



UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

**Rivista scientifica trimestrale di diritto amministrativo (Classe A)**

Publicata in internet all'indirizzo [www.amministrativamente.com](http://www.amministrativamente.com)

*Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"*

**Direzione scientifica**

Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

**Direttore Responsabile**

Gaetano Caputi

**Redazione**

Giuseppe Egidio Iacovino, Carlo Rizzo

**FASCICOLO N. 2/2024**

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009

ISSN 2036-7821

#### Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudia, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, José Manuel Ruano de la Fuente, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

#### Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Coccozza, Andrea Marco Colarusso, Sergio Contessa, Beatrice Coppa, Giuseppe Doria, Manuel Delgado Iribarren, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Giuseppina Lofaro, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Benedetta Piazza, Marcin Princ, Sara Pugliese, Bianca Nicla Romano, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Stefania Terracciano, Salvatore Villani.

#### Coordinamento del Comitato editoriale

Valerio Sarcone.

# The challenge of artificial intelligence for the defense of Human Rights in Europe

di Manuel Estepa Montero

(Profesor Permanente Laboral, Facultad de Derecho, Universidad Complutense Madrid)

## Sommario

1. The unstoppable development of AI; - 2. The challenges of artificial intelligence in relation to Human Rights; - 3. The deontological key in the defence of Human Rights; - 3.1. The necessary protection of Fundamental Rights ; 3.2. The ethical framework of artificial intelligence projected by the European Parliament: Artificial intelligence must have the human being as its axis; 3.3. Tools for the control of intelligent systems; - 3.4. Examination of the system of patrimonial liability; - 3.5. Reactive rights in the face of deviant development in the development, deployment and use of intelligent systems ; - 3.6. The proposed AI Law opts for a regulation focused on risk control (<<Risk Pyramid>>); - 4. Conclusions on the proposed legal framework for the protection of ffdd.

## Abstract

The development of AI seems to have definitely taken off in the 1920s. Breaking into our lives in applications such as chatbots, capable of holding a conversation autonomously to resolve customer doubts. Since 2022, the new technology has led to the release of Chat GPT on the internet by the company OPEN AI, which allows a particular and unrestricted dialogue between any individual who accesses the network and the aforementioned system; The program can analyze large amounts of data that are relevant and generate creative reports or text (such as poems or fiction) on a wide variety of topics.

*\* Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review.*

### **1. The unstoppable development of AI.**

The development of AI seems to have definitely taken off in the 1920s. Breaking into our lives in applications such as chatbots, capable of holding a conversation autonomously to resolve customer doubts. Since 2022, the new technology has led to the release of Chat GPT on the internet by the company OPEN AI, which allows a particular and unrestricted dialogue between any individual who accesses the network and the aforementioned system; The program can analyze large amounts of data that are relevant and generate creative reports or text (such as poems or fiction) on a wide variety of topics<sup>1</sup>.

AI has beneficial effects on many economic sectors: logistics (through the introduction of robots that carry out storage tasks), agriculture (through machines capable of carrying out planting, irrigation, fertilizer and pruning tasks), transport (through the figure of the car or the autonomous drone); education (present through the management of the metaverse); finance (through large-scale financial foresight applications); justice (through evidence-based systems); the environment (energy-saving applications used in industrial processes or human consumption); o health (helping with disease prediction and surgical interventions)

Given the decisive impact that new developments in AI have on our lives, one might wonder to what extent such systems can negatively condition the existence of human beings. If they were capable of relegating the person to merely auxiliary functions; taking on the bulk of intellectual activity. The answer to this crucial question requires a systematic analysis of the key elements that accompany this concept.

The most revolutionary and at the same time the most disturbing aspect of the new applications that are being built is that machines are capable of learning the knowledge and functions that are supplied to them. As a consequence, governments and society as a whole have to question themselves what are the requirements and what are the limits that can not be passed.

### **2. The challenges of artificial intelligence in relation to human rights.**

The European Commission stated, already in 2018, at the time of initially presenting its <<White Paper on Artificial Intelligence>>, that only from a joint approach of all Member States would it be possible to build a solid legal regulation in which to reflect the set of values, principles and fundamental rights that are deduced from the founding Treaties, as well as the European Charter of Fundamental Rights and the common legal tradition<sup>2</sup>. More specifically, it stated that the opportunities and risks

---

<sup>1</sup> The content of the current article is the result of the lecture that the author gave in the Department of Political Science at the University Federico II of Naples on the 13th of May 2024.

<sup>2</sup> EUROPEAN COMMISSION, White Paper on AI, an approach to building trust and excellence, 19-2-2020.



involved in the use of algorithms should be considered and addressed through a comprehensive regulatory framework at EU level containing the ethical principles to be complied with at the various stages of their existence, from the moment of their conception and deployment to their use<sup>3</sup>.

The threats posed by algorithms can affect almost all fundamental rights, directly or indirectly, since the seriousness of the risks mentioned concern the very core of human dignity, preventing the responsible exercise of those rights. The list of human rights immediately concerned highlights the radical nature of the possible attacks on human dignity. In particular, mention should be made of the right to non-discrimination in social life on the basis of race, religious, philosophical or political beliefs or sexual orientation, which is jeopardized whenever a programme restricts access or benefits through the misuse of such personal characteristics. The privacy of our lives, through possible attacks on honour, intimacy and our own image, which is perhaps the most obvious risk for the generality of people to the extent that we are all subject to the daily collection of cookies every time we enter a website or when we establish a commercial relationship with a company that could proceed to the creation of customer <sup>4</sup>profiles. Likewise, its impact on the exercise of freedom of expression and information is noticeable, since search engines can decisively influence the creation of a free public opinion (FPO) by deciding to index or prioritize certain news content over others, so that postponed news has hardly any real dissemination; and in the exercise of the freedoms of assembly and association, since the calls for meetings of participants are today made primarily through the use of the Internet if not through the most widespread social networks.

The right of access to and development of a fair trial, especially in the criminal field, is another human right that could be compromised to the extent that predictive schemes have been developed on the Internet that allow us to deduce that the owners of certain websites could be related to terrorist actions and take the corresponding criminal actions against them.

I would also like to mention possible attacks on the organization and conduct of free elections. The indiscriminate and massive dissemination of false information (*'fake news'*) reaches worrying levels as it is systematically programmed during electoral campaigns to decisively influence the shaping of the opinion of the electorate; to the point that the possible electoral outcome may vary significantly. At the same time,

---

<sup>3</sup> EUROPEAN PARLIAMENT, Resolution of 20 October 2020 on Proposal for a Regulation of the European Parliament and of the Council on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies, recital 1 (hereinafter referred to as the resolution of 20 October 2020), p. 39

<sup>4</sup> See, in this regard, J. M. MUÑOZ VELA, Challenges, Risks and Responsibility and Regulation of Artificial Intelligence, An Approach to Physical, Logical, Moral and Legal Security, Thomson-Reuters Aranzadi, 2022, Cizur Menor (Navarra), p. 64 et seq. He argues that privacy regulatory frameworks require finding a balance between regulation, innovation and competitiveness.

however, it is worrying that, in those countries whose democratic credibility is strongly questioned, remote electronic voting systems are being introduced whose processing and translation into seats lack the necessary independent external controls. This gives rise to a patent opacity that prevents the legitimacy of the electoral process from being confirmed, as has happened in the Russian Federation in the recent presidential elections held between 15 and 17 March 2024. In fact, in the previous elections to the lower house or Duma in 2021, opposition parties challenged the result of electronic voting in Moscow that gave a contrary orientation to that of voters who did so on paper<sup>5</sup>.

Human rights risks can come from failures in each and every phase of the process of creating and implementing a new AI system application.

However, special attention should be paid to the defects that may arise from a lack of sufficient transparency and reasonableness of the configurations adopted during design and execution, as they prevent timely reactions to remedy the damage that may be caused to the individual. In the same way, it is important to underline the special relevance of any deficiencies that may arise in relation to new systems that include artificial intelligence that allow the monitoring and examination of people's behaviour and actions, such as the supervision by management of the actions of a company's staff or the control of the management of the data included in the flow of information that is included in the flow of information that is carried out. maintains an institution. To the extent that, in such cases, the extent of the possible damage to fundamental rights may be relevant.

It would therefore be required that each participant in the value chain of a smart application be in a position to demonstrate that its activity has not contributed to causing the damage (the reason for its action, given that the liability is singular).

The UN links the take-off of AI systems with proper data governance. In this regard, it urges that the regulation to be adopted contemplates the full scope of activity that is carried out, encompassing both the activity of public institutions and that of digital companies in order to guarantee people comprehensive protection. The requirement of maximum transparency is proclaimed, and all persons must exercise their rights of access, deletion or erasure and rectification of their personal data. It also advocates increasing the power of existing regulatory bodies to ensure compliance through, for example, the exercise of regulatory and sanctioning powers.

However, the UN places special emphasis on the necessary prohibition of programs that involve a social categorization of individuals and those that promote massive and indiscriminate surveillance of subjects to the extent that they would directly

---

<sup>5</sup> This is how voting works in Russia: 112 million voters, three days of suffrage... and an electronic system that could lend itself to fraud, Madrid, 15 March 2024. Available at: [www.20minutos.es](http://www.20minutos.es). Editor, President by a click: electronic voting at the service of the Kremlin, Switzerland, 13 October

attack the right to human dignity, the privacy of our personal data and individual freedom, severely affecting the level of protection of human rights<sup>6</sup>.

### *3. The deontological key in the defence of human rights.*

#### *3.1. The necessary protection of Fundamental Rights*

In response to the particular problems posed by the management of AI, such as independent action, the impact on personal data, the obscurity of the process or the complexity of decision-making, the European Commission prepared a proposal on 21 April 2021 that aims to guarantee the values of the European Union (dignity, freedom, democracy, the rule of law, and fundamental rights). More specifically, it sought to mitigate the negative impact that smart systems could have on the long list of fundamental rights enshrined in the CFREU.

That position was intended, broadly speaking, to ensure a high level of protection for those fundamental rights, as well as to respond to the situation created by various potential threats by means of a methodology based on the clear identification of the risks that might arise. To that end, it was based on the desirability of establishing a series of requirements appropriate to the participation of each of the operators in the value chain in accordance with the principle of good administration; demanding, at the same time, a series of requirements.

The institutional position of the European Commission, being configured as a horizontal proposal, also extends its protective effects to fundamental rights relating to certain groups, such as the effectiveness of care and consideration of children's views (Article 24), ensuring the social and professional integration of disabled people (Article 26), the observance of workers' rights to fair and equitable working conditions that guarantee their health and rest (Article 31). It has the same impact on human rights that are held by the entire population, but in relation to the implementation of a certain public policy. I am referring to the guarantee of the health and well-being of citizens (art. 35); The right to enjoy a high level of protection of the environment and to improve its quality in accordance with the principle of sustainable development (Article 37), and also to obtain a high level of protection for individuals as consumers (Article 38).

With a view to achieving better regulation in the protection of human rights, the Council, in its resolution of 6 December 2022, adopted a common position in which it introduced significant improvements compared to the Commission's initial text by clarifying many of the requirements applicable to high-risk AI systems, such as the

---

<sup>6</sup> United Nations (UN), First Global Agreement on the Ethics of Artificial Intelligence, November 25, 2021. Available: [www.news.un.org](http://www.news.un.org)

requirement for more technical documentation or the distribution of responsibilities<sup>7</sup>. But, in addition, the Council was inclined to extend the prohibition of using AI systems for social classification to private subjects as well. In addition, it proposed the provision prohibiting the deployment of AI systems that exploit the weaknesses of a specific group of people. The use of real-time remote biometric identification systems is also restricted to the maximum, extending it to groups with social and economic weaknesses. Finally, I would like to highlight how the Council's eagerness to ensure greater coverage of fundamental rights is also reflected in the provision that the construction of high-risk AI systems will take into account the possible effects of their use on relevant decision-making. And likewise, the consideration of an intermediate category that includes those AI applications that can be classified as medium-high risk<sup>8</sup>.

### ***3.2. The ethical framework of artificial intelligence projected by the European Parliament: Artificial intelligence must have the human being as its axis.***

Within the European Institutions, it has been precisely from the European Parliament, in particular, that a consensus has been generated in relation to the idea that there is a need for a legal regulation on AI that is uniformly applied in the Member States and guarantees the validity of the values of the Union. without diminishing the provisions of sectoral standards.

The position of the human person is at a disadvantage compared to the operation of artificial intelligence technologies, so their use requires legal regulations that generate the necessary legal certainty for them to be able to establish themselves socially. This is because we are facing a series of technological advances that propose a daily relationship with the individual, interacting with him in practically all areas of his life (hence the necessary anthropocentric and anthropogenic vision). Such a guarantee can only come from a clear and harmonious, solid and comprehensible axiological normative scheme which respects, by design and by default, at the same time, the ethical normative core of the law which, as far as Europe is concerned, is constituted by the Treaties, the Charter and secondary EU law directly related to fundamental rights. It is therefore based on the adoption of a position of maximum prevention with respect to the regulation to be adopted (*precautionary principle*); so that the protection of the human person must always be present in the development of new systems; but adjusting the level of the means used to the ends to be achieved

---

<sup>7</sup> Ivan Bartoš, Czech Deputy Prime Minister for digitalisation and minister of regional development, Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights, press release, European Council, 6 December 2022. Disponibile en: [www.consilium.europa.eu](http://www.consilium.europa.eu).

<sup>8</sup> Anne Pingen, Council's Common Position on Artificial Intelligence Act, 10 January 2023. Disponibile en: [www.eurcirm.eu](http://www.eurcirm.eu).]



and requiring their correct use (*principles of proportionality and good management*). Smart applications must be operated in such a way as to ensure that the operations carried out are comprehensible to the recipient (*principle of explainability*); susceptible to possible external and independent verification and evaluation (*auditability*); being accessible to stakeholders (*transparency*). In addition, it is possible to know the totality of the procedure followed (*traceability*) and to actively give an account of what has been done by those responsible (*accountability*).

The above principles, however, are aimed at encouraging the construction, deployment and use of algorithms to be in line with the Union's set of principles and values. It is therefore necessary to affirm and guarantee the validity of a second set of general prescriptions which, on the one hand, guarantee the necessary validity of the previous ideas. And that, on the other hand, it allows, when malpractice on the part of the operators is detected, the necessary legal response from the interested party, without any contrary actions going unpunished and without compensation to the recipient. This is based on the necessary supervision by human beings of intelligent systems in their various phases (*principle of control by the person*) and the right to obtain compensation for the damages suffered (*principle of patrimonial liability*). To this end, it is necessary to arbitrate a set of mechanisms that allow legal reaction against possible breaches and injuries (*safeguards and remedies*).<sup>9</sup>

From the adoption of these principles, a series of legal consequences of the first order can be inferred, such as: it guarantees respect for the CFREU; ensures the coherence of the legal framework with the rest of the existing Community legal order; and finally, to support the take-off of new applications to lead the global market. This will ensure solid development that will facilitate business investment and the take-off of new innovative projects that will allow the growth of the domestic market by allowing legal operators to act on issues related to new technologies according to known parameters. But at the same time, having a legal model that resolves in advance the possible major conflicts that may arise will be a decisive boost to lead the world market by having an additional competitive factor against eventual competitors that move on a plane of uncertainty and whose products do not respond to a clear scheme of values with the distortions and negative effects that this can cause.

In short, there is an '*anthropocentric vision*' of AI that has the human being at its centre, being at their service and for their benefit. But, at the same time, we can speak of an '*anthropogenic perspective*' insofar as intelligent applications must be conceived as an emanation of man's intellectual capacity with a view to its empowerment which, for

---

<sup>9</sup> See EUROPEAN PARLIAMENT, Resolution of 20 October 2020 with recommendations to the Commission on the Ethical Aspects of AI, Robotics and Related Technologies Framework, p.35. Developed in subsequent resolutions such as that of March 13, 2024.

this reason, must have means in each of the phases of its useful life - from design to its application in real life - that allow him to understand it. monitor and improve it. They must empower the human person, enhancing their capacities (AI+Person orientation).

### ***3.3. Tools for the control of intelligent systems.***

The proposed AI Regulation, for its part, also includes throughout its article a whole range of instruments that seek to provide Supervisory Authorities and recipients with guarantees and rights to react to possible breaches of the requirements and obligations imposed. In this way, it is possible to identify the establishment of liability of <<high-risk system providers>> who do not comply with the requirements of harmonised Union legislation (testing processes, notification requirements, information and documentation, Art. 8). The implementation of a management system as part of the quality system referring to such AI systems, conceived as a continuous interactive process that entails periodic reviews of the algorithms throughout their life cycle, art. 9). Similarly, a system of data governance used in the training, validation and testing of such systems is envisaged, affecting decisions on the design, origin and process of data collection (art. 10). Requirement of clear, complete and up-to-date technical documentation of the RAS (Articles 11 and 13). Likewise, the provision of an automatic record of the events that occurred throughout its life, creating <<log files>> facilitating their post-marketing and operational surveillance (art. 12 and 19).

With regard to <<suppliers>>, in particular, they are required, among other measures, to draw up an EU declaration of conformity and affix the CE marking to ensure compliance with the EU AI Regulation (Articles 16, 17, 47 and 48); they must also proceed to the establishment of a quality control system. They are obliged to keep the technical documentation and the documentation of the quality system for a period of 10 years (art. 18). Particularly relevant is the recognition of a general duty to cooperate with the competent authorities, so that in the event of a reasoned request from them, they must give them access to all the necessary information and documentation, including the registry files under their control (art. 20). In addition, it envisages the establishment by providers of a post-market surveillance system appropriate to the nature of AI technologies and the risks of high-risk AI systems that actively and systematically collects, documents and analyses relevant data that are able to be provided by those responsible for deployment or that can be gathered from other sources on the operation of high-risk AI systems risk throughout its lifetime. Provision is also made for a mechanism for the exchange of information held by suppliers to the market surveillance authorities in the event of serious

incidents, which in turn must inform the Commission in accordance with Regulation 2019/1020 (Articles 72 to 74).

In the case of <<importers and distributors>>, they are required to verify that suppliers comply with their conformity assessment obligations, the CE marking and the declaration of conformity (Articles 23 and 24). Finally, as regards the <<responsible for deployment>>, in general scope, they monitor the operation of the high-risk AI system on the basis of the instructions for use and, where appropriate, inform providers (Articles 26, 72 and 79). But above all, as I have already mentioned, it highlights the provision contained in Article 27 of the proposal for a regulation that those responsible for the deployment of high-risk systems <sup>10</sup>should carry out an impact assessment on fundamental rights, obliging them to provide a general description of the deployment processes, as well as the temporal and personal scope of their application. what is the human supervision of the risks and what measures are envisaged in the event that they materialize.

#### ***3.4. Examination of the system of patrimonial liability.***

Therefore, throughout the regulation proposed by the Community institutions, a complete scheme of obligations of the different operators that will intervene throughout the life cycle of algorithmic systems is proposed. The question therefore arises as to whether we are dealing with a traditional model of subjective liability in which the operator in question only has to prove that he or she did not act with fault or negligence. On the contrary, the regulatory project adheres to the new trend in the matter represented by article 24 of the GDPR, according to which the principle of proactive responsibility governs data protection, according to which the defendant professional would have to demonstrate in any case that he or she actively complied with all the obligations that are proper to him or her to guarantee the necessary protection of the data included in the files of which he or she is a member responsible. However, the question raised does not admit of a quick answer since, although it is true that the draft AI Regulation does not proclaim the principle of proactive responsibility in its articles, it does expressly guarantee the application of the GDPR to the extent that intelligent systems affect the handling of personal data; as well as the rest of European Union law (Art. 10, on data and data governance). But the fact is that, in addition to this specific application of the GDPR in the event that AI operates on personal data, the reading of the proposed regulation reflects the imposition on the different operators (suppliers, importers, distributors, those responsible for deployment) not only of specific duties that are specified in the

---

<sup>10</sup> Those provided for in article 6.2 (those referred to in Annex III, which includes, among others, authorised biometric systems, or those relating to critical infrastructures, vocational education and training, employment, access to essential public and private services or law enforcement in the criminal field).



performance of documented procedures but also of obligations of general scope that presuppose diligence in the activity that corresponds to them (design, import, distribution, application). Thus, for example, in the case of suppliers, which is perhaps the most significant, the proposed regulation in Article 16 imposes, in general, on suppliers the obligation to demonstrate at all times, upon reasoned request from the competent authority, that their AI system complies with the prescribed requirements (adequate data governance, transparency, human surveillance, Safety, robustness and precision).

### *3.5. Reactive rights in the face of deviant development in the development, deployment and use of intelligent systems.*

Finally, I would like to highlight the need to establish legal mechanisms to ensure that citizens are able to respond to improper use of AI that has negative effects on their personal or property spheres. The person concerned, whether a natural or legal person, should have the possibility to appeal against any decision taken to his or her detriment by an artificial intelligence, robotics or related technology system which is in breach of Community or national law. A first instrument would be the possibility for consumers to request from national AI supervisory authorities the reparation of any damages in the context of the approved regulatory framework. The means of administrative appeal and, where appropriate, that of judicial protection must also always be available to citizens in order to guarantee the effectiveness of the rights that are recognized to them (individual and collective rights as consumers and users against the use of smart utilities and algorithms by public and private entities. In this regard, it underlines the relevance of the draft directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, which repeals Directive 2009/22/EC, making it possible to react to the introduction or continued use of an artificial intelligence system likely to infringe consumer rights or remedy a violation of rights. It also calls for the establishment at European level of a procedure to finance individuals' access to justice in order to guarantee the effectiveness of their violated rights.

In a context of maximum technological complexity and a high level of risk to the values of the Union and the fundamental rights of individuals, it is essential that the individual, whether as a consumer or as a citizen, has a rapid reaction mechanism, in the form of a judicial injunction or a complaint to competent market surveillance authorities in the form of an arbitration award.

In this regard, it is important to highlight how <<national public authorities or bodies responsible for supervising or enforcing Union law on the protection of fundamental rights>> (such as ombudsmen, judges and prosecutors) can request and access any legal documentation relating to such systems, informing the market surveillance

authorities of the State in whose jurisdiction it operates. They may also, when necessary, request the performance of the technical tests deemed necessary.

However, it is important to highlight that the text of the European Parliament also deals with establishing different <<remedies>> such as the possibility for any interested party to file specific complaints with the corresponding national market surveillance authorities, without prejudice to the fact that they may additionally initiate ordinary administrative and judicial remedies. It also includes the right of every person to obtain from the person responsible for deployment, unless there is a legal exception, sufficient explanations of the decisions taken individually in relation to the application of the most relevant high-risk systems initially provided for in Annex III - essential services, education, health, etc. - that may put their health, safety or fundamental rights at risk. Finally, the affected person who reports infringements of the AI Regulation may benefit from the protection granted to whistleblowers by EU Regulation 2019/1937 (information and advice, legal assistance in criminal and civil proceedings, effective assistance from the competent authorities in the event of possible reprisals, imposition of sanctions, prohibition of waiver of rights and remedies for the whistleblower).<sup>11</sup>

Transparency in the operation of intelligent systems is an essential requirement to ensure the effectiveness of citizens' reactionary measures. Consequently, the mere formal statement of reasons for the decision to be taken will not suffice; but, as I have already mentioned, a further step is required, the <<explainability of what has been adopted>>. That is, the motivation must be accompanied by a set of technical data that corroborates it (the log files).

The list of specific mechanisms for the protection of subjective rights in general and fundamental rights in particular is finally closed by the provision of a table of sanctions in response to the contravention of the main obligations established. As a general rule, the sanction provided for is a fine, although there is the possibility that warnings or other non-economic measures may be issued in minor cases. Apart from special cases, such as those imposed on EU bodies or providers of general-purpose AI models, the violation of the prohibition on the use of AI systems of unacceptable risk, in Article 5, receives the most severe response, reaching €35 million or up to 7% of the total global turnover. Violations of obligations imposed on suppliers, importers, deployers and other operators relating to high-risk systems also deserve a strong response with fines of up to €15 million or up to 3% of global turnover. While the provision of inaccurate, incorrect or misleading information to Notified Bodies

---

<sup>11</sup> See European Parliament resolution of 13 March 2024 on the proposal for an AI Regulation, Articles 82 to 85 Regulation (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who provide information on Union law, Articles 19 to 23.

and national market surveillance authorities deserves lower penalties, of up to €7 million or 1% of global turnover<sup>12</sup>.

### ***3.6. The proposed AI Law opts for a regulation focused on risk control (<<Risk Pyramid>>).***

The AI Act is based on a classification of the various AI systems based on social risk according to who their specific recipients are. Therefore, as the risk of utility in the established classification increases, the different requirements and demands that those responsible must comply with increase proportionately<sup>13</sup>.

"High-risk" AI systems are subject to a wide and detailed set of requirements that must fully ensure that their use does not cause unwanted harm to health, safety and fundamental rights (Articles 8 to 15). The obligations extend to the entire value chain (suppliers, importers, distributors, deployers or third parties) and are expressed in multiple requirements of a positive nature, obligations to do (art. 16 to 27). I would particularly highlight, with regard to the obligations imposed, the duty of those responsible for deployment to carry out an *ex ante* assessment of the possible impact that the use of those systems may have on the protection of fundamental rights in each specific situation.

Certain AI systems, on the other hand, are understood to carry "unacceptable" risks (art. 5.1) and are therefore outlawed; not being able to access the market. The list of prohibited practices contained in Title II of the Commission's proposal of 21 April 2021, which sought to encompass all AI systems whose use was considered to be contrary to the fundamental values and rights of the Union (subliminal techniques or those that exploit the vulnerability of specific groups) has now been substantially extended by the European Parliament.

Parliament also extends the consideration of <<unacceptable>> AI systems to new scenarios, such as the introduction of AI systems linked to predictive policing to carry out risk assessments of natural persons in order to assess or predict the likelihood that a natural person will commit a criminal offence based solely on the profiling of a natural person or the assessment of a natural person. the traits and characteristics of your personality. And likewise, the European Parliament categorically advocates the prohibition of the use of AI systems that facilitate facial recognition in closed environments; as well as the detection of the emotions of a natural person in the areas of border management, in workplaces and in educational

---

<sup>12</sup> See European Parliament resolution of 13 March 2024 on the proposal for an AI Regulation, Articles 99 to 101.

<sup>13</sup> European Parliamentary Research Service, Artificial Intelligence Act, Briefing, European Legislation in Progress, 14 June 2023, European Parliament, makes a detailed presentation of the risk regulation contained in the IAI.

centers; and the biometric categorization of individuals; undoubtedly because of their direct link with the exercise of the fundamental rights to honor and privacy of the individual<sup>14</sup>. An orientation, in short, that aims to project the maximum protection of the identity of the individual and of the subjective rights of which he or she is the holder. Which undoubtedly needs to be monitored and updated periodically.

The regulatory perspective of risk classification should be considered adequate since its existence constitutes a natural component of most of the technological advances that have taken place over the centuries. Consider, for example, the authorisation of operations with aerial drones in urban environments and the prohibition of their use for the transport of people.

#### *4. Conclusions on the proposed legal framework for the protection of ffd.*

1.- Artificial intelligence is currently a material field that, despite its enormous importance, lacks direct legal regulation to respond to the social, economic and technical challenges it poses.

1. The situation of the human person is one of vulnerability
2. The key objective is to have an adequate legal framework that enables the responsible use of AI
3. The absence of an AI law doesn't mean we have to start from scratch

The pyramidal nature of the law requires respect for the list of higher rules of the European and national order represented by the founding Treaties, the values and general principles that make up the common legal tradition, the Constitutions of the Member States and, of course, the declarations recognising fundamental rights and public freedoms. Therefore, there is no vacuum that leads to a disorderly advance of new applications, but rather a pending regulation that, fortunately, already has clear guidelines to follow.

#### 2.- The European Commission's perspective

1. It is based on a <anthropocentric>> view of AI
2. What is needed is a clear, axiological and comprehensible regulatory framework that respects the ethical core of European law
3. It is based on a position of maximum prevention (precautionary principle)

---

<sup>14</sup> Grapevine. the wording of Article 5(1)(d) to (g) and Article 5(2) of the 'AI Act' in the European Parliament Resolution of 14-03-2024.

Since its initial proposal of 21 April 2021, and which has been endorsed by the European institutions with legislative competence, it aims to ensure the safe use of AI that gives companies the necessary confidence so that the work of innovation and business investment is carried out properly. The legislative competence for the new legal framework is based on the provision contained in Article 114 TFEU which confers on the Community institutions the adoption of the decisions necessary to ensure the proper establishment and development of the single internal market. However, it must also be based on Articles 2 and 6 TEU (with regard to the values of the Union and the ECD)

3.- The European AI proposal, in its various versions, opts for an anthropogenic vision that favours an advance in AI adapted to the behaviour and needs of the person.

1. Applications appropriate to the level of understanding and management of citizens are needed (principle of explainability)
2. A <<AI+Person>> orientation

It encourages companies that design, build and market generative AI applications to advance and expand human capabilities and ensure that the individual has effective control over the applications they use. It is a <<person+AI>> orientation that does not threaten or generate negative effects.

The effectiveness of the legal framework designed in Europe for artificial intelligence will ultimately depend on the effectiveness of the numerous obligations that are prescribed to the different operators that have to intervene during the life cycle of each specific AI system (e.g., suppliers, importers, distributors, those responsible for deployment).

(1) Supervision of market surveillance authorities

(2) Control by national authorities in the field of fundamental rights

The mere formal motivation of the decisions is not enough, but the explanation of what has been done is required; This requires knowledge of specific technical data in each case. Ultimately, the legal framework that is designed contemplates a table of economic and other sanctions that ensure substantive compliance with the individual obligations of each participant. All of this must be carried out within a context of continuous internal control of the companies in the sector themselves, as well as supervision of their behaviour both by accredited private bodies - the notified bodies - and by the market surveillance authorities and the AI Office under the European Commission as the ultimate coordinator of the sector.

5.- The AI Law is based on a classification of the various AI systems based on the level of social risk according to who their specific recipients are. A regulatory



scheme that I believe is adequate for the purpose of approving a "*normative minimum*" that does not place an excessive burden on the functioning of the economic and social system.

At the present time, therefore, there are already significant advances regarding what should be the perspective of the issue, what the orientation to follow and what the appropriate mechanisms should be to be able to address the issue of the protection of human rights in Europe. The recent approval by the European Parliament and the Council of the Regulation on AI is a decisive step towards laying the regulatory foundations for the development of algorithmic systems, which may in any case be subject to further modifications and improvements, given the novelty of the subject and the rapid expansion of smart technology.