AI aligns with an organisation's objectives, is developed and used responsibly and ethically, and complies with applicable legal requirements*". Similarly, the industry defines it as "*AI governance is a system of rules, practices, processes and tools that help an organisation use AI in alignment with its values and strategies, address compliance requirements and drive trustworthy* performance"[22]. It is argued that AI governance is likely to be as important as the specific governance of the components of the algorithm itself.[23]

However, regardless of whether there is a normative definition or not, it is unquestionable that the concept of governance takes on its full importance in the field of AI to the point of transcending the concept of data governance to speak of AI governance. Any organisation must establish the necessary procedures to ensure compliance with applicable regulations, the necessary security measures and respect for fundamental rights and freedoms, as well as to guarantee the proactive responsibility of the organisation and its governing bodies in the use of the different AI solutions it decides to implement. In fact, if we had to sum up AIA in one word, it would be "Governance".

It should not be misunderstood that these obligations only fall on the entities that develop AI systems, but that those that design or deploy them (deployers or those responsible for the deployment) also have responsibilities, so that, although at different levels, it is necessary for all organisations to establish AI governance mechanisms.

There are different AI governance systems or frameworks. In the field of *soft law*, the *Artificial Intelligence Risk Management Framework*[24] (AI RMF) of the *National Institute of Standards and Technology* (NIST) in the US and the *Governance Guidelines for the Implementation of AI Principles*[25] in Japan stand out, al-

[21] IAPP, Key Terms for AI Governance, June 2023. https://iapp.org/resources/article/key-terms-for-ai-governance/

[22] Op. cit. IBM, The urgency of AI governance, 2023.

[23] In fact, in 2022, AI governance was the ninth most important strategic priority for privacy functions. In 2023, it is the second most important strategic priority, IAPP-EY Professionalizing Organizational AI Governance Report, p. 9, 2023.

[24] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[25] AI Governance in Japan, REPORT FROM THE EXPERT GROUP ON HOW AI

though to date there is no binding regulatory framework in this area, whilst there is already a glimpse of its forthcoming approval in both countries. By contrast, in Europe there was no specific framework for AI governance until the adoption of the European Regulation.

Regardless of the different approaches to AI Governance, the very concept of Governance is fully in line with Novelli, Taddeo and Floridi's[26] assertion that proactive accountability is a cornerstone of AI governance.

The AIA refers specifically to data governance. Thus, both Recital 67 and Article 10 refer to "good governance and data management practices", which we will analyse below. Therefore, leaving aside Chapter VII dedicated to institutional governance at both the European (European Artificial Intelligence Committee) and national (national competent authorities) levels, the Regulation refers to the concept of data governance, thus at the 'micro' level. This does not mean at all that the AI governance established by the European Regulation is exhausted in this article rather dedicated to data governance, but it must be put in relation with the other obligations established for high-risk AI systems, which require the implementation of other procedures, such as conformity assessment procedures, declaration of conformity and CE marking, quality management systems that include compulsory change management procedures, techniques, procedures and systematic actions to be used for design, design control and design verification and quality control, data management systems and procedures, risk management system, post-market surveillance, serious incident reporting procedure, procedures for recording all documentation and the establishment of an accountability framework. All these obligations make up what we mean by AI governance under the European Regulation.

Finally, there is a broader perspective on AI governance, directed at regulators, in that some authors consider that the regulation being proposed in Europe, Canada and elsewhere is not sufficient to prevent other risks that may occur in the longer term. Thus, KOLT[27] argues that regulatory proposals

PRINCIPLES SHOULD BE IMPLEMENTED, 2021, available at https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_8.pdf.

[26] NOVELLI C., TADDEO M., FLORIDI L., Accountability in artifcial intelligence: what it is and how it Works, AI & Soc (2023) https://doi.org/10.1007/s00146-023-01635-y

[27] Kolt, N., Algorithmic Black Swans (October, 2023). Washington University Law Review, Vol. 101, Forthcoming, available SSRN: https://ssrn.com/abstract=4370566 p. 42. These principles are: Principle 1: AI governance should seek to anticipate and mitigate large-scale harms from AI systems; Principle 2: AI governance should adopt a portfolio approach composed of diverse and uncorrelated regulatory strategies; Principle 3: AI governance should be highly scalable; Principle 4: AI governance should continuously explore and evaluate new

to regulate AI “focus primarily on the immediate risks of AI, rather than on broader, longer-term risks” and therefore “offers a roadmap for “algorithmic preparedness”: a set of five forward-looking principles to guide the development of regulations that address the prospect of algorithmic black swans and mitigate the harms they pose to society”.

III. Development, processing and final content of Article 10

The AIA dedicates Article 10, within Section 2 of Chapter III dedicated to High Risk AI Systems, to *Data and data governance*, aware of the vital importance that data and data governance have within an AI system. To approach the analysis of its content, we will first analyse the roles involved, and then delve into the obligations associated with each of them.

1. Roles involved

It should be emphasised that the obligations set out in Article 10 relating to data and data governance are set out without mentioning the specific data subject, as they are configured as requirements of the high-risk system itself.

Therefore, in order to establish which parties are obliged to implement good data governance and management practices, we must first look at the datasets on which these obligations fall, to see to which part of the value chain they correspond. Thus, Article 10 distinguishes between datasets used for training, validation, and testing of high-risk AI systems, as distinct from those that do not use techniques involving model training. [28]If we look at the various figures that make up the value chain, already analysed throughout this work, leaving aside those roles that do not directly influence the development of the AI system, such as the distributor[29] or the importer[30], the provider[31] stands out. The provider means the entity that *develops or for which* an AI system or a general-purpose AI model *is developed* and brings it to the market or puts it into service under its own name or trademark, whether for payment or free of charge, and should therefore have data sets used for training, validation and testing of the system. However, the provider, by definition, can either de-

regulatory strategies; Principle 5: Cost-benefit analysis of AI governance interventions should take more account of worst-case outcomes.

[28] Article 10.6.

[29] Article 3. 7).

[30] Article 3. 6).

[31] Article 3(3).

velop the AI system directly or contract third parties to carry out such development, in which case, the corresponding obligations must be contractually regulated. In this regard, the European Parliament recalled in its Recitals[32] that algorithm *developers* are particularly relevant as they may have used underlying (historical) data which may not meet the desirable quality requirements due to biases, or may have generated this data in real environments and therefore be biased by default. Finally, the explicit reference to developers has been omitted from the Recital, while maintaining the importance of the quality of the underlying data.

In relation to the figure of the *provider*, it should be borne in mind that, in terms of responsibilities along the AI value chain, the Regulation in certain cases considers[33] "provider" of a high-risk AI system to be any distributor, importer, deployer or other third party and, therefore, subject to the obligations set out in Article 16 for providers and deployers of high-risk AI systems and other parties. In this regard, it should be noted that the Parliament proposed[34] to amend the title of Article 16 to include not only providers, but also deployers and other parties, but this amendment was not finally accepted. However, despite the obvious coherence of the amendment proposed by the Parliament, this does not affect the substance, as Article 25.1 expressly provides for the liability of these figures. Therefore, any distributor, importer, deployer, or other third party who (i) places its name or trade mark on a high-risk AI system already placed on the market or put into service (ii) makes a substantial modification or (iii) makes a modification in such a way that the AI system becomes a high-risk AI system, will be subject to the obligations set out in Article 16 and thus to compliance with all the requirements for high-risk systems, including those relating to data governance. The final version[35] has included the definition of "downstream provider", defined as a provider of an AI system, including a general purpose AI system, which integrates an AI model, regardless of whether the model is provided by themselves and vertically integrated or provided by another entity based on contractual relationships.

For its part, the *deployer*[36] is the entity that uses an AI system under its own

[32] Amendment 78 on Recital 44 (now Recital 67).

[33] Article 25.1.

[34] Amendment 331, Article 16, title: "Obligations of providers and deployers of high-risk AI systems and other parties".

[35] Article 3.68.

[36] Article 3.4. It is worth highlighting the relevant change introduced by the European Parliament (through Amendment 172 which modifies the definition of user in Article 3.4) in coherence with Recital 59) which dispenses with the term "user" to call it "deployer", which

authority, provided that the "domestic exception" does not apply, meaning this that its use is part of a personal activity of a non-professional nature. Although not expressly mentioned, we understand that the deployer will be liable whenever he retrains the system given by the provider. The issue of retraining will be discussed in more detail below.

Article 10 only expressly mentions the provider in relation to the possibility to exceptionally process special categories of data to the extent strictly necessary to ensure the detection and correction of negative bias. The Parliament added[37] a second express reference to the provider, in setting out its possible exemption from liability for breach of any of the obligations laid down in Article 10, transferring such liability to the deployer, in case the provider does not have access to the data, because they are held exclusively by the deployer and this has been laid down in a contract. This paragraph has not been included in the final version, but it is questionable what sense it would make for a deployer to have exclusive access to the data of a system introduced to the market by a provider, but without the deployer using it under their own authority, as in that case they would already have responsibility for it.

In any case, of particular interest is the mention[38] made by the Parliament in relation to the possibility of outsourcing the requirements related to data governance "by using third parties offering certified compliance services, including verification of data governance, data set integrity and data training, validation and testing practices", which has been accepted in the final text. Therefore, we believe that a new figure ("data verifiers" or "certified data service providers") will enter the value chain, precisely in charge of supplying providers or deployers with datasets for the development of AI systems, which comply with the requirements established by the AIA.

2. Obligations

Article 10 on data and data governance is of paramount importance [39] as compliance with the obligations set out therein is the basis for high quality

we understand to be more clarifying as it rules out confusion with the end user of the system, a natural person.

[37] Amendment 291 introducing a new paragraph 6a.

[38] Amendment 78 modifying Recital 44 *in fine* (now Recital 67).

[39] Recital 67 states (unofficial translation) "High quality data and access to high quality data play an essential role in providing structure and ensuring the functioning of many AI systems, in particular where techniques involving model training are employed, with a view to ensuring that the high-risk AI system operates as intended and safely and does not become a source of any discrimination prohibited by Union law (…)".

data and thus for the proper functioning of AI systems, especially high-risk ones.

Thus, high-risk AI systems that make use of techniques involving the training of models with data, should be developed from datasets that meet the *quality criteria* specified in paragraphs 2 to 5. In contrast to the requirement to use training, validation and test datasets that meet the above quality criteria, it should be noted that the European Parliament proposed a modulation[40] that these quality criteria should be met "to *the extent that this is technically feasible* in accordance with the market segment or scope of application concerned". The Parliament also pointed out that these criteria should be met for techniques that do not require labelled input data, such as unsupervised learning and reinforcement learning. Neither of these two proposals of the Parliament was finally accepted, so that the final version has eliminated any kind of modulation of responsibility. We will now look at the quality criteria set out in each of the paragraphs.

The second paragraph specifies the *good* data governance and management *practices* to which training, validation, and test datasets used for training models of high-risk AI systems should be subjected. We can classify these practices around different actions:

- (a) relevant design decisions;

- its recompilation: (b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;

- data preparation: (c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

- (d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;

- to the preliminary study of the datasets: (e) an assessment of the availability, quantity and suitability of the data sets that are needed);

- the quality of the data:

- (f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

- (g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f); and

- (h) the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

[40] Amendment 278 modifying Article 10(1).

Firstly, it should be noted that, unlike the Commission and Council proposals which spoke of "good governance and data management *practices*", the Parliament[41] proposed to replace this term by "*appropriate governance* to the context of use as well as the intended purpose of the AI system" which implied the adoption of a series of *measures*. The final version does not take up the Parliament's proposal and reverts to "appropriate governance and data management *practices* fit for the intended purpose of the AI system".

As regards the specific practices, most of the amendments introduced by the Parliament have finally been accepted. Thus, the Parliament included[42] a new practice concerning transparency on the original purpose of data collection, which the final text[43] further specifies by distinguishing between processes for the collection of non-personal data, in which case the origin of the data must be indicated, and personal data, for which the original purpose of collection must be indicated.

In the practice concerning the preparation operations[44] of the data, the Parliament added the update[45] of the data.

Regarding the prior study of the datasets[46], the Parliament[47] removed the requirement for prior assessment of the availability, quantity, and adequacy of the necessary datasets, which in our view does not make much sense, as, although such an assessment should obviously be prior, it reinforced its *ad hoc* character.

But it is in the measures relating to data quality that the Parliament made the most significant changes. Thus, as regards the examination of possible bias[48], the Council added the precision that they could "affect the health and safety of natural persons or give rise to discrimination prohibited by EU law". For its part, the Parliament added[49] that they could "adversely affect fundamental rights". In relation to that they may give rise to discrimination prohibited by EU law, the Parliament added "in particular where the outgoing data influence the incoming data in future operations ("feedback loop"), a clarification that has not been included in the articles", but has been included

[41] Amendment 279 modifying Article 10(2).

[42] Amendment 280 including a new paragraph (aa).

[43] Article 10.2(b).

[44] Article 10(2)(c).

[45] Amendment 282.

[46] Article 10.2(e).

[47] Amendment 284.

[48] Article 10(2)(f).

[49] Amendment 285.

in Recital 67. The Parliament also introduced a new practice[50], consisting of carrying out "appropriate measures to detect, prevent and mitigate potential biases", which goes beyond *ex ante* examination of particular datasets and requires measures to be put in place to detect, prevent, and mitigate potential biases that may be detected or become apparent at a later stage.

In relation to the practices concerning the identification of possible data gaps or deficiencies and how to remedy them[51], the Parliament introduced[52], and this is reflected in the final version, the qualification that such gaps or deficiencies shall be those "relevant to prevent compliance with this Regulation", thus seeming to narrow the objective scope of these remedyable gaps or deficiencies.

The third paragraph of specifies a series of *obligations* ***that*** began as a result, but which have finally been modulated. Thus, it states that the data sets used for training, validation and testing "shall be relevant, sufficiently representative and, as far as possible, error-free and complete for the intended purpose".

In relation to this first obligation, the Council introduced a first modulation by including "as far as possible" before the imperative ("shall be free of errors and complete"). Subsequently, the Parliament[53] significantly modified the wording and added the adverb "sufficiently" representative to the obligation for the data to be representative.

Secondly, the obligation of result to be free of errors and complete is transformed by the Parliament into "duly assessed for errors and as complete as possible in view of the intended purpose"[54]. The final text similarly states "to the best extent possible free of errors and complete in view of the intended purpose of the system". This development can also be seen in a correlative manner in Recital 67.

Finally, an obligation is added that the datasets shall have appropriate statistical properties, in relation to the persons or groups of persons for whom the high-risk AI system is intended to be used. The datasets *may meet* these characteristics individually for each data item or for a combination of data items. The Parliament corrects that the datasets *shall meet* these characteristics,

[50] Amendment 286 which introduced a new paragraph (f a), now paragraph (g).

[51] Article 10(2)(h).

[52] Amendment 287.

[53] Amendment 288.

[54] Consistent with Recital 44 which states that "(…) they should be sufficiently relevant and representative, adequately checked for errors and as complete as possible in view of the intended purpose of the system (…)".

not individually for each data item, but for each dataset or for a combination of datasets, as the final text reads.

The fourth paragraph states that the data "ss shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used". The Parliament proposed to add[55] that reasonably foreseeable misuses of the AI system should also be taken into account, which will not be taken up by the final version. On the other hand, this obligation should be connected to the presumption set out in Article 42 whereby the requirements of the fourth paragraph shall be presumed to be met provided that high-risk AI systems have been trained and tested with data reflecting the specific geographical, behavioural, contextual, and functional environment in which they are intended to be used.

The fifth paragraph establishes the possibility for providers to process special categories of data "to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction". It should be noted that the Parliament called such *negative* biases and defined them[56] as those that "create(s) a direct or indirect discriminatory effect against a natural person", but in the end, the concept of "negative bias" was not taken up in the final version. It provides for the possibility of establishing an adequate legitimation basis[57] in order to be able to process special categories of data which, in application of data protection law, shall not exempt from the obligation to adopt appropriate safeguards

the rights and freedoms of natural persons. Recital 70 expressly speaks of 'a matter of substantial public interest' and rescinds the express reference to Article 9.2(g) of Regulation (EU) 2016/679 and Article 10.2(g) of Regulation (EU) 2018/1725, which the Council had first introduced. On this point, for data processing to be covered by Article 9.2(g) of the GDPR (processing is necessary for reasons of essential public interest), it should be recalled that this must be provided for in a rule of national or European law, which also specifies the essential public interest justifying the processing of such data, in which circumstances the right to data protection may be limited, precise rules and appropriate safeguards at both technical and organisational level to

[55] Amendment 289.

[56] Amendment 78 in Recital 44 *in fine*.

[57] Amendment 160 introducing a new Article 2.5a: "This Regulation shall not affect Regulation (EU) 2016/679 (…), without prejudice to the mechanisms provided for in Article 10(5) (…)" which is finally included in the final text.

protect the interests and fundamental rights of the data subject. Here, the Parliament, instead of listing by way of example a number of measures, introduced[58] a catalogue of necessary conditions that must apply for processing to take place, including that the processing of synthetic or anonymised data does not effectively achieve the detection and correction of bias; that the data to be used are pseudonymised or subject to technical limitations on the re-use of personal data and to the most advanced security and privacy-preserving measures; or that they are deleted once the bias has been corrected or when the personal data reach the end of their retention period, which have been set out in the final text.

The European Parliament underlines the exceptionality of the fact that providers of such systems may process special categories of data by introducing the adverb 'exceptionally'. In this regard, the Parliament introduced a requirement that providers making use of this provision should produce documentation explaining why the processing of special categories of personal data is necessary to detect and correct bias. In the final version this obligation does not expressly mention providers and merely states that records of processing activities in accordance with Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725 should include such justification.

Having seen the quality criteria established for training, validation, and test datasets for the development of high-risk AI systems using techniques involving model training with data, the sixth paragraph establishes that these quality criteria, with respect to the development of high-risk AI systems that do not employ techniques involving model training, shall only apply to test datasets. Interestingly, while the Commission stated for these systems that they should ensure compliance with the good data governance and management practices set out in the second paragraph, the Council, the Parliament and the final version extend this obligation to all quality criteria (paragraphs 2 to 5) but limit such compliance only to test datasets.

IV. Critical approach

In the light of the development of the normative proposal for Article 10, this section will critically assess the final content of Article 10.

Firstly, in relation to roles, a general criticism is the absence of a definition of end-user or 'affected' by the AI system, especially considering that

[58] Amendment 290.

the Parliament proposed to introduce a definition[59] of 'affected person' and that these fall within the scope of the AIA[60]. In relation to the AI value chain and the roles involved in it, following the important reference[61] introduced by the Parliament in relation to the possibility of outsourcing the requirements related to data governance, as discussed in the section on roles, we understand that all the circumstances are in place for the emergence in the value chain of new figures that exclusively provide "verified" data and certify that the data comply with the established governance requirements, as well as their integrity and training ("data verifiers" or "certified data service providers"). Regulation and possible transfer of responsibility will therefore be key. However, is questionable whether this model of "verified" data provision can deliver the individualised compliance with such governance requirements that the Regulation aspires to, since, firstly, governance must be tailored to the context of use as well as to the intended purpose of the AI system[62] and, secondly, the sets of data sets that will be used for the purpose of the AI system will need to be defined, secondly, datasets should take into account, to the extent required by the intended purpose, the characteristics or elements specific to the geographical, behavioural, contextual, or functional environment in which the high-risk AI system is intended to be used.[63] In this way, as PEGUERA POCH[64] warns, the value chain could acquire "different configurations to those considered by the legislator depending on the evolution of the business models that end up being consolidated".

Moreover, as recommended by the European Data Protection Supervisor (EDPS)[65], it should be specified that AI operators who retrain pre-trained AI systems are included in the concept of providers, as AI systems may be

[59] person concerned: any natural person or group of persons who are exposed to an AI system or otherwise affected by an AI system". The reasons which may have led to the non-acceptance of this amendment are not understood, especially when it does introduce the reference to the mechanisms of guarantee or protection in the event of infringement of the Regulation, which, on the other hand, are not reserved to the person affected by the AI system, but to any person who considers that there has been an infringement of the Regulation; and, finally, because it does provide other definitions which do not seem so relevant, such as the "subject" who participates in tests under real conditions or the "informed consent" of this person.

[60] Article 2.1(g).

[61] Amendment 78 modifying Recital 44 *in fine*.

[62] Article 10, second paragraph.

[63] Article 10, fourth paragraph.

[64] Peguera Poch, M. "La propuesta de reglamento de AI: una intervención legislativa insoslayable en un contexto de incertidumbre", in Peguera Poch (coords.) *Perspectivas regulatorias de la Inteligencia Artificial en la Unión Europea*, Madrid: Reus, 2023.

[65] EDPS, *Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legisla-*

trained more than once during their lifecycle or may apply continuous learning techniques. Retraining may be due, says the EDPS, either to the lack of large data sets for training, or because they are retrained in order to be used for a similar task in a different domain (transfer learning). The AIA also does not clarify whether retraining or continuous learning activities are considered as part of the 'development' of the AI system, as in that case they would clearly be considered as providers. The EDPS states that this point is particularly relevant in relation to foundational models and the generalised possibility of retraining them. The Regulation does not include a definition of the operations that are included in the 'development' of an AI system, and in the definition of provider, although it includes a reference to the development or marketing under its name or brand of a general purpose AI model, there is no mention of retraining. However, only one Recital[66] expressly mentions retraining as a process that can be incorporated by the provider into the AI system. Therefore, a systematic and teleological interpretation would lead us to consider the provider as the one who introduces a retrained system on the market, although the clarification made by the EDPS would have been appropriate.

Secondly, Article 10 refers to the requirements to be met by training, validation and test datasets to be used for the development of high-risk AI systems using techniques that involve training models with data. It has been highlighted by certain authors[67] that it ignores other stages of *machine learning that* should also be subject to data quality criteria and data governance practices and also with respect to data licences that allow access to data.

The first paragraph establishes a sort of obligation of result, stating that high-risk AI systems that make use of techniques involving the training of models with data "shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 (…)". The Parliament proposed to introduce a liability modulation, or rather the removal of such an obligation of result in respect of all governance ob-

tive developments, p. 8. https://edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf

[66] Recital 88: 'Within the AI value chain, multiple parties often provide AI systems, tools and services, but also components or processes that are incorporated by the provider into the AI system for various purposes, including model training, model *retraining*, model testing and evaluation, integration into software or other aspects of model development (…)'.

[67] Ebers, M., Hoch, V. R. S., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. "The european Commission's proposal for an Artificial Intelligence Act-A critical assessment by members of the robotics and AI law society (RIALS)", 2021, J, 4(4), p. 595. doi: https://doi.org/10.3390/j4040043

ligations, by making compliance with such requirements "technically feasible in accordance with the relevant market segment or scope ". This modulation was a significant modification, but in practice it might not be so, since it was based on purely technical criteria, and the justification for the impossibility of complying with some of the required quality criteria would have to demonstrate precisely the technical impossibility in each specific case. What is relevant is that the final version has eliminated any kind of modulation of liability, regardless of the specific segment or scope of application or technical impossibility, which reinforces the importance of complying with the quality criteria in any case.

The second paragraph introduces the governance and management practices to be complied with by the data sets for training, validation, and testing of high-risk systems, which involve a whole data management system. These data governance practices must necessarily be connected to the quality management system and, in particular, to the risk management system, although this is not expressly stated, which would have been desirable, as it would underline the importance of compliance with Article 10, which, as we have said, is essential. The quality management system does mention[68] "data management systems and procedures including data acquisition, collection, analysis, labelling, storage, filtering, searching, aggregation, preservation and any other data-related operations carried out before the introduction to the market or commissioning of high-risk AI systems", but we believe it would have been desirable to make express reference to the complete data governance system established in Article 10, in the same way as the express reference to the risk management system is included. In relation to the risk management system established in Article 9, it is stated that "The risks referred to in this Article shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information", which seems to exclude risks arising from non-compliance with data quality criteria. However, the same article specifies that the known and foreseeable risks to health, safety, or fundamental rights that the high-risk AI system may entail should be identified and analysed, which implies that risks arising from non-compliance with data quality criteria and governance practices cannot be ignored. In any case, the data governance system set up by the AIA has sufficient substance of its own that it transcends the risk management system, but this does not imply that it is unknown to the latter.

The importance of the data governance system is evidenced by the fact

[68] Article 17.1(f).

that it forms part of the technical documentation (Annex IV) to be retained by the provider for ten years, although it does not explicitly mention Article 10, but refers, in relation to the data, to a general description of the training data sets used and information about their provenance, scope and main characteristics; the way in which the data were obtained and selected; the labelling procedures (e.g., for supervised learning) and data cleaning methodologies (e.g., anomaly detection); and the validation and test procedures used, including information about the validation and test data used, and its main characteristics. It would have been desirable to include an explicit reference to Article 10 data governance procedures in order to provide sufficient traceability for potential liability claims.

In the Commission's proposal, the third paragraph established an obligation of result that the data sets to be used for training, validation, and testing "shall be relevant, representative, error-free and complete". Industry or even some governments, such as the Norwegian government[69] and some authors, were reluctant to draft it as an "absolute requirement", as it is an impossible task that data can always be free of errors and such a level of perfection is "technically unfeasible" and could hamper innovation[70]. Other authors[71] have highlighted the existence of conditionalities to the fulfilment of these apparently strict obligations, which in fact lower the level of requirements. Thus, the successive versions have introduced formulas that have lowered the level of requirements for obtaining these results, so that the final version establishes that the data must be relevant, sufficiently representative *and, as far as possible*, free of errors and complete, taking into account the intended purpose. It would have been advisable to also introduce, together with the purpose, the reference to reasonably foreseeable misuses[72], for the sake of consistency as these are taken into account in the risk assessment of Article 9.[73]

This apparent modulation of responsibility, we believe, should be connected to the concept of proactive responsibility, so it must be possible to demonstrate relevance, sufficient representativeness, analysis of possible errors, and data completeness, although it is true that due to the very nature

[69] https://www.regjeringen.no/contentassets/939c260c81234eae96b6a1a0fd32b6de/norwegian-position-paper-on-the-ecs-proposal-for-a-regulation-of-ai.pdf

[70] *Cit*. Ebers, M. *et alia.*

[71] Veale M. and Borgesius F., "Demystifying the Draft EU Artificial Intelligence Act", Computer Law Review International, 2021, 22(4), pp. 97-112, para. 41. DOI https://doi.org/10.48550/arXiv.2107.03721

[72] Article 3. 13).

[73] Article 9.2(b).

of AI, it may be problematic to evaluate the responsibility for the results obtained.[74]

On the other hand, it is somewhat paradoxical to speak of "quality criteria" when no criteria for measuring the quality of the datasets are specified, referring only to the desirable outcome[75]. In other words, the AIA leaves such specification to the field of standardisation, which is in a way understandable as it deals with mostly technical aspects, but at the same time leaves the standard somewhat empty of substantive content[76]. Thus, it is stated[77] that "standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation(…)". It should be noted at this point that the amendments[78] made by the Parliament imply an active role for the Commission and not a mere "outsourcing" of the issue to standardisation bodies. Thus, the Commission, taking into account the importance of standards in ensuring compliance with the requirements of the Regulation and the competitiveness of enterprises, provides that in the development of standards there should be a balanced representation of interests by encouraging the participation of all relevant stakeholders. In order to facilitate regulatory compliance, the Commission should, no later than two months after the adoption of the AIA, issue the first requests for standardisation to the European standardisation organisations.[79]

At this point, it should be noted that the use of private bodies for the elaboration of standards is criticised by certain authors[80], especially when such apparently "technical" standards have an impact on fundamental values or rights. This is evident when the AIA[81] states that the Commission shall be empowered to adopt common specifications when the relevant harmonised

[74] Op. cit. Novelli C., Taddeo M., Floridi L., Accountability in artifcial intelligence.

[75] *Cit.* Ebers, M. *et alia* mention predictive accuracy, robustness and the unbiasedness of trained machine learning models as possible criteria.

[76] In the Proposed Standard Contractual Clauses for the procurement of Artificial Intelligence by public bodies, September 2023 version, Article 3 (characteristics of datasets) is exactly the same for high-risk AI systems as for all other systems. Available at https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai

[77] Recital 121.

[78] Amendments 103 to 107 concerning Recital 61 (now Recital 121).

[79] CEN (European Committee for Standardisation), CENELEC (European Committee for Electrotechnical Standardisation) https://www.cencenelec.eu/

[80] Veale M., and Borgesius F., "Demystifying the Draft EU Artificial Intelligence Act- Analysing the good, the bad, and the unclear elements of the proposed approach", *Computer Law Review International*, vol. 22, no. 4, p. 105.

[81] Article 41(1)(a)(iii).

standards do not sufficiently address fundamental rights issues. It should be recalled that high-risk AI systems or general purpose AI models which are in conformity with harmonised standards to be adopted will be *presumed*[82] to comply with the requirements[83] set for high-risk AI systems, and therefore a procedure based on internal control (Annex VI), which does not foresee the involvement of a Notified Body, will suffice to obtain conformity assessment (Annex VI). Therefore, only where harmonised standards or common specifications do not exist or have not been implemented, a conformity assessment procedure involving a Notified Body (Annex VII) will be followed. It is the providers of these systems, before placing them on the market or putting them into service, who shall ensure that they have been subject to the appropriate conformity assessment procedure[84] and, if positive, shall draw up the EU declaration of conformity[85] and affix the CE marking[86]. It goes without saying that the "self-assessment" of conformity ultimately entails fewer guarantees precisely with regard to the verification of compliance with the requirements, let us remember, for high-risk AI systems, and it would therefore be desirable that the prior conformity assessment procedure for high-risk AI systems should always be carried out by a third party other than the provider. This point has also been called for by both the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), which state [87] that, although the GDPR does not provide for an obligation to carry out a third party conformity assessment for high-risk data processing, the risks in the field of AI are not yet fully known. This is why they advocate introducing *ex-ante* third party conformity assessment in general, and not only for certain high-risk systems, as this would 'further enhance legal certainty and confidence in all high-risk AI systems'. The EDPS subsequently reaffirms[88] and adds that, taking into account the sectoral legislation applicable to the activity in the context of which the AI system will be used, the third party assessment of the high risk AI system, in order to ensure the reliability of the

[82] Article 40.1.

[83] Chapter IV.

[84] Article 43.

[85] Article 47.

[86] Article 48.

[87] EDPB-EDPS *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act),* 18 June 2021, paragraph 37. Available at https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf.

[88] *Cit.* EDPS, *Opinion 44/2023,* para. 28.

AI, will require the involvement of the supervisory authority with specific expertise in the field.

Therefore, considers that it cannot be left to the provider's discretion whether or not to submit to third party verification as has been maintained both by the Parliament[89], and by the final text. On the other hand, we also fail to understand why the reference to the existence or not of harmonised standards or common specifications is only taken into account for one type of high-risk AI systems (specifically those related to biometric identification and categorisation of natural persons) and is not taken into account in a generalised way for all of them.

In relation to the requirement for data to be complete and, as far as possible, error-free, it has become clear that the use of techniques such as differential privacy implies the introduction of noise to avoid inadvertent disclosure of sensitive data. For this reason, some authors[90] advocate that Article 10 should allow the use of these privacy enhancing techniques (*PETs*) in the data governance practices of high-risk systems. In this regard, it should be noted that the Council introduced in Recital 44 (now Recital 67) the clarification that the requirement for complete and error-free datasets should not affect the use of privacy-enhancing techniques in the context of developing and testing AI systems. In the Parliament's later version, this clarification disappeared, but it has finally been reinstated in the final text, which we believe is positive.

As discussed in the previous section, the Council introduced a first modulation of this obligation of result, not with regard to the relevance and representativeness of the data, but with regard to the requirement of error-free and the completeness of the data, by stating that "to the greatest extent possible, they shall be error-free and complete". The Parliament, for its part, validates that the data sets are "sufficiently representative", "duly assessed for errors" and "as complete as possible in view of the intended purpose", thus clearly diluting the requirement on data quality introduced by the Parliament, which is similarly taken up in the final text. In relation to data quality, as this may depend on the context, the introduction by the Parliament of such a reference to the intended purpose of the processing is welcome. This was proposed by the Norwegian government, when it recommended including in the third paragraph a reference to the purpose of processing in the sense of relating relevance, necessity, and accuracy to the purpose of processing, as the GDPR does when defining the Data Minimisation and Accuracy Principles in Article 5.1(c) and (d) respectively.

[89] Article 43(2) and Amendment 453 as regards Article 43(1)(d).

[90] Cit. Ebers, M. *et alia*.

Regarding the *presumption*[91] that high-risk AI systems 'that have been trained and tested on data reflecting the specific geographical, behavioural, contextual or functional setting within which they are intended to be used' meet the requirements laid down in Article 10.4 is, in our view, questionable. According to this presumption, it is sufficient to 'train and test' a system with such data in order to consider that the data sets used take into account 'the characteristics or elements specific to the specific geographical, contextual, behavioural or functional environment in which the high-risk AI system is intended to be used' to the extent required for the intended purpose, which seems quite different, as the intended purpose of the system must in any case be taken into account, and these characteristics or elements will therefore vary from case to case. In any case, it is a somewhat diffuse and generic presumption to infer compliance with such an important requirement as that set out in 10.4.

In addition to the substantive content, we cannot ignore that, in order to verify compliance, in this case, with the data governance requirements, it will be necessary for the competent body to have the necessary powers to carry out *on-site* and remote unannounced inspections, as well as to access training, validation, and test data and source code of high-risk AI systems. This had been requested by the EDPS[92] and proposed by the Parliament[93]. This will require that the provider, or obliged party, is in a position to provide such samples that the national supervisory authority is empowered to request. The Parliament proposed that the obliged party should retain sufficient evidence and samples to enable the authority to "reverse engineer AI systems and acquire evidence to detect non-compliance". However, the final version[94] has not adopted this wording, but states[95] that the provider shall grant market surveillance authorities full access to the documentation, as well as to the training, validation and test data sets used and including, where appropriate and subject to security safeguards, through application programming interfaces ("APIs") or other relevant technical means and tools that allow remote access. In certain cases, access to source code will be granted[96]. It is therefore clear that the provider must retain the datasets used for the development of the system[97], which is why we believe that it would have been desirable to

[91] Article 42.1.

[92] *Cit.* EDPS, *Opinion 44/2023,* para. 45.

[93] Amendment 587 introducing a new paragraph 3a) in Article 63.

[94] Article 74.5.

[95] Article 74.12.

[96] Article 74.13.

[97] Ex Article 18, technical documentation (Annex XI) must be retained for ten years in-

clearly establish such obligation in Article 10, especially in view of the presumption discussed above, although the AIA does not expressly establish it as a *rebuttable presumption*.

As regards the *sanctioning regime* in this area, the Parliament introduced important changes. The Commission and Council versions provided for the highest penalties, on the one hand, for infringements relating to prohibited Artificial Intelligence practices (Article 5) and those relating to non-compliance with data and data governance requirements (Article 10), with fines of up to EUR 30 000 000 or, if the offender is a company, of up to 6 % of the total annual worldwide turnover in the preceding financial year, whichever is higher, and on the other hand, non-compliance with the other requirements or obligations set out in the Regulation, with administrative fines of up to EUR 20 000 000 or, if the offender is a company, up to 4 % of the total annual worldwide turnover. The Parliament proposed to increase the penalties for prohibited AI practices to EUR 40,000,000 but, interestingly, to remove from that range infringements relating to Article 10, and to create a new range of penalties for breaches of data and data governance requirements and transparency obligations[98] with penalties of EUR 20,000,000 or, if the offender is a company, up to 4% of the total annual worldwide turnover in the preceding financial year. For all other infringements of certain articles, it proposed to halve the penalties. It also proposed to halve[99] infringements for submitting inaccurate, incomplete or misleading information to notified bodies and national competent authorities, which, in a system based on "self-assessment" of compliance with requirements, is of particular relevance. Finally, the most serious penalties[100] are only for infringement of Article 5 (prohibited practices) and will entail fines of up to EUR 35,000,000 or up to 7% of its total annual worldwide turnover for the preceding business year, whichever is higher. A catalogue of certain provisions, not including Article 10, is included, the

cluding (Section 1, point 2c): "information on the data used for training, testing and validation, where appropriate, including the type and provenance of data and data management methods (e.g. cleaning, filtering, etc.), the number of data points, their scope and their main characteristics; how the data were obtained and selected, and any other measures to detect inadequacy of data sources and methods to detect biases; and any other measures to detect inadequacy of data sources and methods to detect biases.), the number of data points, their scope and their main characteristics; how the data were obtained and selected, as well as any other measures to detect inadequate data sources and methods to detect identifiable biases, where appropriate'. Note that this does not refer to the totality of the datasets.

[98] Amendment 650, Article 71, new paragraph 3a.

[99] Amendment 652.

[100] Article 99.2.

infringement of which is punishable by fines of up to EUR 15,000,000 or, if the infringer is an undertaking, up to 3% of its total annual worldwide turnover in the preceding business year. Therefore, the infringement of Article 10 has gone from being one of the most serious infringements to not appearing in the sanctioning regime, perhaps by mistake as the new sanctioning range proposed by the Parliament for infringements of Articles 10 and 13 of the AIA has been deleted from the final version.

On the other hand, the penalty for supplying incorrect, incomplete or misleading information to notified bodies and national competent authorities is increased to administrative fines of up to EUR 7,500,000 or, if the offender is an undertaking, up to 1% of its total annual turnover, so the Parliament's proposal was not accepted on this point either.

It is also striking that, despite the general mandate[101] that sanctions should take particular account of the interests of SMEs and start-ups, as well as their economic viability, the Parliament proposed to eliminate the modulation of liability introduced by the Council in relation to SMEs and start-ups, establishing a lower percentage in terms of their annual global turnover in all sanctions. The final version recovers the mention[102] to SMEs and *start-ups* and includes a modulation of liability consisting of applying the percentage or the amount of the sanction, depending on which of them is lower, contrary to what is established in the general sanctioning regime, in which the higher amount should be chosen. We consider that, although the introduction of such modulation is positive, it will only benefit those SMEs and *start-ups* whose total annual turnover is very high.

Like other authors[103], we believe that a compliance system based on "self-assessment" has been constructed without the compulsory intervention of external bodies, which, together with the reduction in penalties, even for providing inaccurate, incomplete or misleading information to the notified authorities or bodies, significantly reduces the degree of legal certainty expected to be achieved with the Regulation. Even if we think of high-risk AI systems, which have gone from being a list of *numerus clausus* to, with the amendments introduced by the Council, having to meet the cumulative criterion of posing "a significant risk to health, safety or fundamental rights",

[101] Article 99.1.

[102] Article 99.6.

[103] Cit. Ebers, M. *et alia*, p. 601; Peguera Poch, M., *La propuesta de reglamento de AI: una intervención legislativa insoslable en un contexto de incertidumbre,* Chapter closed on 20 May 2023, p. 24. Published in: Peguera Poch, Miquel (coord.) "Perspectivas regulatorias de la Inteligencia Artificial en la Unión Europea", Madrid: Reus, 2023.

it is ultimately also up to the providers to determine whether or not they are dealing with a high-risk system. EBERS *et alia*[104] sums it up nicely by stating that "in contrast to the impending over-regulation attributable to the broad definition of AI, the self-fulfilment approach raises problems of under-regulation" (translation).

V. Confluence of data protection regulation

In this section we will address the connections of data governance requirements with data protection principles, as the interaction of AIA with data protection law has been dealt with at a general level in another chapter of this work by Jiménez López.

Considering that one of the legal bases for AIA is Article 16 of the Treaty on the Functioning of the European Union (TFEU), the importance of data protection regulation in AIA is beyond doubt. It should be borne in mind that many AI systems will be trained or process personal data, or will either assist individuals in making decisions or directly be able to make and execute the decision, so the GDPR will fully apply. However, the AIA does not include within its articles a general obligation to comply with data protection regulations, without prejudice to mentions of specific obligations. The closest is the requirement[105], introduced by the Parliament and taken over in the final text, that the declaration of compliance should include a statement that the AI system complies with the GDPR.

This is not a trivial issue. Not for nothing, initially, the violation of data governance requirements was set at the same sanction level as prohibited practices. At this stage, we should not start from the premise that technology is neutral, but rather the opposite, as Floridi states[106]. Even the approach to risk regulation used is not neutral[107], so both the design and the data used are absolutely relevant, as we can see in the AIA. The consequences of not having the right type of data, nor the required quality, could be disastrous, as they condition the results from the design, thus being invalid, and more importantly, could affect the fundamental rights of individuals. The relationship between the data and the AI system is therefore directly proportional to the quality of the results obtained. This is why Article 10 includes, among good

[104] Cit. Ebers, M. *et alia*, p. 601.

[105] Annex V, point 5.

[106] Op. cit. Floridi, L., "On Good and Evil…".

[107] Op. cit. Kaminski M., "Regulating the risk of AI", p. 1351.

data governance and management practices, issues related to the design of the system and the transparency and quality of the data.

The EDPB and the EDPS stated[108] that 'the proposal (for a regulation) lacks a clear link to data protection legislation'. Other authors[109] stated that the AIA 'should aim at better harmonisation and coordination with data protection law'. This problem has been partly reduced thanks to the amendments introduced in this area by the European Parliament, by positivising in the AIA the importance of compliance with data protection rules, which, although not mentioned, is not mandatory, but highlights the importance of compliance in the field of AI.

In addition, the AIA lacks any guiding principles that would guide the different obliged parties in the application of the AIA and that would govern any interpretation by legal operators. In this regard, the Parliament proposed to introduce[110] a set of general principles applicable to all AI systems which, by informing the application of the AIA, could be enforceable on all operators within its scope, as is the case with the GDPR. However, for some unknown reason, this proposal was not taken up in the final version. Among the principles proposed by the Parliament was the principle of "*Privacy and data governance*: AI systems shall be developed and used in accordance with existing privacy and data protection rules, and shall process data that meet high standards in terms of quality and integrity". This principle is evidence of the mutual conditioning between data protection law and data governance obligations.

From the point of view of data governance obligations, possible shortcomings of the current regulation have been highlighted. However, the obligations set out in Article 10 apply irrespective of whether personal data are involved or not, and without prejudice to any obligations arising from the application of the GDPR. Likewise, allowed practices by the AIA may not be feasible if they do not comply with the requirements of data protection law[111]. It is therefore clear that data protection principles will apply in any case. However, on this point the EDPB and the EDPS[112], in relation to the

[108] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council on harmonised rules in the field of Artificial Intelligence (Artificial Intelligence Act), 18 June 2021, paragraph 76.

[109] Cotino L., Castillo J.a., Salazar I., Benjamins R., Cumbreras M., Esteban A., "Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (*Artificial Intelligence Act*)", in Diario La Ley, Wolters Kluwer, 2 July 2021.

[110] Amendment 213. Article 4a:

[111] Recital 63.

[112] Op. cit. EDPB-EDPS, Joint Opinion 5/2021, para. 76.

certification scheme, proposed to include the principles of minimisation and data protection by design as one of the requirements to be taken into account in order to obtain the CE marking, due to the 'possible high level of interference of high-risk AI systems with the fundamental rights to privacy and personal data protection, and the need to ensure a high level of trust in the AI system'. A view subsequently reiterated by the EDPB.[113]

Although Article 10, and the AIA in general, do not expressly state compliance with any data protection principles, the Recitals do. Thus, Recital 67 states that, in order to facilitate compliance with data protection law, data governance and management practices should include, in the case of personal data, transparency about the original purpose of data collection. Therefore, the principle of transparency in data protection becomes a condition for complying with this requirement in data governance, and vice versa, since as the AEPD states[114] "the information available under the Transparency-AIA framework should be sufficiently complete to enable controllers and processors to fulfil their different obligations under the GDPR". Recital 69 states that 'the right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed'. Recital 67 also clarifies that the requirement for data sets to be, as far as possible, complete and error-free 'should not affect the use of privacy-preserving techniques in the context of the development and testing of AI systems' and in the same vein Recital 69, where it indicates that providers to ensure compliance with these principles may use 'technology that permits algorithms to be brought to the data and allows training of AI systems without the transmission between parties or copying of the raw or structured data themselves, without prejudice to the requirements on data governance provided for in this Regulation'.

When Article 10 requires data to be error-free and complete for the intended purpose, we understand it to refer directly to the principle of accuracy. As the AEPD states[115] "the performance of an algorithm, including Artificial Intelligence (AI) algorithms, could be compromised by the inaccuracy of the

[113] EDPS, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, 23 October 2023, paragraph 27.

[114] AEPD, "Artificial Intelligence: Transparency", 20 September 2023. https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-transparencia

[115] AEPD, "Artificial Intelligence: Principle of Accuracy in Processing", 31 May 2023 https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-principio-de-exactitud-en-los-tratamientos

input data used in the execution of the algorithm, not only by the data used in its development", which is why "it is necessary to assess the accuracy of the input data, as it could introduce biases and compromise the performance not only of the algorithm, but of the entire processing".

Therefore, controls should be put in place to prevent the input of inaccurate input data and also controls to put in place adequate safeguards in case of inaccurate data input. This is the purpose of the obligation in Article 10 to put in place appropriate measures to detect, prevent and mitigate possible biases that are identified.

Precisely to ensure the detection and correction of bias in relation to high-risk AI systems, providers of such systems are exceptionally allowed to process special categories of data provided that a number of conditions are met (i) it cannot be done using synthetic, anonymised or other data; (ii) the special categories of personal data processed are subject to technical limitations on re-use and to the most advanced security measures; (iii) they are subject to measures ensuring the security and protection of the personal data processed; (iv) they are not transmitted, transferred or otherwise made accessible to third parties; (v) they are deleted once the bias has been corrected or the personal data have reached the end of their retention period. This Article refers to the principle of lawfulness for the processing of such special categories of data. Some authors[116] argue that it is an exception to the GDPR as it constitutes in itself a basis for lawfulness. On the contrary, we understand that an adequate legitimacy basis will be necessary, firstly, because of the application of the GDPR itself and, secondly, because paragraph 5 itself, when it lists the conditions necessary for the processing to take place, expressly indicates that the provisions set out in Regulation (EU) 2016/679 (…) must be taken into account.

Therefore, the importance of the principles of data protection in relation to data governance is clear, which highlights the very important interrelation and interdependence between both regulatory frameworks. So much so that if we look at both the subjective and material scope of application of the Fundamental Rights Impact Assessment[117] which has been completely blurred to the point, in our opinion, of not being able to fulfil the purpose for which it was conceived. Data protection regulations and, especially, its principles and the Data Protection Impact Assessment, ultimately stand as the guardian of the aforementioned fundamental rights, without prejudice to the fact that the risk analysis includes them within its objective scope.

[116] Op. cit. Ebers, M. *et alia*, p. 600.

[117] Article 27.

VI. Conclusions

First. At the level of AI governance, we consider that it is necessary to establish an international governance framework. Initiatives at the level of AI regulation in different continents demonstrate the need for international regulation and, therefore, the establishment of the necessary coordination mechanisms[118]. Notwithstanding the above, Europe, aware of its shortcomings in terms of technological sovereignty and seeking to safeguard health, security and fundamental rights, has established its own AI governance framework through which it aspires to repeat the "Brussels effect" it achieved with the General Data Protection Regulation. To ensure the single market for data ('macro' level governance), it is imperative that organisations have strong data governance in place internally ('micro' level), which will also enable progress towards AI governance. It should not be misconceived that these obligations only fall on the entities that develop AI systems, but that those that design or deploy them (deployers) also have responsibilities, so that, although at different levels, it is necessary for all organisations to establish AI governance mechanisms. Governance has never been more important, not only at the implementation and management level, but it must start with the management bodies that are responsible for setting and leading the AI strategy, as well as overseeing its implementation. If we had to sum up AIA in one word, it would be "Governance". In relation to data governance we consider that a broad concept should be used, not only referring to the one set out in Article 10, but also including post-marketing monitoring[119] and, in addition, long-term monitoring to detect systemic risks in relation to the gradual erosion of institutions and social and political values.[120]

Secondly, Article 10 on data and data governance is of paramount importance. Article 10 on data and data governance is of paramount importance, as compliance with the obligations set out therein results in the availability of high quality data and thus in the proper functioning of AI systems, especially high-risk ones. It sets out the requirements ('quality criteria') that datasets used for training, validation and testing of high-risk systems must meet. It is of paramount importance to have quality data for both training and system development, otherwise both the system itself and its results may be affected, which is of vital importance when we are talking about security and fundamental

[118] Roberts, H., Hine, E., Taddeo, M. and Floridi, L., "Global AI governance: barriers and pathways forward", 29 September 2023. http://dx.doi.org/10.2139/ssrn.4588040

[119] Annex IV, 2. d) and g).

[120] Op. cit. KOLT, N., Algorithmic Black Swans, p. 37.

rights. For this reason, a robust data governance system is imperative and transcendental, both to ensure the proper functioning of the system and to demonstrate the necessary proactive accountability. Data governance obligations must necessarily be connected to the quality management system and, in particular, to the risk management system, even if this is not explicitly stated. It is true that the data governance system set up by the AIA has its own entity in a way that transcends the risk management system, but this does not imply that it is unknown to the latter. The inclusion of the express reference to Article 10 would have been desirable, both in the quality management system and in the risk analysis, not only for the sake of emphasising the importance of compliance with Article 10, but also for reasons of systematic consistency.

Third. We understand that all the circumstances are ripe for the emergence in the value chain of new figures that exclusively provide "verified" data and certify that the data comply with the established governance requirements, as well as their integrity and training ("data verifiers" or "certified data service providers"). Regulation and possible transfer of responsibility will therefore be key. We have questioned whether this model of "verified" data provision can deliver the individualised compliance with such governance requirements to which the Regulation aspires since, firstly, governance must be tailored to the context of use as well as the intended purpose of the AI system[121] and, secondly, data sets should take into account, to the extent required by the intended purpose, the characteristics or elements specific to the geographical, behavioural contextual or functional environment in which the high-risk AI system is intended to be used. It will therefore be the ultimate responsibility of the deployer to assess the appropriateness of such datasets for the use case for which the AI system will be used. In other words, the fact that new figures may enter the value chain as a result of the outsourcing of data governance requirements does not exempt the deployer (and, where applicable, data controller) from compliance with the other obligations, as "proactive accountability is a cornerstone of AI governance"[122] both proactive (*ex ante*) and reactive (*ex post*). Without prejudice to the questioning of this model, the regulation and possible transfer of liability at the contractual level will be key.

Fourth. In order to verify compliance with the data governance requirements by the competent authorities, the provider or obliged party shall retain the data sets used for the development and training of the system. This follows from the post-market surveillance measures[123] stating that "providers

[121] Article 10, second paragraph.

[122] Op. cit. Novelli C., Taddeo M., Floridi L., Accountability in Artificial Intelligence.

[123] Article 74(12).