The European Regulation on Artificial Intelligence

A first constitutional-ethical consideration

Fereniki Panagopoulou

λογος

The European Regulation on Artificial Intelligence

A first constitutional-ethical consideration

Fereniki Panagopoulou

Logos Verlag Berlin

λογος

Fereniki Panagopoulou
Associate Professor at Panteion University
Ph.D. (Humboldt), M.P.H. (Harvard), LL.M., Ph.D. (NKUA)

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de .

Logos Verlag Berlin GmbH, 2025

ISBN 978-3-8325-6016-4

Printed on Lessebo Design Natural, 100 g/qm,
one of the most climate friendly paper qualities in the world.
Cradle to Cradle Certified® at Gold level.

Logos Verlag Berlin GmbH
Georg-Knorr-Str. 4 Geb. 10
D-12681 Berlin

phone: +49 (0)30 / 42 85 10 90
https://www.logos-verlag.com

Contents

INTRODUCTION **7**

I. General remarks 8
II. Terminology and characteristics of artificial intelligence . . 11
A. Artificial intelligence (AI) 11
B. General Purpose Artificial Intelligence (GPAI) 15
C. The parties involved 16
D. Algorithm 17
E. Distinctive characteristics of artificial intelligence . . . 18
F. Difference from human beings 21
G. The issue of the dangerousness of artificial intelligence 22
H. The use of artificial intelligence 24

GENERAL SECTION **25**

I. The adoption of the Artificial Intelligence Act and related legislation 26
II. Comparative overview of the regulation of artificial intelligence outside the EU 31
A. United Kingdom 31
B. United States of America (U.S.) 32
C. Canada 35
D. China 36
E. India 37
III. Does artificial intelligence require specific regulation? . . . 39
IV. Philosophy and objectives 42
V. Guiding principles that should govern artificial intelligence 46
A. Respect for human dignity 46
B. Privacy 47
C. Human well-being 48
D. Pluralism 48

E. Participation 48
F. Algorithmic transparency 49
G. Human control and supervision 51
H. Adaptability 51
I. Sustainability 52
J. Do no harm 53
K. Prevention and precaution 53
L. Concluding remarks 54
VI. Scope of application 55
VII. Similarities with the General Data Protection Regulation (GDPR) 62
VIII. Key pillars 66
A. General 66
B. Risk-based categorisation 66
C. Risk mitigation measures: Assessing the impact of high-risk artificial intelligence systems on fundamental rights 72
D. Specific knowledge in the field of artificial intelligence . 78
IX. Obligations of the Parties 80
A. Providers 80
B. Authorised representatives 83
C. Importers 84
D. Distributors 85
E. Deployers 85
X. Control and supervision 89
A. Union level 90
B. National level 91
C. The issue of the supervisory authority in Greece 92
XI. Penalties 98
XII. Liability 100
XIII. Entry into force 109
XIV. Concerns 111
A. List-based categorisation 111
B. Insufficient protection of rights 111
C. "Quasi-Directive" Regulation model 113
D. Multiple supervisory authorities 113
E. Lack of guidance 113

F. Extended scope 114
G. Competition with non-European systems 114
H. Extraterritoriality 114

SPECIAL SECTION:
Constitutional issues for examination 117

I. Biometric identification 119
A. Introduction 119
B. Terminology 119
C. Importance 120
D. The issue of public trust in the United States (U.S.) . . 121
E. The Union's legislative framework 122
F. The concept of publicly accessible space 126
G. The exception of national security 127
H. Concluding remarks 131
II. Employment and the workplace 133
A. General remarks 133
B. Managing employees through artificial intelligence . . 134
C. The response of the EU and national legislator 135
D. Artificial intelligence as a tool of public policy to strengthen the protection of workers 138
E. Artificial intelligence and the future of work 138
F. Concluding remarks 139
III. Artificial intelligence and democracy: Towards digital authoritarianism or a democratic upgrade? 140
A. Introduction 140
B. Risks posed for democracy 141
C. Upgrading democratic institutions 153
D. Changing representative democracy 159
E. Abstention or conditional acceptance? 164
F. Recommendations 165
G. Concluding remarks 168
IV. Artificial intelligence and education: Towards a right to digital literacy? 169
A. Introduction 169

B. European legal framework 170
C. The Greek constitutional framework 175
D. Legislative and advisory framework 177
E. Case studies 179
F. Challenges and considerations 188
G. The question of language 193
H. Concluding remarks 194
V. Applications for predicting illness and death 196
A. Introduction 196
B. Terminological clarification 196
C. History 197
D. Issues and considerations 201
E. Constitutional analysis 206
F. The European regulatory framework: Risk categorisation under the Artificial Intelligence Act 211
G. The matter of oversight 212
H. Recommendations 212
I. Concluding remarks 214
VI. Regulatory sandboxes 215
A. Introduction 215
B. Terminology 215
C. Their enshrinement in the Artificial Intelligence Act . 216
D. Rationale for the establishment of regulatory sandboxes 220
E. Regulatory sandboxes and EU innovation policy . . . 221
F. Critical assessment 224
G. Concluding remarks 227
VII. Is it necessary for the Greek revising constitutional legislator to regulate artificial intelligence? 228

CONCLUSIONS **231**

BIBLIOGRAPHY **239**

INTRODUCTION

I. General remarks

The regulation of artificial intelligence (AI) has been the subject of intense ethical, legal, technical, and theological debate and reflection. Numerous frameworks set out the fundamental principles that should govern AI. These are usually summarised as the principles of value, fairness, accountability, and transparency, but they are not limited to these: the principles of well-being, security, and sustainability are equally important.[1] All major international organisations and related NGOs have articulated the fundamental basic principles of AI in the context of soft-law instruments. Their adoption, however, was far from self-evident. The drafting process was marked by heated disagreements, particularly regarding the appropriate degree of regulatory stringency.[2] On the one hand, strict rules provide legal certainty and stability for the market; on the other, they risk stifling innovation and research. Hence the pressing need to strike a balance between these constitutionally protected, yet often conflicting goods.

The first attempt at a comprehensive, binding regulation of AI is the European Regulation on Artificial Intelligence (EU) 2024/1689 (the Artificial Intelligence Act, or AI Act). The AI Act marks an important milestone for the European Union,[3] as it is the first piece of legislation world-

[1] Christiane Wendehorst, "Art. 1," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 1.

[2] Ibid., para. 2.

[3] In the United States, the *National Defence Authorization Act for Fiscal Year 2019* preceded this development. This federal law determines the budget, expenditures, and policies of the U.S. Department of Defence. Article 238 of the Act regulates joint activities of research, development, and transition in the field of AI. The Secretary of Defence established a range of activities within the Department to coordinate efforts aimed at developing, maturing, and transitioning artificial intelligence technologies to operational use. These activities apply AI and machine learning solutions to operational problems and coordinate AI-related initiatives within the Department. No later than one year after the Act entered into force, the Secretary was required to desig-

wide that seeks to regulate a global technological challenge which, while posing risks, also creates opportunities for our societies and economies.[4]

This study provides an initial analysis of the AI Act. It is structured into four parts: the Introduction, the General Part, the Special Part, and the Concluding Remarks. The Introduction sets out the general framework of the study and provides some brief terminological clarifications. The General Part traces the legislative process leading to the AI Act and its related instruments, followed by a comparative overview of the Act. The question of the necessity of this legislation is then examined. Next, the philosophy and objectives of the legislative text are outlined, and the guiding principles that should govern AI are analysed. Then comes an analysis of the scope of its application, along with an outline of its similarities with the General Data Protection Regulation (EU) 2016/679 (GDPR). The main pillars of the AI Act are then analysed, the obligations of the parties (providers, importers, distributors, implementing bodies, authorised representatives) are identified, and the issue of control and supervision of AI at both national and supranational levels is discussed. This is followed by a systematisation of the sanctions regime and liability, along with an analysis of the entry into force of the regulatory framework. The study continues with the Special Part, focusing on key areas that raise significant constitutional concerns, such as biometric identification, labour, democracy, education, health, and innovation. A dedicated section examines whether the revising legislator should incorporate AI into the revised constitutional text. Lastly, there are some concluding remarks. The aim is to critically outline the main aspects of the new regulatory framework and to shed selective light on specific constitutional issues that call for deeper reflection.

---

nate a senior Department official with primary responsibility for coordinating AI and machine learning development and demonstration. The designated official's duties include preparing a detailed strategic plan for the development, maturation, adoption, and transition of AI technologies to operational use; accelerating AI development and deployment; governing and overseeing AI and machine learning policy; conducting studies on AI matters; and defining the concept of AI.

[4] Council of the European Union, "Artificial Intelligence Act: Council Gives Final Green Light to the First Worldwide Rules on AI," press release, May 21, 2024, https://www.consilium.europa.eu/el/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai

Part of this work draws on, and significantly extends, my earlier study titled "The European Artificial Intelligence Act (AI Act): An initial constitutional-ethic reflection", published in epoliteia.

Warm thanks are expressed to Georgios Yiannopoulos, Professor of Law at the School of Law of the University of Athens; Emmanouil Bouyakiotis, Lawyer and Stefanos Vitoratos, Lawyer, for the highly constructive dialogue we had.

Sincere thanks are also extended to Dimitra Nassibian for her excellent editorial assistance, and to Volkhard Buchholtz for hosting this study with Logos Verlag Berlin, as well as for our excellent collaboration.

II. Terminology and characteristics of artificial intelligence

A. Artificial intelligence (AI)

According to Recital 4 of the Regulation, "AI is a fast-evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial outcomes, for example in healthcare, agriculture, food safety, education and training, media, sports, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, the conservation and restoration of biodiversity and ecosystems and climate change mitigation and adaptation".

According to Article 3(1) of the Regulation, 'AI system' means a machine-based system that (...) for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Moreover, in the everyday use of AI, irrespective of the specific purpose, numerous legal issues arise which can be resolved independently of the definition adopted. This is because the regulation of AI is addressed primarily to AI providers, namely, the manufacturers, developers, and distributors of AI applications.[5]

AI is the field of computing concerned with designing and implementing systems that emulate aspects of human intelligence, such as

[5] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 6.

learning, adaptation, inference, contextual understanding, and problem-solving, and so on.[6]

Machine learning was first conceived by the British mathematician Alan Turing.[7] During World War II, Turing built a machine designed to decode German messages. He later devised another mechanism, which was named in his honour the 'Turing machine'. The machine in question was simple in its design, yet capable of performing any computation. Its creation gave rise to the question of whether a machine could think like a human being. If the answer were affirmative, a further question would arise: to what extent could human thought be controlled or determined? Turing proposed a simple test, based on a game known as 'the imitation game', played by three participants who do not know each other. Two of them, called the witnesses, are a man and a woman, while the third assumes the role of the interrogator. The third player, the so-called interrogator, must determine the gender of each participant without seeing them, relying only on their written answers. The players must try to prevent the interrogator from guessing their gender. The entire game is played, as mentioned, without the aid of external clues such as appearance or vocal characteristics. For that reason, communication takes place via teletypes, revealing only the internal element of communication (the content) and not the external traits of the players (their personal attributes). Turing then replaced one of the human players with a computer. The goal of the game was no longer for the interrogator to identify the players' gender, but to distinguish the human from the machine. If the interrogator could not tell the machine from the human, then the machine had successfully passed the test. This test was regarded as a reliable criterion for identifying human-like thought in a computer, and constitutes the famous Turing Test, which is a way to determine whether a machine, lacking human appearance, could produce speech resembling that of an average person in comparable circumstances. Such a machine could take part in human conversations as if it were a person. According to Turing himself, when computers win the imitation game, they do

[6] John McCarthy, *What is Artificial Intelligence?*, November 12, 2017, http://www-formal.stanford.edu/jmc/whatisai/node1.html

[7] "Turing Machine," Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/turing-machine/

so because humans have programmed them to do so. Humans, on the other hand, take part in the game without having been programmed by any designer.[8]

John McCarthy is also one of the fathers of AI. A pioneer in artificial intelligence, computer science, and interactive computing, he coined the term "artificial intelligence" in 1955. Among his most significant contributions was the development of a programming language designed specifically for AI research, which went on to become one of the field's most influential. AI is a branch of computer science concerned with equipping machines with capabilities that require mental functions similar to those of humans.[9] These include abilities such as reasoning, learning, and self-correction. The aim is to develop computer systems capable of autonomously solving complex problems. It is in this context that the term "artificial intelligence" was coined to encompass computer applications that could imitate specific areas of human knowledge and experience.[10] AI seeks to understand specific areas of human thought and mimic them.[11] It should be noted that the more accurate term is "computational intelligence", as intelligence itself cannot be technologised.[12]

AI differs from conventional software primarily in its ability to solve problems autonomously, to learn and analyse, to adapt to new situations, and to perform more complex tasks not precisely defined by programmers. The basic premise of AI is that intelligence, but not "self-awareness", is independent of the medium in which it is expressed and can therefore be implemented in computers.[13]

---

[8] A. M. Turing, "Computing Machinery and Intelligence," *Mind* 59, no. 236 (1950): 442.

[9] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 1.

[10] Giorgos Giannopoulos, *Introduction to Legal Informatics* (Athens: Nomiki Vivliothiki, 2018), 218.

[11] Ibid.

[12] Fereniki Panagopoulou and Metropolitan of Mesogaia and Lavreotiki Nikolaos (Chatzinikolaou), "Ethical, Philosophical, and Theological Approaches to the Impact of Artificial Intelligence on Human Life," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 549 ff. (563).

[13] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 1.

AI refers to systems that exhibit intelligent behaviour by analysing their environment and taking steps, with a certain degree of autonomy, to achieve their objectives.[14] In this sense, AI systems are designed by humans and are capable of perceiving and interpreting data from their environment, making optimal decisions, and reproducing human cognitive functions, such as learning, planning and decision-making.

The discipline of AI engages all five human senses and encompasses various approaches and techniques: (a) machine learning, including deep learning and reinforcement learning; (b) machine reasoning, covering design, programming, knowledge representation and reasoning, search, and optimisation; and (c) robotics, which involves control, perception, sensors, and actuators, as well as the integration of all these techniques into cyber-physical systems.[15]

AI contrasts with human intelligence, as it does not originate from living beings.[16] In reality, it constitutes automated decision-making without human mediation, through sequences of logical operations derived from machine learning or deep learning. Machine learning is divided into supervised and unsupervised. In the first case, algorithms are "trained" to draw conclusions based on data provided by their programmers.[17] By contrast, in unsupervised machine learning, algorithms have not been trained and are left without guidance in drawing conclusions.[18] This in-

[14] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe*, COM(2018) 237 final, Brussels, April 25, 2018.

[15] High-Level Expert Group on Artificial Intelligence, *A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines* (Brussels, December 18, 2018), https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

[16] Konstantinos N. Christodoulou, "Legal Issues Arising from Artificial Intelligence," in *Law and Technology: 22nd Scientific Symposium of the University of Piraeus and the Hellenic Court of Audit, 28–29 March 2019*, ed. Kornilia Delouka-Igglesi, Anna Ligomenou, and Aristea Sinanioti-Maroudi (Athens–Thessaloniki: Sakkoulas, 2019), 117 ff.

[17] ICO, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (2017), 7, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[18] Ethem Alpaydin, *Introduction to Machine Learning* (Cambridge, MA: MIT Press, 2020).

volves the capacity for efficient action with little or no supervision.[19] It is important, however, to emphasise the following: (a) machines do not act independently (though they may give the impression of doing so), but mimic human behaviour;[20] (b) the knowledge base is the result of human effort; (c) machines do not learn on their own: they are guided by us; and (d) they do not display discriminatory behaviour on their own (for example, on the basis of race, ethnicity, or gender), but reproduce patterns of human behaviour which they copy.[21]

B. General Purpose Artificial Intelligence (GPAI)

According to Article 3(63) of the Regulation, a General Purpose AI (GPAI) model is defined as an AI model trained on very large volumes of data using self-supervision at a scale that demonstrates significant generality. Such a model can competently perform a wide range of discrete tasks, regardless of how it is brought to market, and may be integrated into a variety of downstream systems or applications. This definition does not cover AI models used, prior to market release, for research, development, or prototyping activities.

A GPAI system is an AI system based on a GPAI model that has the potential to serve a variety of purposes, both for direct use and for integration into other AI systems.

GPAI systems may be used as, or integrated into, high-risk AI systems. GPAI models that do not pose systemic risks will be subject to limited requirements, for example on transparency, whereas those that do pose systemic risks will be required to comply with stricter rules. GPAI systems, unlike task-specific AI systems, do not have a single specified purpose of use. For example, a single bot could be used to generate both love poems

[19] Giorgos Giannakopoulos, *Artificial Intelligence: A Discreet Demystification* (Athens: Ropi, 2020), 129.

[20] Georgios I. Zekos, *Internet and Artificial Intelligence in Greek Law* (Athens–Thessaloniki: Sakkoulas), 73.

[21] Georgios Giannopoulos, presentation at the webinar of the European Laboratory of Bioethics, Technoethics and Law on Artificial Intelligence, May 16, 2022, https://bioethics.panteion.gr/webinar-%cf%84%ce%b5%cf%87%ce%bd%ce%b7%cf%84%ce%ae%cf%82-%ce%bd%ce%bf%ce%b7%ce%bc%ce%bf%cf%83%cf%8d%ce%bd%ce%b7%cf%82/

and hate speech. The system can be likened to digital plasticine: from the same raw material one can fashion outputs of very different risk profiles, depending on how it is used. From the same digital plasticine, one could fashion a harmless toy water pistol, or, if adapted maliciously, something far more dangerous.[22]

C. The parties involved

According to Article 3(3-8), the parties involved are defined as follows:

'Provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

'Deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

'Authorised representative' means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.

'Importer' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

'Distributor' means a natural or legal person in the supply chain, other than the provider or the importer that makes an AI system available on the Union market.

'Operator' means a provider, product manufacturer, deployer, authorised representative, importer or distributor.

[22] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 7.

D. Algorithm

The word algorithm derives from the Persian mathematician Muhammad ibn Mūsā al-Khwārizmī, who lived around 825 A.D. The Latin form of his name, Algoritmi, gave rise to the term algorithm.[23] Some algorithms have existed for thousands of years.[24] An algorithm[25] is a finite sequence of actions[26], strictly defined and executable within finite time, aimed at solving a problem. It consists of operating rules for solving a problem through a finite number of steps.[27] It is a set of predefined rules that must be applied in a specific sequence to solve a problem.[28] For example, tying a tie or solving a Rubik's cube requires a finite sequence of actions. Solving a problem requires not only identifying a logical procedure but also seeking the method that minimises cost in terms of time and resources.[29] The sequence of actions leads to the desired result. The sequence is not necessarily unique, since there are multiple ways to tie a tie or solve the cube. The term algorithm survived for a thousand years as a rare expression, meaning a systematic process of numerical manipulation.[30] In short, it is a rule-based process.[31]

---

[23] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 38.

[24] *Introduction to the Principles of Computer Science*, available at https://ebooks.edu.gr/ebooks/v/html/8547/2716/Plirofo riki_B-Lykeiou_html-empl/index2_2.html

[25] On the concept of the algorithm, see in detail Chryssoula P. Moukiou, *Algorithms and Administrative Law* (Athens–Thessaloniki: Sakkoulas, 2025), 1 ff.

[26] Leonidas Kanellos, *Applications of Artificial Intelligence in Law and Judicial Practice* (Athens: Nomiki Vivliothiki, 2021), 50.

[27] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 33.

[28] Matina Giannakourou, "The Regulation of Algorithmic Labour Administration in the Draft Legislative Initiatives of the EU: Quo vadis, Europa?," in *Artificial Intelligence and Labour Law*, ed. Matina Giannakourou and Christina Deliyianni-Dimitrakou, *Labour Law Review* (2023), 645 ff. (648).

[29] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 59.

[30] *Introduction to the Principles of Computer Science (2nd Lyceum) – Student Book (Enriched)*, available at https://ebooks.edu.gr/ebooks/v/html/8547/2716/Plirofo riki_B-Lykeiou_html-empl/index2_2.html

[31] Manolis Andriotakis, *Artificial Intelligence for All* (Athens: Psychogios, 2022), 27.

An algorithm may use AI techniques and therefore fall within the scope of the AI Act, but if it does not act autonomously and lacks adaptability, it will not fall within that scope. Often, linear algorithms do not fall under the definition of AI.

One of the most significant issues associated with algorithms is bias. Biases may arise from many factors, including social environment, education, experience, and statistics.[32] Women, for example, are underrepresented in computer science research teams and tend to be perceived as research team secretaries rather than full members.[33] Similarly, algorithms may suggest higher insurance premiums for people of colour than for white people, on the basis that, on average, they have lower incomes, drive older cars, and thus pose higher costs to insurers.[34] This, however, is not a valid reason to treat such a trend as a systematic condition applying to every person of colour.[35] A potential solution would be the development of algorithmic observers, designed to assess the validity and representativeness of the data.[36]

E. Distinctive characteristics of artificial intelligence

It follows from the above that AI is a distinct, autonomous technology, largely dependent on the boundaries set by its developer. On a certain level, AI may be compared to an animal whose nature cannot be fully controlled.[37]

Given that the AI Act is very recent, that the necessary experience has not yet been acquired, and that case law and interpretative guidelines are still lacking, it is not entirely clear what does and does not fall within the concept of AI under it.[38] Notwithstanding the above, if one were

[32] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 138.
[33] Ibid.
[34] Ibid., 139.
[35] Ibid.
[36] Ibid., 154.
[37] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 6.
[38] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 6.

to identify the building blocks of AI under the AI Act, these would be autonomous operation, adaptability, learning, inference, and contextual understanding. A consequence of autonomy is unpredictability.[39]

The difference between algorithms and AI lies mainly in autonomy, inference, and adaptability.[40] This means that a predefined algorithm lacks autonomy and adaptability and does not generate inferences. By contrast, AI can operate on the basis of imprecise rules, adapt, evolve, and develop autonomously, setting its own operational goals and the means for achieving them.[41] The inference mechanism relies on the knowledge base, applying the facts to the rules in order to draw conclusions.[42] A classical algorithm is predictable and mechanical, executing the precise instructions programmed into it without any possibility of deviation.[43] By contrast, AI does not operate on predefined rules, but relies on learning mechanisms and systems that adapt to data. An algorithm is a precise step-by-step procedure for solving a problem or performing a task, such as tying a tie.[44] By contrast, AI relies on algorithms for its operation but uses them to learn and make decisions. An algorithm is a strictly defined sequence of instructions, executed in a predictable manner. Although AI relies on algorithms, it goes beyond them, as it can adjust its behaviour without explicit instruction. In other words, the algorithm executes, whereas AI evolves.[45]

According to Christos Papademetriou: "[...] AI is not algorithms [...] the usage is common, but it is inaccurate. An algorithm is something else: it is something we have programmed, corrected, tested, and essentially we know how it works and can more or less predict it. AI is something

[39] Roman Yampolskiy, *Artificial Intelligence: Inexplicable, Unpredictable, Uncontrollable* (Athens: Epikentro, 2024), 33.

[40] Giorgos Giannakopoulos, *Artificial Intelligence: A Discreet Demystification* (Athens: Ropi, 2020), 128.

[41] Spyros Vlachopoulos, *The Selfish Gene of Law and the Law of Artificial Intelligence* (Athens: Eurasia, 2023), 89.

[42] Giorgos Giannopoulos, *Introduction to Legal Informatics* (Athens: Nomiki Vivliothiki, 2018), 218, op. cit.

[43] Panagiotis Soilentakis, *Artificial Intelligence at the Core of Constitutional and Administrative Law* (Athens: Nomiki Vivliothiki, 2025), 31.

[44] Ibid.

[45] Ibid.

far more elusive and unpredictable, more organic. It is an artefact that we have exposed to an astronomical number of experiences, which have subtly reshaped its inner workings in the process of adaptation. And of course, it reproduces the flaws of our culture, since it was trained on it".[46]

In this context, autonomy in AI lies in the ability of a programme to act without human intervention. This action does not consist of carrying out a task assigned by the user, but of altering the instructions originally given by the programmer in order to complete it.[47]

A typical example is the traffic light that regulates traffic without human intervention. A conventional traffic light will alternate between red and green as programmed, for example two minutes green, half a minute red. At certain junctions and times of day this works well, but when conditions change it frustrates drivers, with short green lights at rush hour or standstills despite the absence of traffic.[48] This may irritate some drivers, but the technology behind such lights is not dangerous; it merely enforces rules set by humans.[49] By contrast, an autonomous traffic light system can change its operation without human intervention and adapt to actual traffic volume. It could, for example, recognise that pedestrians with children need more time to cross, or that the braking distance of a 16-tonne lorry requires the red light to be activated earlier than for a moped. The technological advantage expected from such systems is the automated personalisation of services.[50] If it determines on its own when to activate the red and green lights, we are dealing with AI. If, by contrast, it has merely been trained to stop when it detects a parent with a baby, then it is acting non-autonomously on the basis of human instructions, and we are not dealing with AI.

AI systems are often described as a black box, reacting and communicating in ways that resemble human behaviour. This is precisely the

[46] Sofia Christou, "Christos Papadimitriou in *Kathimerini*: 'Archimedes Is in Danger,'" *Kathimerini*, July 10, 2025, https://www.kathimerini.gr/opinion/interviews/563640649/christos-papadimitrioy-stin-k-o-archimidis-vrisketai-se-kindyno/

[47] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 16.

[48] Ibid.

[49] Ibid.

[50] Ibid.

aim of modern AI tools: to appear "creative" and generate "new" content. There are various types of AI systems, but most share the feature that – with few exceptions – they are controlled by textual commands, known as prompts. Some AI tools generate text, others create images, some "compose" music, and others produce video, among other outputs. Meanwhile, multimodal systems already exist, such as ChatGPT-4.[51] Such systems can process not only text, but also voice commands, and can even interpret visual content. Moreover, they can generate not only text but also images and other forms of media.[52]

Expert systems that merely compare patterns, without being designed for autonomous operation and adaptability, do not fall within the scope of the AI Act. Any system that cannot adapt on its own does not fall within the scope of AI law. Classic examples of non-autonomous systems include corporate tools for assessing contracts according to defined specifications (for example, checking which contract is subject to limitation) and the AI system used in the land registry. Other systems monitor purchasing behaviour to optimise inventory management. In the field of medicine systems can assist in indicating whether an intestinal abnormality or a skin lesion is benign. In this case, the requirements of the GDPR on the obligation of human intervention under Article 22 in automated individual decisions apply, but the AI Act does not.[53]

F. Difference from human beings

AI applications possess vast reserves of knowledge, enabling them to support humans in solving complex problems and making significant decisions for the future of a country and the planet.[54] Due to rapid advances

[51] This is the fourth generation of OpenAI's software, which has analysed vast amounts of information from across the Internet in order to determine how to generate text resembling human writing and to provide users with detailed answers to questions.

[52] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 7.

[53] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 6.

[54] Prokopios Pavlopoulos, "'Dilemmas' of Legal Science in the Context of the Challenges of Artificial Intelligence," https://www.constitutionalism.gr/dilimata-tis-nomikis-epistimis-stis-prokliseis-tis-ai/

in their programming, they may even surpass human beings.[55] In this context, "it is relatively easy to make computers perform well on intelligence tests or in chess matches, but difficult, if not impossible, to endow them with the sensory and motor skills of a one-year-old child".[56] Even so, the transition from AI to "artificial consciousness" remains impossible.[57] In the absence of artificial consciousness, AI can function only in a subsidiary role and within defined limits,[58] and always under human supervision. An algorithm will never fully understand a human being, as it has no access to the subconscious.[59]

At the end of the day, AI differs fundamentally from human intelligence: human intelligence lies in the capacity to learn and comprehend,[60] whereas AI lies in the ability of machines to perform tasks that, if carried out by humans, would require the exercise of intelligence.[61]

G. The issue of the dangerousness of artificial intelligence

The risk posed by AI is assessed on a case-by-case basis. The technology in question carries both benefits and risks.[62] For instance, a translation tool

[55] Ibid.

[56] Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, trans. Giorgos Nathanael (Athens: Kritiki, 2016).

[57] Prokopios Pavlopoulos, "'Dilemmas' of Legal Science in the Context of the Challenges of Artificial Intelligence," https://www.constitutionalism.gr/dilimata-tis-nomikis-epistimis-stis-prokliseis-tis-ai/; and idem, "Critical Reflections on the Relevance of Aristotle's Positions on Law and Justice in the Age of Artificial Intelligence," *Public Law Review* 1 (2025): 41 ff. (51).

[58] Prokopios Pavlopoulos, "'Dilemmas' of Legal Science in the Context of the Challenges of Artificial Intelligence," https://www.constitutionalism.gr/dilimata-tis-nomikis-epistimis-stis-prokliseis-tis-ai/

[59] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 198.

[60] Michael Negnevitsky, *Artificial Intelligence: A Guide to Intelligent Systems*, 3rd ed. (Boston: Addison Wesley, 2011), 1.

[61] Max Tegmark, Rob Shapiro, et al., *Life 3.0: Being Human in the Age of Artificial Intelligence* (New York: Vintage Books, 2018), 50–51.

[62] Kyriakos Pierrakakis, introduction to Manolis Andriotakis, *Artificial Intelligence for All* (Athens: Psychogios, 2022), 9.

can generally be very useful for translating a restaurant menu. If, however, the translation is incorrect, a customer may consume something to which they are allergic and suffer harm. Translation for tourist purposes is largely harmless, but if it is carried out on behalf of a court[63] for certificate verification, human oversight is essential.[64] Similarly, the use of AI is harmless when generating a shopping list based on a buyer's preferences but becomes risky when applied in education (for example when assessing trainees) or employment (such as in recruitment processes). Beyond education and employment, AI poses particular risks when applied in health, justice[65] and electoral processes.

The boundaries between beneficial and harmful uses of AI are often blurred. Consider, for example, an application that can identify why a newborn is crying. At first sight this seems highly useful, yet it raises a dilemma: should a device intrude into the parent–child relationship, or is it preferable for parents to turn to their own child rather than a machine?[66]

The danger of AI lies in three important capabilities that merit special attention:

(a) Its ability to programme, reproduce, and improve itself.

(b) Its access through the internet to virtually all services across the globe.

[63] With Decision 13/2024, the HDPA imposed on the Ministry of Migration and Asylum a fine of €175,000 for the Centaur and Hyperion systems. Two years earlier, the NGO Homo Digitalis, in collaboration with civil society organisations (the Hellenic League for Human Rights and HIAS Greece) and Niovi Vavoula, had filed a complaint against the Ministry for these systems in reception and accommodation centres for asylum seekers. Source: https://homodigitalis.gr

[64] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 9.

[65] Ibid., 10.

[66] Giorgos Giannakopoulos, *Artificial Intelligence: A Discreet Demystification* (Athens: Ropi, 2020), 39.

(c) Its capacity to communicate with other AI systems, exchange information, and upgrade itself through new algorithms.[67]

H. The use of artificial intelligence

In the same context, AI can be used to serve both beneficial and harmful purposes. Examples of beneficial uses include text generation, customer service, website design, and word processing, while harmful uses include cyber-attacks, the creation of autonomous weapons,[68] data harvesting, the spread of disinformation, and manipulation, among others.[69] Numerous anxieties and dystopian scenarios surround AI.[70] Assessments of AI use range from viewing it as "the solution to all our problems" to predicting that it "will lead to humanity's destruction". Neither extreme is accurate; as is often the case, the truth lies somewhere in between.[71]

[67] Metropolitan of Mesogaia and Lavreotiki Nikolaos, "Bioethical Approaches to the Impact of Artificial Intelligence on Human Life," https://bioethics.panteion.gr/dimosieyseis/.

[68] On autonomous weapons and the challenges and perils that come along see Nigel Biggar, "An Ethic of Military Uses of Artificial Intelligence: Sustaining Virtue, Granting Autonomy, and Calibrating Risk," *Conatus – Journal of Philosophy* 8, no. 2 (2023): 67–76, https://doi.org/10.12681/cjp.34666; also, Joshua M. Hall, "Just War contra Drone Warfare," *Conatus – Journal of Philosophy* 8, no. 2 (2023): 217–239. https://doi.org/10.12681/cjp.34306; and Ioanna K. Lekea, George K. Lekeas, Pavlos Topalnakos, "Exploring Enhanced Military Ethics and Legal Compliance through Automated Insights: An Experiment on Military Decision-making in Extremis," *Conatus – Journal of Philosophy* 8, no. 2 (2023): 345–372, https://doi.org/10.12681/cjp.35213, as well as Ashley Roden-Bow, "Killer Robots and Inauthenticity: A Heideggerian Response to the Ethical Challenge Posed by Lethal Autonomous Weapons Systems," *Conatus – Journal of Philosophy* 8, no. 2 (2023): 477–486, https://doi.org/10.12681/cjp.34864

[69] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 19–20.

[70] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 3.

[71] Ibid.

GENERAL SECTION

I. The adoption of the Artificial Intelligence Act and related legislation

The AI Act is a cornerstone of EU policy to foster the development and uptake of safe and lawful AI applications within the single market, ensuring respect for fundamental rights. It lays down rules intended as comprehensive legal standards for AI across all branches of law.[72] The Commission, through Thierry Breton, Commissioner for the Internal Market, tabled the proposal for the AI Act in April 2021. Brando Benifei (S&D, Italy) and Dragoş Tudorache (Renew Europe, Romania) acted as rapporteurs for the European Parliament, with a provisional agreement between the co-legislators reached on 8 December 2023.[73]

On 13 March 2024, the European Parliament adopted the AI Act by 523 votes to 46, with 49 abstentions. The European Council gave its final approval on 21 May 2024. The Regulation was published on 12 July 2024, under the title "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)".

It is an ambitious yet complex and not entirely well-crafted legislative text[74] that attempts to regulate AI and assess the risks it poses in order to

[72] Chryssoula P. Moukiou, *Algorithms and Administrative Law* (Athens–Thessaloniki: Sakkoulas, 2025), 5, 317.

[73] Council of the European Union, "Artificial Intelligence Act: Council Gives Final Green Light to the First Worldwide Rules on AI," press release, May 21, 2024, https://www.consilium.europa.eu/el/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

[74] Vasilis Tzemos, "The New Regulation on Artificial Intelligence and the Charter of Fundamental Rights of the European Union (CFR)," in *Exploring Aspects of Artificial In-*

avoid irreversible future consequences. It comprises 180 Recitals, 113 Articles, and is structured into 13 Chapters. Its complexity is evident from the 68 definitions set out in Article 3.

The AI Act applies only to fields governed by EU law and provides exceptions, such as systems used solely for military or defence purposes, and for research.

It forms part of a wider package of policy measures to support the development of trustworthy AI, which also includes the AI innovation package[75] and the coordinated plan for AI.[76] Together, these measures safeguard the security and fundamental rights of people and businesses with regard to AI. They also boost AI adoption, investment and innovation across the EU. The new rules aim to promote trustworthy AI in Europe and beyond, ensuring that AI systems respect fundamental rights, security and ethical principles and addressing the risks of very powerful and influential AI models. A central pillar is a human-centred approach to AI.[77] Algorithms may ease our lives, but they can never replace free will.[78]

To ease the transition to the new framework, the Commission put forward the AI Pact, a voluntary initiative intended to support future implementation, inviting AI developers from Europe and beyond to align with the core obligations of the AI Act ahead of its entry into force. The Commission announced that more than one hundred companies

---

telligence: Cutting-Edge Technologies as a Legislative Challenge, 2nd Interdisciplinary Conference on Law and Informatics, ed. Eugenia Alexandropoulou-Aigyptiadou, Theoharis Dalakouras, and Christos Mastrokostas (Athens: Nomiki Vivliothiki, 2025), 99 ff. (101).

[75] European Commission, "Artificial Intelligence Act: Council and Parliament Reach Agreement," press release, February 2024, https://ec.europa.eu/commission/presscorner/detail/el/ip_24_383

[76] European Commission, "Coordinated Plan on Artificial Intelligence," https://digital-strategy.ec.europa.eu/en/policies/plan-ai

[77] Chryssoula P. Moukiou, *Algorithms and Administrative Law* (Athens–Thessaloniki: Sakkoulas, 2025), 5.

[78] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 198.

are among the first signatories of the EU AI Pact and its voluntary commitments.[79]

The signatories include multinational corporations and European small and medium-sized enterprises (SMEs) spanning sectors such as IT, telecoms, healthcare, banking, automotive, and aerospace. The Pact underpins industry's voluntary commitments to begin applying the principles of the AI Act prior to its formal application and reinforces cooperation between the EU AI Office and all relevant stakeholders, including industry, civil society, and academia.

The voluntary commitments of the EU AI Pact call on participating companies to undertake at least three core actions:

(a) Develop an AI governance strategy to foster adoption within the organisation and prepare for future compliance with the AI Act.

(b) Map high-risk AI systems by identifying those that may be categorised as high risk under the AI Act.

(c) Promote AI literacy and awareness among staff, ensuring ethical and responsible AI deployment.

Beyond these core actions, more than half of the signatories also undertook additional commitments, including human oversight, risk mitigation, and clear labelling of certain types of AI-generated content, such as deepfakes. may join the AI Pact and commit to its core and additional obligations at any time prior to the full application of the AI Act.

In parallel with the AI Act, there is also at international level (UN, OECD, and so on) the Council of Europe (CoE) Framework Convention on AI (CAI – Convention on AI), which establishes the foundation for AI governance grounded in respect for human rights, democracy, and the rule of law. The Council of Europe Framework Convention on AI and Human Rights, Democracy and the Rule of Law is the first international, legally binding treaty in this field. Its aim is to ensure that all

[79] European Commission, "Over a Hundred Companies Sign EU AI Pact with Pledges to Drive Trustworthy and Safe AI Development," https://digital-strategy.ec.europa.eu/en/news/over-hundred-companies-sign-eu-ai-pact-pledges-drive-trustworthy-and-safe-ai-development

activities throughout the AI life cycle are fully compatible with human rights, democracy, and the rule of law, while encouraging progress and innovation.

Work on the Convention began in 2019, when the Ad Hoc Committee on AI was mandated to examine the feasibility of such an instrument. It was succeeded in 2022 by the Committee on AI, which drafted and negotiated the text. The Framework Convention was drafted by Council of Europe member states, with the participation of all observer states: Canada, Japan, Mexico, the Holy See, and the United States of America, together with the European Union and a significant number of non-member states: Australia, Argentina, Costa Rica, Argentina, Israel, Peru, and Uruguay. In line with the Council of Europe's tradition of multi-stakeholder engagement, 68 international representatives from civil society, academia, and industry, as well as several international organisations, were also actively involved.

Activities within the AI life cycle must comply with the following fundamental principles: Human dignity and individual autonomy; equality and non-discrimination; respect for privacy and protection of personal data; transparency and oversight; accountability and responsibility; reliability; and safe innovation

The Framework Convention covers the use of AI systems by public authorities – including private entities acting on their behalf – and by private entities.The Convention provides parties with two options for complying with its principles and obligations in regulating the private sector: parties may either accept direct obligations under the Convention or adopt alternative measures to achieve compliance, provided they fully respect their international commitments on human rights, democracy, and the rule of law.

Parties to the Framework Convention are not required to apply its provisions to activities relating to the protection of national security interests, but they must ensure that such activities comply with international law and respect democratic institutions and procedures. The Framework Convention does not apply to matters of national defence or to research and development activities, unless the testing of AI systems could affect human rights, democracy, or the rule of law. The Framework Convention establishes a monitoring mechanism, the Conference

of the Parties, composed of its signatories, tasked with assessing the extent of its implementation. Their findings and recommendations support state compliance with the Framework Convention and safeguard its long-term effectiveness. The Conference of the Parties also facilitates cooperation with stakeholders, including through public hearings on aspects of the Convention's implementation. Ultimately, the AI Act does not resolve all issues, as other legal regimes continue to apply in parallel, including data protection, labour, consumer protection, media, child protection, and intellectual property law.

The introduction of the AI Act is not without its difficulties. According to former Italian Prime Minister Mario Draghi, the AI Act is "a source of uncertainty". In his view, implementation at this stage should be paused until the drawbacks are better understood. The rules aim to regulate AI systems based on the level of risk they pose to society, ranging from limited oversight to stricter compliance requirements for high-risk systems and outright prohibitions. "The first rules, which included the ban on 'unacceptable risk' systems, were introduced without major complications. Codes of practice signed by most major developers, along with the Commission's guidelines, have clarified responsibilities. The next stage, however, which concerns high-risk AI systems in sectors such as critical infrastructure and health, must remain proportionate and continue to support innovation and development".[80]

[80] "Draghi Calls for Pause to AI Act to Gauge Risks," *Euronews*, September 16, 2025, https://www.euronews.com/my-europe/2025/09/16/draghi-calls-for-pause-to-ai-act-to-gauge-risks

II. Comparative overview of the regulation of artificial intelligence outside the EU

A. United Kingdom

The UK has distanced itself from the EU's approach to regulating AI. In its 2023 White Paper on AI regulation, the government outlined a proportionate, innovation-friendly approach designed to enable the UK to seize the opportunities of AI while addressing the risks the technology may pose. This principles-based framework is implemented through the UK's existing regulators, drawing on their expertise to foster innovation and the uptake of AI across the economy. The White Paper rests on five principles but lacks binding legislative force, as implementation is largely left to regulators, with no obligation to enforce it. In 2024, the Government published its response to the consultation on the White Paper on AI regulation. That same year, ministers asked key sectoral and cross-sector regulators to report on how they were implementing the White Paper's proposals and developing their strategic approaches to AI.

The UK Data Act, which received Royal Assent on 19 June 2025, establishes a new regulatory framework for AI and algorithmic systems through amendments to existing data protection laws. The Act imposes strict controls on significant decisions made solely by automated processing. Where algorithms process special categories of data, such as data on health, race, or biometric information, organisations must obtain explicit consent, demonstrate contractual necessity, or hold legal authority. Decisions based on recognised legitimate interests cannot be fully automated. Regardless of the legal basis, controllers must inform affected individuals, allow human intervention, and establish formal procedures for challenging automated decisions. To support AI development, the Act broadens the concept of scientific research to include technological development and demonstration, creating clearer legal bases for using per-

sonal data in model training. Further processing for research purposes is automatically deemed compatible with the original purposes. Within nine months, the government must present to Parliament an economic impact assessment and a comprehensive report on the implications of AI development for intellectual property rights, including technical standards, licensing, and enforcement mechanisms. New criminal provisions target the creation, and solicitation of creation, of AI-generated personal images without consent.

B. United States of America (U.S.)

The U.S. has also taken steps to regulate AI. The first federal AI measures were enacted either as stand-alone statutes or as AI-related provisions embedded in broader laws. Notable among these is the National Artificial Intelligence Initiative Act of 2020 (H.R. 6216), which established a U.S. AI initiative and set guidance for AI research, development, and evaluation across federal science agencies. Other Acts directed agencies to advance AI programmes and policies across the federal government, such as the AI in Government Act (H.R. 2575) and the Advancing American AI Act (S.1353). In the 117th Congress, at least 75 bills were introduced addressing AI, machine learning, or related provisions. Six of these were enacted. In the 118th Congress, as of June 2023, at least 40 AI-related bills had been introduced, none of which have been enacted.

AI-related bills have been enacted since 2015. In January 2023, the White House Office of Science and Technology Policy released the Blueprint for an AI Bill of Rights, and the National Institute of Standards and Technology issued its AI Risk Management Framework. In the summer of 2023, two broader policy roadmaps were announced, namely the SAFE Innovation Framework for AI Policy and the Blumenthal–Hawley Comprehensive AI Framework, both seeking bipartisan backing to guide future congressional action on AI. In April 2023, in a joint statement, four federal agencies emphasised that their enforcement powers apply to AI and that advanced technology is no excuse for breaking the law. At state level, Stanford University reports that between 2016 and 2022, fourteen states enacted AI-related legislation, led by Mary-

land (seven bills), followed by California (six), and Massachusetts and Washington (five each).[81]

On 30 October 2023, President Joe Biden issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. It builds on earlier initiatives, including an Order directing agencies to tackle algorithmic discrimination and voluntary commitments by major U.S. companies (Amazon, Google, Meta, Microsoft, OpenAI) to deploy AI safely, securely, and responsibly.

The Order spans eight policy areas:

First, it focuses on new standards for the safety and security of AI. For example, developers of the most powerful AI systems must share safety-test results and other critical information with the U.S. government. Government agencies are tasked with developing standards, tools, and tests to help ensure that AI systems are secure and reliable. New standards will address the risk of using AI to create dangerous biological materials and protect U.S. citizens from AI-enabled fraud and deception.

Second, the government will launch an advanced cyber-security programme to develop AI tools that identify and remediate vulnerabilities in critical software. The National Security Council and the White House Chief of Staff have been tasked with developing a national-security memorandum to guide further action on AI and security.

Third, to protect privacy from AI-related risks, the Order prioritises federal support for privacy-preserving techniques, strengthens related research and technologies, requires agencies to assess how they collect and use commercially available data, and calls for guidelines to evaluate the effectiveness of privacy-preserving methods.

Fourth, to promote equity and civil rights, the Order calls for clear guidance for homeowners, federal benefit programmes, and federal contractors; measures to address algorithmic discrimination; and best practices to ensure fairness across the criminal-justice system. It also seeks measures to foster responsible use of AI in healthcare and to support its potential to transform education.

[81] Stanford Institute for Human-Centered Artificial Intelligence (HAI), *AI Index Report 2023, Chapter 6*, https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report-2023_CHAPTER_6-1.pdf

Fifth, to support workers, the Order calls for principles and best practices to mitigate harms and maximise benefits, and for a report on labour-market impacts with proposals for mitigation through stronger federal support.

Sixth, to promote innovation and competition, the Order aims to catalyse research nationwide, support fair, open, and competitive AI ecosystems, and attract highly skilled immigrants and non-immigrants in critical fields to study, live, and work in the U.S.

Seventh, to advance U.S. leadership abroad, the Order calls for expanding bilateral and multilateral AI commitments, accelerating vital AI standards, and promoting safe, responsible, rights-affirming AI development and deployment to address global challenges.

Eighth, to ensure responsible and efficient government use of AI, the Order seeks new agency guidelines, faster and more efficient procurement of AI products and services, and accelerated recruitment of AI experts across government.

The Executive Order was followed by detailed implementation guidance from the Office of Management and Budget.

In 2025, 48 states and Puerto Rico introduced AI-related legislation, while 26 states adopted or enacted more than 75 new measures. Examples include:

- Arkansas enacted legislation clarifying ownership of AI-generated content, recognising either the person who provides the data or inputs to train a generative AI model, or the employer if the content is created in the course of employment. The law further requires that such content must not infringe existing copyright or other intellectual property rights.

- Montana's new Right to Compute Act sets requirements for critical infrastructure managed by AI systems. It obliges administrators to develop risk management policies aligned with defined standards, such as the latest version of the National Institute of Standards and Technology's Artificial Intelligence Risk Management Framework. It further prohibits government restrictions on private ownership or use of computing resources for lawful purposes, unless necessary to serve a compelling public interest.

- North Dakota enacted legislation prohibiting the use of AI-powered robots to monitor or harass individuals, thereby extending existing harassment and surveillance laws.
- New Jersey has adopted a resolution urging generative AI companies to make voluntary commitments to protect workers who report violations.
- New York passed a law requiring state agencies to publish detailed information about automated decision-making tools on public websites. Said law also amended the Public Administration Law to enhance employee protections, including that when an AI system is used by state government, it cannot affect employees' existing rights under a collective bargaining agreement, and that it must not lead to the replacement or loss of a job.

C. Canada

In September 2023, François-Philippe Champagne, Minister of Innovation, Science and Industry, announced the Voluntary Code of Conduct for the Responsible Development and Management of Advanced Generative Artificial Intelligence Systems (Artificial Intelligence and Data Act, AIDA). Said Code temporarily provides Canadian companies with common standards and allows them to demonstrate, on a voluntary basis, that they are responsibly developing and using AI generative systems until formal regulation enters into force. The Code, which draws on feedback from the consultation process to develop a Canadian code of practice for generative AI systems, aims to strengthen public confidence in these technologies. Under AIDA, companies are held accountable for AI activities under their control. They must implement governance mechanisms and policies that identify and address risks associated with their AI systems, while providing users with sufficient information to make informed decisions. AIDA would introduce new requirements for firms to ensure the security and fairness of high-impact AI systems at every stage of the process:

- Risk-based approach: AIDA would regulate AI systems based on their potential impact, with stricter rules for high-impact systems.

- Focus on harm prevention: It aimed to minimise the risks of harm to individuals and communities associated with AI systems.
- Accountability: AIDA would hold companies accountable for the AI systems they develop and use.
- Prohibition of unacceptable risks: It was proposed to ban certain AI applications, such as social scoring and predictive policing.
- Transparency and protection of users: AIDA emphasised transparency and the provision of sufficient information to users to enable them to make informed decisions about AI systems.

Bill C-27, which contained AIDA, was repealed following the suspension of Parliament, meaning that AIDA is not currently in force and Canada has no specific AI legislation in place.

Although AIDA is not currently applied, the Canadian government is expected to revisit AI legislation in the future, potentially incorporating some of AIDA's concepts.

D. China

On 27 August, the State Council of China released the "AI Plus" plan, designed to integrate artificial intelligence across a broad spectrum of sectors. The plan prioritises the adoption of AI in science and technology, industrial development, consumer services, public welfare, governance, and international cooperation. It sets clear milestones for AI integration in key sectors, aiming to exceed 70 per cent by 2027 and 90 per cent by 2030. By 2035, China envisions a fully intelligent economy and society.

On 22 August the Ministry of Industry and Information Technology, together with the Ministry of Science and Technology, the Cyberspace Administration of China and other agencies, issued draft AI ethics rules for public consultation.[82] The draft ethics rules apply to all AI research and development and services in China that could affect health and safety, reputation, the environment, public order and sustainability.

[82] "China Releases 'AI Plus' Plan, Rolls Out AI Labelling Law," *IAPP News*, August 27, 2025, https://iapp.org/news/a/china-releases-ai-plus-plan-rolls-out-ai-labeling-law

Developers and service providers must adhere to principles of fairness, accountability, justice, risk responsibility and respect for life and human dignity. AI projects falling under the rules must undergo ethics review, either internally by ethics committees or externally through qualified service centers. Regulators are also preparing a detailed list of high-risk AI activities, such as algorithms that can mobilize public opinion or automated decision-making systems with major safety and health implications that will require expert second-level review.[83]

Another major shift came 1 September with the rollout of China's mandatory AI labeling rules.[84] AI-generated content service providers must now clearly mark AI-generated content. Visible labels with AI symbols are required for chatbots, AI writing, synthetic voices, face generation/swap and immersive scene creation or editing. For other AI-generated content, hidden labels, such as watermarks, are acceptable. Internet platforms must act as watchdogs; if they detect or suspect AI-generated content, they must alert users and may add implicit labels themselves. Non-compliance carries serious consequences, including regulatory investigations, fines, business suspensions and revocation of business permits. In severe cases, criminal liability under the Cybersecurity Law, Data Security Law and Personal Information Protection Law may be triggered.[85]

E. India

The Data Security Board of India has issued a policy template for security, privacy, and governance of AI, which outlines requirements for organisations that use AI systems.[86] The standard covers machine learning, generative AI and agent-based AI, including autonomous systems capable of making independent decisions. Organisations are required to establish AI governance committees.

[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] Data Security Council of India, "AI Security, Privacy and Governance Policy Template," https://www.dsci.in/resource/content/ai-security-privacy-and-governance-policy-template

Key requirements include documenting data sources, model selection criteria, and validation results. High-risk applications, such as loan approval and fraud detection, must be subject to human oversight with defined intervention protocols. Organisations must implement safeguards against promptinjection, data poisoning, and unauthorised model extraction. The framework treats policies as "living documents" requiring regular updates. It distinguishes between business-facing and consumer-facing AI. Consumer applications must disclose AI interaction and provide feedback mechanisms for reporting errors or bias. For autonomous AI systems, the standard requires boundary constraints, security mechanisms, and accountability structures for emergent behaviours. It also requires monitoring for cascading failures and unintended interactions between agents. Organisations can determine which provisions apply depending on their context. The standard further includes guidance on data governance, secure deployment, access controls, and privacy protection.

III. Does artificial intelligence require specific regulation?

A legitimate question that arises is whether specific regulation is needed for AI or whether it could be addressed within the existing institutional framework. Is a new set of legal rules necessary or is the analogous application of existing legal principles and doctrine sufficient?[87] AI is regarded as the fourth industrial revolution and cannot be placed under the umbrella of existing legislation enacted for other purposes. Therefore, effective legislation is needed that (a) balances the protection of autonomy, privacy, and intellectual property with the promotion of innovation and research, the strengthening of the market, and the protection of competition; and (b) guarantees the security of AI systems. At the same time, legislation must support progress and avoid hindering it. The lawyer's position on AI, however, is somewhat uneasy, oscillating "in a pendulum between hope and fear".[88] Continuous information and strong reflexes are required to address new risks.[89] The call for "no legislation"[90] is not without problems, either, as we are not yet ready for such an approach. It is further argued that technology does not in itself change the law, but that the law changes when technology creates a powerful new economic interest.[91]

---

[87] Dimitrios Koukiadis, "The Regulatory Challenges of Artificial Intelligence and the Issue of Recognition of Personality," *Journal of Law and Technology* (2020): 17 ff. (19).

[88] Lilian Mitrou, "The Regulation of Artificial Intelligence," *Ta Nea*, January 29, 2022, https://www.tanea.gr/print/2022/01/29/greece/i-rythmisi-tis-texnitis-noimosynis/

[89] Eugenia Alexandropoulou-Aigyptiadou, *Personal Data* (Athens: Nomiki Vivliothiki, 2016), 219.

[90] Konstantinos Christodoulou, presentation at the webinar of the European Laboratory of Bioethics, Technoethics and Law on Artificial Intelligence, May 16, 2022, https://www.youtube.com/watch?v=4W3npEt_WDA

[91] Curtis E. A. Karnow, "Introduction to Law and Artificial," in *Research Handbook on the Law of Artificial Intelligence*, ed. Woodrow Barfield and Ugo Pagallo (Cheltenham, UK: Edward Elgar, 2018), xix.

If the legislator rushes to regulate, they may not be aware of all its aspects. Regulation may become uncertain if it fails to take account of the technological developments and breakthroughs occurring during the regulatory process.[92] If, on the other hand, regulation is delayed, technological developments will have overtaken it. Thus, the so-called "Collingridge dilemma" arises: legislation is precarious while the matter under regulation is still evolving. Yet once perfected, it may have permeated our lives so deeply that its consequences become irreversible and beyond regulation.[93] This problem is compounded by concern that the European Union is rushing to oppose and compete with non-European AI products, mainly from the United States and China, thereby undermining the unity of AI philosophy and technology. Europe lags behind in initiatives in this field,[94] and any overshadowing of the market by others will neutralise efforts at human-centric regulation. Emphasis must also be placed on innovation. Notwithstanding the above, non-regulation is not a solution: inclusive legislation is necessary, and that is the task of the AI Act.

Moreover, care and caution are required, since over-regulation may stifle innovation. There must be scope for unregulated but controlled experimentation to foster innovation. This is the direction in which regulatory sandboxes are moving. In this context, according to Article 57(5) of the Regulation, regulatory AI sandboxes are established to provide a controlled environment that promotes innovation and facilitates the development, training, testing, and validation of innovative AI systems for a limited period before they are placed on the market or put into service, in accordance with a specific test-bed plan agreed between

[92] Lilian Mitrou, "The 'Regulation' of Artificial Intelligence or the Collingridge Dilemma," paper presented at the 4th SciFY Academy 2020, *Artificial Intelligence: Ethics and Institutional Framework*, co-organised with the Institute of Informatics and Telecommunications of NCSR "Demokritos," June 2020, 9, https://www.iit.demokritos.gr/wp-content/uploads/2020/06/Dr.-Lilian-Mitrou-The-regulation-of-Artificial-Intelligence-or-the-Collingridge-dilemma.pdf

[93] Ibid., 7.

[94] European Commission, *Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe*, Brussels, April 25, 2018, 6, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

providers, or prospective providers, and the competent authority. Such sandboxes may also include tests under real-life conditions conducted under supervision.

In short, regulation requires careful handling, as it operates ex post, meaning after the fault has been committed, while relying on an ex-ante action.[95]

[95] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 152.

IV. Philosophy and objectives

The AI Act aims to protect fundamental rights, democracy, the rule of law and environmental sustainability, while fostering innovation and seeking to establish Europe as a leader in this field. It lays down obligations for AI based on potential risks and the level of its impact.

Indeed, the objectives of the Regulation are set out in Article 1: "The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation".

The improvement of the internal market lies in the creation of a uniform framework for AI, which would be undermined if each Member State adopted its own legislation.[96] In contrast, a single legal framework provides legal certainty and enables entrepreneurs to offer their products throughout the EU without having to adapt to the legislation of the 27 Member States.[97] At the same time, it seeks to establish uniform and high security standards, thereby strengthening trust in AI applications.

The promotion of human-centred and trustworthy AI lies in ensuring that applications serve people and are aligned with the fundamental rights and values of the EU. In essence, this means prioritising human needs, values, and ethical principles.[98] At the core of the anthropocentric theory lies the prohibition of altering the human condition.[99] In this sense, technology is not an end in itself but a means to advance

[96] Christiane Wendehorst, "Art. 1," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 40.

[97] Ibid.

[98] Ibid., para. 43.

[99] Dimitris Orfanidis, *Homo Sapiens or Cyborg Sapiens? Legal Order for the Human or the Posthuman?* (Athens–Thessaloniki: Sakkoulas, 2024), 41.

human progress, addressing real challenges on the basis of human dignity and ethical principles.[100] Therefore, AI must foster the well-being of people, protect their rights and freedoms, and improve their quality of life.[101] Improvement entails tackling social challenges, such as the provision of health, education, environmental protection, and social justice. Emphasis is thus placed on a people-centred perspective, while avoiding a technophobic stance.[102] The AI Act does not repudiate or exorcise technology.[103] In this context, the classification and assessment[104] of risks into acceptable and unacceptable risks is of paramount importance. Applications must be rejected where risks are unacceptable, while preventive measures should be taken to address those deemed acceptable, despite the inherent difficulties of classification. This, however, cannot occur in the absence of ethical debate, since it is precisely within this arena that each society concerned decides which path it wishes to follow and which to abandon among those open to it.[105]

Achieving trustworthy AI requires the creation of systems that meet ethical, legal and social standards.[106] In this sense, technology must serve human beings. Reliability has legal, ethical, technological and social dimensions.[107]

---

[100] Christiane Wendehorst, "Art. 1," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 44.

[101] Ibid., para. 43.

[102] Fereniki Panagopoulou-Koutnatzi, *Artificial Intelligence: The Path to a Digital Constitutionalism – An Ethical-Constitutional Approach* (Athens: Papazisis, 2023), 20.

[103] Fereniki Panagopoulou, "Algorithmic Decision-Making in Public Administration," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 137 ff. (176).

[104] On the concept of technology assessment, see Ismini Kriari-Katrani, *Technology and Parliament: The Institutional Role and Work of Parliamentary Committees and Technology Assessment Offices* (Athens–Thessaloniki: Sakkoulas, 2001), 11 ff.

[105] Fereniki Panagopoulou, "Algorithmic Decision-Making in Public Administration," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 137 ff. (176).

[106] Christiane Wendehorst, "Art. 1," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 45.

[107] Ibid.

Supporting innovation is of paramount importance. By establishing a clear legal framework, the market is encouraged to invest in new technology and to develop innovative ideas. Innovation will not only drive economic growth but will also establish the EU as a leader in the ethical and responsible use of AI.[108] Innovation lies in the creation of regulatory sandboxes (Article 57).

A serious question that arises for any proposed regulatory system for AI is whether it achieves a defensible integration of respect for fundamental rights with the promotion of market-driven technological innovation. This question is further complicated by the fact that there is no binary opposition between the protection of rights on the one hand, and innovation and market values on the other. This is because both technological innovation and market freedoms enjoy rights-based protection. Moreover, technological innovations and the increased wealth they generate can further support the fulfilment of other rights, such as the rights to health, an adequate standard of living, and so on.

The AI Act raises the issue of integrating rights and market-driven innovation in a particularly stark way because it uses a modified version of a typical product regulation regime to address the regulatory challenges of AI. Yet AI is not a product in the usual sense of the term; it is an amorphous and constantly evolving technology that can be incorporated into the provision of various kinds of goods and services. Moreover, the harms it poses are not limited to easily quantifiable harms to life, physical integrity, or economic interests. They also include more intangible harms, such as discrimination, invasions of privacy, and other violations of fundamental rights.

In this respect, education about AI is of utmost importance. In particular, according to Article 4, providers and implementers of AI systems must take measures to ensure, to the maximum extent possible, an adequate level of literacy in the field of AI for their staff and other persons involved in the operation and use of AI systems on their behalf. This must be done by taking into account their technical knowledge, experience, training and education, as well as the context in which the AI systems are to be used, also considering the individuals or groups for whom the sys-

[108] Ibid., para. 55.

tems are intended. Training in AI will also result in the creation of new jobs, which will address the needs of those who lose employment as a result of AI.

In this light, the main objective of the AI Act could be described as twofold. First, to establish the EU as a world-class hub for AI and, second, to ensure that citizens and businesses reap the benefits of human-centred AI, while feeling safe and protected.

At the same time, its structure is also twofold. On the one hand, it regulates AI; on the other, it categorises risks into four groups.

V. Guiding principles that should govern artificial intelligence[109]

The development of AI should be based on the following guiding principles, dictated by the ethics of responsibility.[110]

A. Respect for human dignity

AI systems must be developed in ways that respect the value of human beings and do not reduce human beings to mere instruments to serve other ends. In this respect, the protection of the value of human choice and control is of central importance.[111] A classic example of degradation is biometric monitoring, which is in principle prohibited by the AI Act as an unacceptable risk. In the same vein, AI must not be designed to manipulate individuals or influence their will. It is therefore necessary to take measures to prevent AI systems from exploiting, undermining, or diminishing people's self-determination. People must retain the power to make their own choices.[112] Furthermore, applications must not exploit the vulnerabilities of at-risk individuals, such as people with dementia. A typical example is the interaction of a patient with a robot, when the patient thinks they are interacting with a human being.[113] All these factors must be taken into serious consideration by the algorithm developer

[109] For an in-depth analysis of the principles, see *Plan for Greece's Transition to the Age of Artificial Intelligence*, 15, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[110] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility", in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (274).

[111] Ibid.

[112] Ibid.

[113] Vasileios Baros and Louis Henri Seukwa, "Article 2, Protection of Human Dignity," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 27 ff. (31).

so that the use of AI respects human dignity and does not lead to the instrumentalisation of human beings.

B. Privacy

The functioning of AI requires the collection and processing of large volumes of data that are difficult to control by the data subject. The dependence of AI reliance on data has created a critical paradox: the more data that are fed into an AI system, the more accurate its output will be, but also the greater the risk of privacy breaches[114] by malicious actors seeking to extract sensitive information.[115] In short, personal data feeds AI, which in turn generates new – and more – data.

The complexity of coexistence between an efficient algorithm, which requires a lot of data for its training, and data protection raises the question of whether existing data protection law can cope with the demands of new technologies, or whether it has become a problem in new developments. The answer to this question is complex. It is a fact that classical data protection principles tend to give priority to the good of data protection over equivalent goods of information, innovation and research.[116] For this reason, the regulation of AI requires a holistic approach that considers both data protection and the free flow of information, technology and research. Intelligent systems must not operate in a way that unlawfully interferes with the right to privacy.[117]

[114] Mousam Khatri, *Data Privacy in the Age of Artificial Intelligence (AI)*, 2023, https://www.linkedin.com/pulse/data-privacy-age-artificial-intelligence-ai-mousam-khatri/

[115] According to the Identity Theft Resource Center, in 2021 there were 1,862 data breaches, 23% higher than the previous all-time high (2017). See Cem Dilmegani, *Responsible AI: 4 Principles & Best Practices in 2024*, AI Multiple Research, 2024, https://research.aimultiple.com/responsible-ai/

[116] Fereniki Panagopoulou-Koutnatzi, "Constitutional Consideration of Law 4624/2019 on Data Protection," *DiMEE* (2019): 328 ff. (329).

[117] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility", in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (275).

C. Human well-being

AI applications should promote individual well-being, rather than human marginalisation, degradation or decline. This means that they must be recognised as a tool that supports and inspires people to improve their quality of life by making use of their unique human abilities, in the workplace, education, personal relationships, the aesthetic realm, as well as in their interaction with the state. In this sense, measures must be taken to ensure people's well-being as far as possible.[118] AI should not be seen as a means of replacing human labour with the sole aim of reducing costs. Notwithstanding the above, however, the fact that well-being is difficult to measure is a cause for concern.

D. Pluralism

The principle of pluralism in AI has three main components. First, algorithms must be trained on data that reflect the majority of the population, and not only the characteristics of a single population group. Linguistic, educational and intellectual monoculture should not be promoted. Second, the regulation of AI must take into account human rights, economic well-being, environmental protection, human security and national security, and seek to resolve any tensions between them. Third, regulatory issues must concern a wide range of disciplines, from the mathematical and physical sciences to the humanities and social sciences, since AI applications cover fields ranging from healthcare to the judicial system.

E. Participation

As AI will permeate and affect all aspects of human life, it is crucial that citizens have equal opportunities to participate in AI through access to relevant education, knowledge, technology, computational resources, and datasets. Such opportunities must exist in various areas, including in basic research related to AI, the development of AI applications, and the

[118] Ibid., 276.

use of AI in the workplace and other fields. It is also necessary that AI governance reflects the views of all stakeholders, including citizens. Despite the risk of AI misuse that may threaten democratic processes through misinformation, deepfakes, and other means, it is equally important to recognise the ability of AI tools to support democratic processes, public debate, and large-scale decision-making. The principle of participation is inextricably linked to the principle of fairness, in the sense of determining who is entitled to receive benefits and who must bear the costs of developing AI applications.[119]

F. Algorithmic transparency[120]

Algorithms, data and decision-making processes of AI systems must be sufficiently accessible to interested parties so that the functioning of AI systems is understandable, explainable, reliable, justified, and accountable.[121] This is a function of visibility and traceability of the decision-making process.[122] In this sense, the publication of the algorithm is required under the condition laid down by the legislator.[123] Transparency is essential for responsible decision-making regarding the development and implementation of AI systems, and for identifying the risks and benefits they entail.

The principle of transparency seems to be put to the test in the case of AI. The information requirements imposed by the GDPR in Articles 13 and 14 are onerous, in particular with regard to the metadata recorded in the system's database. The information provided may be incomplete, either because it is difficult to determine the purpose of the processing in advance with accuracy, or because of the technical complexity of the purpose or of the processing itself.

---

[119] Ibid.

[120] Chryssoula P. Moukiou, *Algorithms and Administrative Law* (Athens–Thessaloniki: Sakkoulas, 2025), 283.

[121] Apostolos Vorres, "Can the Algorithm Be Transparent?" in *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, ed. Lilian Mitrou (Heraklion: University of Crete University Press, 2023), 151 ff. (151).

[122] Ibid., 44.

[123] Ibid., 108, 115.

In addition to any difficulties in providing information, particular emphasis must be placed on the obligation of the controller to explain the logic applied by the AI system in the automated processing of the data, both prior to processing, in the context of informing the data subject in accordance with Articles 12 et seq. GDPR, and afterwards, when the data subject exercises the right of access under Article 15 GDPR. The purpose of providing this information is to enable the decision to be challenged.[124] This raises concerns about the actual possibility of informing the average person — whether by the controller or, more generally, by any party involved — about the functioning of highly complex information systems and AI algorithms.[125] Indeed, some AI systems have reached such a degree of autonomy that it is extremely difficult, if not impossible, for their manufacturers or operators to understand the system's operating mechanism, let alone explain it in a simple, clear, and comprehensible way to someone without the necessary technical knowledge. These are the so-called "black boxes", based on complex and constantly evolving algorithms that exceed the limits of human control.[126]

The principle of transparency is inextricably linked to the principle of explainability, in the sense that the processes of decision-making through AI must be understandable.[127] It must be possible to see and understand

[124] Ibid., 45.

[125] ICO, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (Wilmslow: Information Commissioner's Office, 2017), 19, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf; and EDPS, *Artificial Intelligence, Robotics, Privacy and Data Protection*, Room Document, 38th International Conference of Data Protection and Privacy Commissioners, October 2016, 4, https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

[126] Apostolos Vorres and Lilian Mitrou, "Artificial Intelligence and Personal Data: A Perspective under the EU General Data Protection Regulation (GDPR) 2016/679," *Media and Communication Law Review* (2018): 460 ff. (463); Agata Ferretti, Manuel Schneider, and Alessandro Blasimme, "Machine Learning in Medicine: Opening the New Data Protection Black Box," *European Data Protection Law Review* 3 (2018): 320 ff.; and Chris Reed, "How Should We Regulate Artificial Intelligence?" *Philosophical Transactions of the Royal Society A* 376, no. 2128 (September 13, 2018). https://doi.org/10.1098/rsta.2017.0360

[127] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility", in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (277).

all stages of decision-making. This is directly linked to the principle of clarity.[128]

G. Human control and supervision

Technology must not be left free, but there must be constant human supervision.[129] The ultimate responsibility lies with man. The human factor must never be eliminated. To this end, limits must be placed on the powers of AI.

It is necessary to establish oversight mechanisms to ensure that AI systems uphold the values we seek to govern their operation. Particular attention must be paid to the choice of the appropriate form of supervision, including human oversight, depending on the characteristics of the different AI systems and their field of application. In addition, it is necessary to weigh the risks and benefits associated with them. Nevertheless, supervision is not without problems, as the question arises whether humans can safely maintain control while benefiting from a higher form of intelligence.[130]

H. Adaptability

AI is a multidimensional and constantly evolving technology, which requires an equally detailed and dynamic policy for its management. Such policy must adapt to new opportunities and challenges that arise over time, while maintaining a stable and predictable regulatory environment. International multilateral cooperation: effective regulation of AI cannot be achieved through the efforts of a single state alone. It is therefore crucial for Member States to participate in and contribute to international initiatives, and to draw lessons from the policy pro-

[128] Chryssoula P. Moukiou, *Algorithms and Administrative Law* (Athens–Thessaloniki: Sakkoulas, 2025), 77–78.

[129] Spyros Tassis, "Can the Algorithm Be Ethical?" in *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, ed. Lilian Mitrou (Heraklion: University of Crete University Press, 2023), 35 ff. (58 ff.).

[130] Roman Yampolskiy, *Artificial Intelligence: Inexplicable, Unpredictable, Uncontrollable* (Athens: Epikentro, 2024), 22.

posals of other states, regional bodies and international organisations. International cooperation within the European Union (EU), the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD) is vital to ensure that AI is developed and applied in ways that promote the common good of humanity.

I. Sustainability

The rapid development and widespread deployment of powerful generative AI models have environmental consequences, such as increasing electricity and water consumption. The excitement surrounding the potential benefits of AI, from improving worker productivity to advancing scientific research, is hard to ignore. While the explosive growth of this new technology has enabled the rapid development of powerful models across many industries, the environmental consequences of this "golden age" remain difficult to determine.

The computing power required to train generative AI models, which often have billions of parameters, such as OpenAI's GPT-4, can demand vast amounts of electricity, leading to increased carbon emissions and pressures on the power grid.

Moreover, deploying these models in real-world applications, enabling millions of people to use generative AI in their daily lives, and subsequently optimising them to improve their performance requires significant amounts of energy long after the initial development.

In addition to electricity requirements, large quantities of water are required to cool the hardware used to train, develop, and optimise generative AI models, which can strain local water supplies and disrupt local ecosystems. The growing number of production AI applications has also led to an increase in demand for high-performance computing hardware, adding indirect environmental impacts from manufacturing and transportation.

All these issues can be addressed if AI is treated as a tool for development and sustainability. AI plays an important role in addressing environmental challenges, from designing more energy-efficient buildings to monitoring deforestation and optimising the development of renewable energy sources. The contribution of AI includes satellite monitoring of global emissions and smart homes that automatically switch off

lights or heating after a set period. At the same time, specialised applications can curate, aggregate, and visualise the best available Earth observation and sensor data in near real time, producing forecasts on multiple factors such as atmospheric carbon dioxide concentration, changes in glacier mass, sea level rise, and so on. As experts hope, over time the goal is for the platform to become a mission control centre for planet Earth, where all vital environmental indicators are monitored seamlessly and guide corresponding actions.

The solutions will not come from the use of AI alone. In most cases, multiple complementary technologies are combined, such as robotics, the Internet of Things, distributed energy resources, electric vehicles and others.

While data and AI are essential for enhanced environmental monitoring, there is also an environmental cost to processing such data that must also be taken into consideration.

The above highlights the need to integrate environmental considerations into the design of AI systems.

J. Do no harm

The principle of "do no harm" plays a central role in the sense of protecting the life and health of individuals.[131] In this light, AI tools must not be used in ways that cause actual or potential physical or psychological harm or damage.[132] Preventing or averting harm includes preventing both potential and unforeseeable, as well as malicious harm.[133]

K. Prevention and precaution

The principle of prevention requires the discontinuation or reinforcement of applications when specific risks are identified, while the precautionary principle requires the discontinuation or reinforcement of appli-

[131] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility", in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (275).
[132] Ibid., 275.
[133] Ibid.

cations even when the risk remains uncertain.[134] The anticipation of risks takes place within the framework of the impact assessment process. The principle of prevention and the precautionary principle sometimes seem to conflict with the principle of effectiveness.[135] This is because anyone who makes use of algorithms is aware of their uncertainty and, therefore, has to take responsibility for them.[136]

L. Concluding remarks

The above principles largely stem from the relationship between Greek philosophy and modern technology.[137] This is because the idea of creating autonomous machines that make decisions without human involvement raises important questions regarding control, free will, and dependence.[138] This autonomy must be based on responsibility, in the sense of moral responsibility.[139] Scientific autonomy should be pursued with an understanding of the relevant concepts, as well as awareness of the risk of hubris.[140] Therefore, AI must respect ethical boundaries and consider its wider implications for society and humanity.[141] It must serve humanity, and contribute to its advancement.[142] Aristotle's teachings are extremely useful in defining the limits of the use of AI.[143]

---

[134] Ibid., 277.

[135] Chryssoula P. Moukiou, *Algorithms and Administrative Law* (Athens–Thessaloniki: Sakkoulas, 2025), 268.

[136] Ibid.

[137] Konstantinos Karpouzis, "From Plato's Forms to the Norms of Artificial Intelligence: A Guide to Modern Technology through Ancient Greek Philosophy," *dia-LOGOS* 14 (2014): 275 ff. (278).

[138] Ibid.

[139] Ibid.

[140] Ibid., 280.

[141] Ibid.

[142] Manolis Andriotakis, *Artificial Intelligence for All* (Athens: Psychogios, 2022), 212.

[143] Prokopios Pavlopoulos, "Critical Reflections on the Relevance of Aristotle's Positions on Law and Justice in the Age of Artificial Intelligence," *Public Law Review* 1 (2025): 41 ff. (41).

VI. Scope of application

Article 2 of the Regulation defines the scope of its application. According to a literal interpretation, this constitutes the personal scope, as it defines the persons to whom the Regulation applies. In addition to the personal scope, said Article also sets out the territorial – in this case international – scope of the Regulation, introducing the principle of extraterritoriality. According to Article 2, the Regulation applies first and foremost to providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country. In this respect, the criterion of the undertaking's place of establishment is adopted.[144] This criterion ensures fair competition in the same market, irrespective of the location of the branch, which is essential for digital services.[145]

'Placing on the market', under Article 3(9) of the Regulation, means the first making available of an AI system or a general-purpose AI model on the Union market. Likewise, according to Article 3(10), 'making available on the market' means the supply of an AI system or a general-purpose AI model for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.

The great difficulty of the AI Act lies in the fact that it is not linked to a traditional physical product, but to a purely software-based product, whose local presence is extremely difficult to determine.[146] Ultimately, an AI system or a general-purpose AI model is deemed to be placed on the Union market if it is made available to end-users in the Union with

[144] Christiane Wendehorst, "Art. 2," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 12.
[145] Ibid.
[146] Ibid., para. 15.

the consent of the provider.[147] Where an AI system or a general-purpose AI model is made available online, or through any other means of distance selling, it is considered to be made available specifically for the Union market if the offer is directed to dealers or other end-users in the Union.[148] An offer for sale is deemed to be directed to a dealer or other end-user in the Union if the economic operator directs its activities in any way to at least one Member State of the Union.[149] The mere accessi-

[147] Ibid.

[148] Ibid., para. 16.

[149] CJEU, Case C-230/14, *Weltimmo s.r.o.*. The case concerned two important aspects of EU data-protection law – applicable law and the territorial scope of supervisory authorities' powers. It arose from a dispute between Weltimmo, a company registered in Slovakia operating real-estate advertising websites concerning Hungarian properties, and the Hungarian Data Protection Authority. Several advertisers filed complaints and the authority fined Weltimmo for breaching the Hungarian information law. On applicable law, Article 4(1)(a) of Directive 95/46/EC provided that a Member State's law applies where personal data are processed "in the context of the activities" of an establishment of the controller in that Member State. The Court held that this provision cannot be interpreted restrictively; EU legislature set a "very broad territorial scope" for the Directive. Rejecting a formalistic approach that companies are established only where registered, the Court interpreted "establishment" in light of the specific nature of the activities and services provided; the presence of even a single representative may suffice. Even minimal, real activity (here, running Hungarian-language fee-based real-estate portals) carried out through stable arrangements in a Member State can meet the establishment criterion and trigger that State's data-protection law. In this case, the existence in Hungary of a representative responsible for debt collection and representation in proceedings, together with a bank account and a PO box, sufficed to constitute activity through stable arrangements. Confirming *Google Spain* (C-131/12), the Court reiterated that Article 4(1)(a) does not require that the processing be carried out by the establishment itself—only that it occurs "in the context of the activities" of that establishment. Here, publishing owners' personal data on Weltimmo's sites and using them for billing constituted processing in the context of Weltimmo's Hungarian activities; the data subjects' nationality was irrelevant. As to powers of DPAs, where a DPA receives complaints about a controller not established on its territory, it may still investigate irrespective of the applicable law; however, it cannot enforce that law or impose sanctions on a controller not established within its jurisdiction. In such a case, the DPA should seek cooperation from the authority of the Member State where the controller is established, which may itself undertake further investigations following the first authority's guidance.

Regarding the applicable law, Article 4(1)(a)' of EU Data Protection Directive 95/46/EC provided that the national law of a Member State applies when personal data are processed in the context of the activities of an establishment of the data controller

bility of a website is not sufficient as a criterion for online distribution.[150] The actual supply of an AI system ordered by an economic operator established outside the Union to operators or other end-users within the Union, including through a fulfilment service provider, constitutes irrefutable confirmation that a product is available on the EU market.[151]

---

in that Member State. According to the Court, this provision cannot be interpreted restrictively; on the contrary, the EU legislator '... has defined a particularly broad territorial scope of Directive 95/46/EC'.

The Court rejected a formulaic approach "according to which undertakings are established only in the place where they are registered", but held that the concept of "establishment" must be interpreted in the light of the specific nature of the economic activities and the provision of the services concerned. The Court clarified that the presence of a single representative may, in certain cases, be sufficient. Even a 'minimal' real and effective activity (in this case, the operation of real estate marketing websites written in Hungarian with advertisements subject to remuneration) carried out through stable arrangements in a Member State may be sufficient to trigger the 'establishment' criterion and make the data protection law of that Member State applicable. In the present case, the Court held that the existence of an agent in Hungary, who is responsible for the collection of debts arising from the activity and who represents the controller in administrative and judicial proceedings, as well as the existence of a bank account and a letterbox in Hungary, would be sufficient to qualify as an activity carried out through fixed arrangements. The Court confirmed its findings from Google Spain (C-131/12) that Article 4(1)(a) of Directive 95/46/EC does not require that such processing of personal data be carried out by the establishment concerned, but only processing "in the course of the activities" of the establishment. In the present case, in the Court's view, the fact that Weltimmo's websites published personal data of property owners and in some cases used those data for billing purposes constituted processing in the course of Weltimmo's activities in Hungary. The nationality of the persons concerned by such processing is irrelevant.

On the powers of data protection authorities, the Court considered a scenario where a data protection authority received complaints about the activities of a data controller not established on its territory. In this case, the Court held, the national data protection authority may nevertheless investigate the complaint independently of the applicable data protection law. However, the data protection authority cannot enforce the applicable data protection law and impose sanctions on a controller not established in its jurisdiction. Instead, in such a case, the data protection authority should request the cooperation of the data protection authority of the country where the controller is established, which may itself carry out other investigations, on the instructions of the previous supervisory authority.

[150] Christiane Wendehorst, "Art. 2," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 16.

[151] Ibid.

According to Article 3(11), 'putting into service' means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose. The distinction from placing on the market is that the AI system is never placed on the market, since the supplier either develops it for own use or provides it directly to a company as a customised AI system, without placing it on the market.[152]

The place of establishment within the Union, according to Article 2(1)(b) of the Regulation, is a criterion for its application. The Regulation establishes the principle of establishment, which applies only to users and not to providers. That provision is problematic, as providers are not required to comply with the Regulation if the systems they develop are intended exclusively for export, that is, for placing on the market or putting into service outside the Union. If providers were required to comply, this would unjustifiably weaken the Union as a place of establishment, as suppliers may wish to develop certain AI systems for export outside the Union.[153] This enables European businesses to profit from unethical and dangerous AI systems.[154] Thus, while the AI Act prohibits or strictly limits the use of certain AI technologies in the Union due to the unacceptable risks they pose to human rights, it permits the export of the same technologies from the Union to the rest of the world. This provision is open to justified criticism, as it reflects a contradiction: on the one hand, the Union presents itself as a global leader in promoting "safe, reliable, and ethical AI," while on the other, it allows its companies to export AI systems that violate rights to the rest of the world.[155]

The concept of the seat or location of the operator within the Union is not clarified. The English term "established or located" appears in several places in the Regulation and in a number of other digital acts of the

[152] Ibid.

[153] Ibid., para. 20.

[154] Amnesty International. *EU: Lawmakers Reluctant to Stop EU Companies Profiting from Surveillance and Abuse through the AI Act.* December 5, 2023. https://www.amnesty.org/en/latest/news/2023/12/eu-lawmakers-reluctant-to-stop-eu-companies-profiting-from-surveillance-and-abuse-through-the-ai-act/

[155] Ibid.

Union, but it is translated inconsistently.[156] Furthermore, the use of the two terms "established" and "located" is intended to address legal persons and partnerships in the same way as natural persons. At the same time, the registered or actual seat is often treated as an alternative, while in the case of natural persons it is generally linked to habitual residence.[157] According to the case law of the Court of Justice of the European Union (CJEU), however, excessively high requirements should not be imposed for the existence of a branch.[158] In particular, it is not necessary for all, or even only the essential material operational resources (for example, buildings, servers, staff), to be located in the Union, provided that the relevant processes are controlled by persons resident in the Union, or that not entirely unrelated supporting activities are transferred outside the Union.[159]

The criterion of using all outputs in the Union, under Article 2(1)(c) of the Regulation, is that it applies to providers and operators of AI systems established or located in a third country when the output generated by the AI system is used in the Union. This provision is intended as a general clause for cases where an AI system is neither placed on the market, nor put into service, nor used in the Union. A characteristic example is when a company established in the Union concludes a contract for services in a third country, which are carried out by a high-risk AI system.[160] Without this provision, application of the Regulation by the companies involved could be undermined in such a case. To avoid circumvention of the Regulation and ensure effective protection of natural persons established in the Union, it should also apply to providers and operators of AI systems established in a third country, insofar as the output generated by

[156] Christiane Wendehorst, "Art. 2," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 20.

[157] Ibid., para. 20.

[158] CJEU, Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639 (1 October 2015).

[159] Christiane Wendehorst, "Art. 2," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 23.

[160] Ibid., para. 24.

those systems is intended for use in the Union.[161] The Regulation applies only to the activities of the company established in the third country, not to those of the contracting entity in the territory of the Union. The latter does not appear to be subject to specific provisions, although it could, and arguably should, be made equally liable.[162]

The provisions of Article 2(1)(d) to (f) extend the scope of the Regulation to other entities that are neither providers nor operators of AI systems. These include the importers and distributors of AI systems. Under Article 3(1)(6), 'importer' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country. According to Article 3(7), 'distributor' means a natural or legal person in the supply chain, other than the provider or the importer that makes an AI system available on the Union market. In this case, extraterritoriality arises not from Article 2(1) of the Regulation but from the definitions in Article 3, without sufficient justification for that different treatment.[163] There is also no convincing reason why only a person resident or established in the Union should qualify as an importer.[164] A supplier's representative established in a third country could, for instance, import an AI system into the Union by distributing it directly to end-users in the Union.[165] Such a person is nevertheless treated as a distributor, meaning it is subject to the obligations of Article 27 (impact assessment of high-risk AI systems on fundamental rights), not to the stricter obligations of Article 26 (obligations of deployers of high-risk AI systems).[166] Extension of the Regulation's scope also applies to product manufacturers who market or sell an AI system with their product under their own name or trademark.[167] Moreover, the extension of the scope also affects authorised representatives of providers not established in the

[161] Ibid.
[162] Ibid., para. 25.
[163] Ibid., para. 26.
[164] Ibid.
[165] Ibid., para. 27.
[166] Ibid.
[167] Ibid., para. 28.

Union.[168] According to Article 3(5), 'authorised representative' means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.

Finally, under Article 2(1)(g) of the Regulation, it applies to data subjects located in the Union. The residence requirement applies in particular for the purposes of Article 86, which grants data subjects the right to request explanations for decisions concerning them.

According to Article 2(2) of the Regulation, it does not apply to the military, defence, and national security sectors. Consequently, the system in question must be used for military purposes, with the purpose being objectively defined and understood; a mere potential use is not sufficient. Under Article 42 of the Treaty on European Union, defence policy purposes cover all military measures to protect national territory against armed attacks from abroad, including military organisation and defence against cyber-attacks by other states.[169] National security encompasses the activities of domestic and foreign intelligence agencies, as well as activities ensuring state security. In essence, it concerns the responsibility of Member States to defend against external attacks and internal threats to state order, including the prevention and suppression of terrorist acts.[170]

Article 2(4) of the Regulation introduces an exception for AI systems used in the context of international cooperation or agreements on law enforcement and judicial cooperation with the Union or its Member States, provided that the third country or international organisation offers sufficient safeguards for fundamental rights and freedoms. This may include information exchange, support for investigations, or coordination of anti-crime measures. The use of AI systems must still comply with data protection, privacy, and fundamental rights requirements.[171]

Article 2(6) and (8) of the Regulation introduce exclusions for scientific research and development.

---

[168] Ibid.
[169] Ibid., para. 64.
[170] Ibid., para. 63.
[171] Ibid., para. 71.

VII. Similarities with the General Data Protection Regulation (GDPR)

AI is directly linked to data protection, as algorithms rely on data. AI is not explicitly mentioned in the GDPR, but many of its provisions are relevant to AI, and some are challenged by new methods of processing personal data[172] made possible through AI.[173] The AI Act seems to be modelled on the GDPR. In fact, it would not be an exaggeration to describe it as an "imitation" of it.[174]

The similarity is particularly evident in the following key areas:

First, the AI Act is extraterritorial in nature. According to Article 2(1)(a) to (c) it applies to (a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country; (b) deployers of AI systems that have their place of establishment or are located within the Union; and (c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union. This means that the provider of the AI does not need to be established in the Union, as long

[172] Athina Moraiti and Charalampos Stamelos, "The Impact of AI on Data Protection: Evolution of Court of Justice of the European Union Case Law Regarding the General Data Protection Regulation (GDPR) in the Artificial Intelligence Era," in *EU Digital Law in the AI Era*, ed. Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou, and Thalia Prastitou-Merdi (Cham: Springer, 2025, forthcoming).

[173] European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA). *Study Panel for the Future of Science and Technology.* PE 641.530, June 2020, II. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

[174] Vagelis Papakonstantinou and Paul De Hert, *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis, and EU Law Brutality at Play* (London: Routledge, 2024).

as the AI system exists and operates within the Union.[175] The GDPR has a corresponding extraterritorial character. According to Article 3 of the GDPR, its scope extends to the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not, where the processing concerns data subjects located in the EU, such as in cases of online commerce or profiling.

Second, the AI Act introduces the concept of quasi-self-regulation, meaning that AI applications are not, as a rule, licensed by a supervisory authority. The GDPR operates similarly, as Article 36(5) leaves it to Member States to determine whether prior authorisation by a supervisory authority is required.

Third, in the event of a breach of the Regulation's provisions, the fines are extremely high.[176] The same applies to the high fines provided for under the GDPR.[177]

Fourth, the AI Act leaves Member States discretion to make their own choices. In practice, it is a Regulation with many features similar to those of a Directive. A typical example is the discretion of Member States to impose fines on public authorities (Article 99(1)).

Fifth, the AI Act requires each Member State to designate one or more national competent authorities and a single point of contact (Article 70). At EU level, coordination is ensured by the European Artificial Intelligence Board (Articles 65 and 66). A comparable model is established in the GDPR in Articles 51 et seq. on supervisory authorities and Articles 70 et seq. on the European Data Protection Board.

---

[175] Vasilis Tzemos, "The New Regulation on Artificial Intelligence and the Charter of Fundamental Rights of the European Union (CFR)," in *Exploring Aspects of Artificial Intelligence: Cutting-Edge Technologies as a Legislative Challenge, 2nd Interdisciplinary Conference on Law and Informatics*, ed. Eugenia Alexandropoulou-Aigyptiadou, Theoharis Dalakouras, and Christos Mastrokostas (Athens: Nomiki Vivliothiki, 2025), 99 ff. (100).

[176] Infra, chapter XI, "Penalties".

[177] According to Article 83(6) GDPR, "non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher".

Sixth, the AI Act introduces a set of actors that, although unique in their configuration, resemble those of the GDPR.[178] The "provider" is the decision-maker, who, either directly or through intermediaries such as the "importer", "distributor", or "authorised representative", influences the passive recipients, the "deployers". All these actors are involved in the use of an AI system.[179]

Seventh, certain provisions of the Regulation are clearly influenced by the GDPR. These include the home use exemption (Article 3(4)), certification mechanisms such as declarations of conformity and codes of conduct (Articles 47 and 95), the AI registration system (Articles 51 and 49), the mandatory appointment of representatives in the Union for any non-EU AI operator (Article 22), and the principle of accountability (Articles 23 and 26(5)).[180]

Eighth, both the GDPR and the AI Act are guided by the need to facilitate scientific research, recognising its importance. In this regard, regulatory sandboxes are of particular importance.

The facilitation of research under the GDPR can be seen in the following aspects:

(a) The GDPR adopts the principle of compatibility with the original purpose, thereby granting wide discretion to the controller, who has the final say regarding any change of processing purpose.

(b) Exceptionally, according to Recital 33 of the GDPR, broad consent may be granted for certain areas of scientific research, to the extent permitted by the purpose pursued. The aim of this provision is to facilitate scientific research in order to relieve researchers of the burden of obtaining multiple consents when changing the purpose of their research.[181]

[178] Article 3 of the AI Regulation.

[179] Vagelis Papakonstantinou and Paul De Hert, *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis, and EU Law Brutality at Play* (London: Routledge, 2024), part 5.2.3.

[180] Ibid.

[181] Fereniki Panagopoulou-Koutnatzi, "Research in Historical Sources and Protection of Information," *Media and Communication Law Review* (2014): 28 ff. (30 ff.).

(c) Similarly, Article 89(2) of the GDPR provides an exception to the storage limitation principle, allowing further retention of personal data where required for historical, statistical, or scientific research purposes.

(d) Research purposes constitute an independent and sufficient lawful basis even for the processing of special categories of data, namely sensitive data such as racial or ethnic origin, political opinions, health, criminal prosecutions, and convictions.

VIII. Key pillars

A. General

The AI Act is a horizontal instrument aiming at product safety and a risk-based approach. It aims to protect health, safety, and fundamental rights. It is innovation-friendly, complementing the existing acquis. It applies to public and private entities, both within and outside the EU, where an AI system is placed on the Union market or its use affects individuals in the EU. It does not apply to military, defence, or national security activities, to free and open-source software (with exceptions), or to research, development, and prototyping prior to market placement.

B. Risk-based categorisation

The AI Act classifies artificial intelligence systems into four categories according to the level of risk that they pose. Systems presenting only limited risk are subject to light transparency obligations. High-risk AI systems require conformity assessment and must meet a series of requirements and obligations to access the EU market. Systems involving, for instance, cognitive behavioural manipulation of persons or social scoring are prohibited, as their risk is considered unacceptable. It also prohibits predictive, profiling-based policing and systems using biometric data to categorise people by characteristics such as racial origin, religion, or sexual orientation.

1. Unacceptable risk (Article 5)

The AI Act prohibits certain AI applications that threaten citizens' rights. This is an agreement not to accept dangerous systems.

In particular, the prohibition applies to:

(a) The use of subliminal techniques, or manipulative or deceptive practices, that materially distort behaviour in a manner likely to cause significant harm.

(b) The exploitation of vulnerabilities related to age, disability, or social or economic situation, in a manner likely to cause significant harm.

(c) Biometric categorisation systems that infer specific categories of data (race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation), except where used solely for the labelling or filtering of lawfully acquired biometric datasets, or when carried out by law enforcement authorities under strict conditions.

(d) Social scoring, meaning the evaluation or classification of individuals or groups based on social behaviour or personal characteristics, causing harmful or adverse treatment of those individuals.

(e) The assessment of the risk of an individual committing criminal acts solely based on profiling or personality traits, except where it is used to reinforce human assessments based on objective, verifiable facts directly related to criminal activity.

(f) The compilation of facial recognition databases through untargeted extraction of facial images from the internet or from CCTV footage.

(g) Drawing inferences about emotions in workplaces or educational institutions, except for medical or safety reasons.

(h) 'Real-time' remote biometric identification in publicly accessible spaces for law enforcement purposes, except where it relates to:

   i. The search for missing persons, abducted victims and victims of trafficking in human beings or sexual exploitation.

   ii. The prevention of a substantial and imminent threat to life or a foreseeable terrorist attack; or

iii. The identification of suspects of serious crimes (such as murder, rape, armed robbery, drug and illegal arms trafficking, organised crime, environmental crime, and so on).

The above use is permitted only where non-use of the tool would cause significant harm and must take into account the rights and freedoms of the persons concerned.

Prior to deployment, the police must carry out a fundamental rights impact assessment and register the system in the EU database, although, in duly justified cases of urgency, deployment may commence without registration, provided that it is registered later without undue delay.

Prior to putting it into service, authorisation must be obtained from a judicial or independent administrative authority, although, in duly justified cases of urgency, deployment may commence without authorisation, provided that authorisation is requested within 24 hours. If authorisation is refused, deployment must cease immediately, with all data, results, and output being erased.

2. High risk (Article 6 et seq.)

Most of the AI Act concerns high-risk AI systems, which are subject to specific regulation. These systems require an impact assessment study. The Act lays down clear obligations for high-risk AI systems, due to the significant potential harm they may cause to health, safety, fundamental rights, the environment, democracy, and the rule of law. These systems must assess and mitigate risks, keep usage logs, ensure transparency and accuracy, and guarantee human oversight. Citizens will have the right to lodge complaints about such systems and to receive explanations about decisions based on high-risk systems that affect their rights. High-risk regulation derives from the safety of the products concerned.

As mentioned above, the AI Act prohibits, in principle, the use of biometric personal identification systems by law enforcement authorities. Exceptionally, the use of such systems is permitted in exhaustively listed and narrowly defined circumstances. In such cases, the use of the systems must be limited in time and geographic scope and subject to specific prior judicial or administrative authorisation. Such uses may include, for example, the targeted search for a missing person or the prevention of

a terrorist attack. The ex-post use of such systems is considered a case of high-risk use, which requires judicial authorisation and is linked to a criminal offence.

High-risk AI systems must undergo a third-party conformity assessment unless the AI system:

- Performs a narrow procedural task.
- Improves the outcome of a previously completed human activity.
- Detects patterns of decision-making or deviations from previous decision-making patterns and is not intended to replace or influence the previously completed human assessment without appropriate human review; or
- Performs preparatory work for an assessment relevant to the purposes of the following use cases:
  (a) Non-prohibited biometrics (remote biometric identification systems, AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics; and AI systems intended to be used for emotion recognition).
  (b) Critical infrastructure (safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity).
  (c) Education and vocational training (AI systems to determine access or admission or assignment of natural persons to educational and vocational training institutions at all levels, evaluation of learning outcomes, assessment of the appropriate level of education, monitoring and detecting prohibited behaviour of students during tests).
  (d) Employment, employee management, and access to self-employment (AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job

applications, and to evaluate candidates, promotion and termination of contracts, allocation of tasks based on personality and behavioural traits or attributes, and monitoring and evaluation of performance).

(e) Access to and enjoyment of essential public and private services (AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services; credit assessment, except for financial fraud detection; emergency call assessment and triage, including prioritisation of police, fire, medical assistance and emergency triage services; risk assessments and pricing in health and life insurance).

(f) Law enforcement (AI systems used to assess a person's risk of becoming a victim of crime, polygraphs, assessing the reliability of evidence during criminal investigations or prosecutions, assessing a person's risk of committing or re-offending not only on the basis of profiling or assessing personality traits or past criminal behaviour, profiling during criminal investigations, interrogations or prosecutions).

(g) Management of migration, asylum and border controls (polygraphs, irregular migration or health risk assessments, examination of applications for asylum, visas and residence permits, as well as related complaints concerning eligibility, tracing, identification or identification of persons, except for the verification of travel documents).

(h) Justice and democratic processes (AI systems used to investigate and interpret facts and apply the law to specific events or used in alternative dispute resolution).

AI systems are always considered high-risk if they create profiles of individuals, that is, the automated processing of personal data to evaluate various aspects of an individual's life, such as work performance, financial situation, health, preferences, interests, trustworthiness, behaviour, location, or movement.

Providers who consider that their AI system, which does not fall under the above categories (a to h), is not high-risk, must substantiate this assessment before the system is placed on the market or put into service.

3. Limited risk

Such systems are subject to lighter transparency obligations: providers and developers must ensure that end-users are aware that they are interacting with an AI system (chatbots and deepfakes).

4. Minimal risk

Not regulated and covering the majority of AI applications currently available in the EU Single Market, such as AI-enabled video games and spam filters.

The AI Act imposes most obligations on high-risk AI systems. Other systems with a lower risk potential are subject mainly to transparency requirements, primarily regulated in Article 50.[182]

For example, Article 50(1) sets out labelling obligations for AI chatbot providers: Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, unless those systems are available for the public to report a criminal offence. This rule therefore requires the labelling of AI chatbots. Moreover, AI systems used for the detection, prevention, investigation, or prosecution of criminal offences are not, of course, subject to such transparency obligations.

Article 50(2) also sets out labelling obligations for AI systems with which audio, image, video or text content can be generated, such as, in-

[182] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 168.

ter alia, ChatGPT, DALL-E, Midjourney, Sora & Co. In this regard, the Regulation sets out the following: "Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards. This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where they are authorised by law to detect, prevent, investigate or prosecute criminal offences. Providers of such AI systems must therefore ensure that the content generated by their applications is labelled in a machine-readable format so that it can subsequently be identified as AI content. Such labelling must be "efficient, interoperable, robust and reliable." Whether, when, and which solutions that are genuinely secure against forgery or counterfeiting can be implemented in practice will become clear over time.[183]

Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system and the personal data processed (Article 50(3)). In this case too, the Regulation provides an exception for AI systems authorised for the detection, prevention, or investigation of crimes.

C. Risk mitigation measures: Assessing the impact of high-risk artificial intelligence systems on fundamental rights

The interaction of AI systems with the protection of fundamental rights has been a central point of the debate on the regulation of AI.[184] Article

[183] Ibid.

[184] Iris Eisenberger, "Art. 17," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 15.

27 establishes the obligation for deployers to conduct an impact assessment of the effects of high-risk systems on fundamental rights.

According to Article 27 (1), "Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce".

It is noted that this Article limits the personal scope, since an impact assessment is not required for all deployers of high-risk AI systems, but only for (a) public law bodies; (b) private entities providing public services; and (c) deployers in the banking and insurance sector intending to use AI systems to assess or rate the creditworthiness of natural persons and to set pricing for natural persons in the context of life or health insurance. An exception is made for AI systems used for the purpose of detecting financial fraud. The impact assessment does not aim at the a priori exclusion or reduction of risks, but at their mitigation or management once they arise.[185] The a priori exclusion of risks is addressed in the risk management system provided for in Article 9.

The impact assessment study shall, according to Article 27(1), consist of a documentation of the risks. This documentation must contain very different aspects:

(a) A description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose.

(b) A description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used.

(c) The categories of natural persons and groups likely to be affected by its use in the specific context.

(d) The specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant

[185] Ibid., para 4.

to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13.

(e) A description of the implementation of human oversight measures, according to the instructions for use.

(f) The measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

With regard to the methodology used for carrying out the impact assessment study, no detailed specifications exist so far.[186] The AI Act does, however, provide various mechanisms that can facilitate the standardisation of the process. A classic example is Article 40 on "harmonised standards and standardisation deliverables", which, although intended for the cases in Chapter III, Section 2 (Requirements for high-risk AI systems), could also be used for the impact assessment. A second option is the Commission's Article 41 Common Specifications. Moreover, the involvement of the European Artificial Intelligence Board under Article 65 is important for standardisation.

The results of the fundamental rights impact assessment must be communicated by the deployer to the market surveillance authority by submitting the completed template referred to in Article 27(5). The model questionnaire will be drawn up by the AI Office, including through an automated tool, in order to facilitate deployers in fulfilling their obligations in a simplified way.

According to Article 27(4), if a data protection impact assessment is required under Article 35 of Regulation (EU) 2016/679 or Article 27

[186] Ibid., para. 6.1. According to Article 5 of Law No. 4961/2022, any public sector body using an artificial intelligence system must, prior to its operation, conduct an algorithmic impact assessment. This assessment must take into account, inter alia: (a) the intended purpose, including the public interest served; (b) the capabilities, technical features, and operating parameters; (c) the type and categories of decisions or acts taken or supported; (d) the categories of data collected, processed, entered into, or generated; (e) the risks that may arise for the rights, freedoms, and legitimate interests of natural or legal persons affected; and (f) the expected benefit for society in relation to potential risks and impacts, particularly for racial, ethnic, social, or age groups, and for persons with disabilities or chronic conditions.

of Directive (EU) 2016/680, the fundamental rights impact assessment shall complement that data protection impact assessment. It should be noted, however, that the GDPR impact assessment had assumed the role of an overall impact assessment not only for personal data but also for all fundamental rights. This approach is taken by the European Data Protection Board, which has adopted the "Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", issued by the Article 29 Working Party. Some concerns may be expressed about the comprehensive consideration of rights beyond privacy by the Data Protection Authority, which is entrusted with supervising the implementation of data protection law (Article 9 of Law No. 4624/2019) and not with the general protection of all constitutional rights. This concern, however, is mitigated by the fact that the rights in question are affected precisely because of the interference with privacy and, therefore, a balancing between privacy and other conflicting goods takes place.[187]

Article 27(1) of the Regulation provides that only high-risk AI systems are subject to the obligation to carry out a fundamental rights impact assessment.

These systems are:

1. Remote biometric identification systems intended to be used for biometric categorization and recognition of emotions.

2. AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

3. AI systems intended to be used:

   (a) To determine access or admission or to assign natural persons to educational and vocational training institutions at all levels.

[187] Fereniki Panagopoulou-Koutnatzi, "The Issue of Body and Portable Cameras Worn by the Riot Police (MAT) of the Hellenic Police," *Syntagma Watch*, January 4, 2021, https://www.syntagmawatch.gr/trending-issues/to-zitima-twn-kamerwn-foritwn-kai-swmatos-poy-feroun-oi-monades-apokatastaseos-tis-taxis-mat-tis-ellhnikhs-astynomias/

(b) To evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels.

(c) For the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels.

(d) For monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

4. AI systems intended to be used:

(a) For the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates.

(b) To make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

5. AI systems intended to be used by or on behalf of public authorities:

(a) To evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services.

(b) To evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud.

(c) For risk assessment and pricing in relation to natural persons in the case of life and health insurance.

(d) To evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.

6. AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies:

   (a) In support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences.

   (b) In support of law enforcement authorities as polygraphs or similar tools.

   (c) In support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences.

   (d) In support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups.

7. AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies:

   (a) As polygraphs or similar tools.

   (b) To assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State.

   (c) To assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence.

(d) In the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.

8. Administration of justice and democratic processes:

(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution.

(b) To be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda.

D. Specific knowledge in the field of artificial intelligence

No later than when an AI system is introduced into an undertaking, there must be at least one person with the necessary specific knowledge of AI technology, both technical and legal. Ideally, a multidisciplinary "AI-competent team" should exist. This may only be feasible in larger organisations. Still, even in smaller companies, AI should not be introduced merely "because the competition does it". Realistic use cases must be considered in advance, and expertise in AI should be developed and consolidated within the undertaking. Article 4 states that providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used. Accordingly, providers and deployers of AI systems are legally required to ensure that their staff and other persons working on their behalf have an adequate level of AI literacy. This requirement is so important to the EU legislator that the Regulation expressly defines the term "AI literacy". According to Article 3(56), this term means skills, knowledge and understanding

that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and the possible harm it may cause. The AI Act thus establishes a de facto legal obligation for continuous training.[188]

[188] Michael Rohrlich, *KI und Recht* (Munich: Hanser, 2025), 172.

IX. Obligations of the Parties

As noted, the AI Act distinguishes between different categories: providers, deployers, importers, distributors, and authorised representatives, allocating distinct responsibilities along the AI value chain.

A. Providers

Under Article 16, providers of high-risk AI systems are under obligation to:

(a) Establish and maintain a risk management system throughout the life cycle of the high-risk AI system.

(b) Establish a data governance and management system ensuring that training, validation, and testing data sets are relevant, sufficiently representative, free of errors and complete, in accordance with the intended purpose.

(c) Draw up and keep the technical documentation demonstrating compliance and provide it to the competent authorities upon request.

(d) Design the high-risk AI system for record-keeping so that it can automatically log events relevant to the identification of risks and any substantial modifications throughout the life cycle of the system.

(e) Provide instructions for use to subsequent developers so as to enable their compliance.

(f) Design the high-risk AI system in such a way that developers are able to apply human oversight.

(g) Design the high-risk AI system to achieve appropriate levels of accuracy, robustness, and cybersecurity.

(h) Establish quality management systems to ensure compliance.

In line with the transparency obligations, general-purpose AI systems and their underlying models must respect EU copyright law and publish detailed summaries of the training data. Moreover, any artificial or manipulated images, sound, or video content (deepfakes) must be explicitly labelled as such.

Article 17 sets out the obligations of providers of high-risk AI systems, requiring them to put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a) A strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system.

(b) Techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system.

(c) Techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system.

(d) Examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out.

(e) Technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full or do not cover all of the relevant requirements set out in Section 2, the means to be used to ensure that the high-risk AI system complies with those requirements.

(f) Systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed

before and for the purpose of the placing on the market or the putting into service of high-risk AI systems.

(g) The risk management system referred to in Article 9.

(h) The setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 72.

(i) Procedures related to the reporting of a serious incident in accordance with Article 73.

(j) The handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties.

(k) Systems and procedures for record-keeping of all relevant documentation and information.

(l) Resource management, including security-of-supply related measures.

(m) An accountability framework setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph.

Article 17(2) introduces the criterion of proportionality, as the application of the aspects set out in paragraph 1 must be proportionate to the size of the provider's organisation. In all cases, providers must respect the degree of rigour and the level of protection necessary to ensure that their high-risk AI systems comply with the Regulation.

The obligation to keep documentation is set out in Article 18. In this respect, the provider must keep at the disposal of the national competent authorities, for a period of ten years after the high-risk AI system has been placed on the market or put into service:

(a) The technical documentation referred to in Article 11.

(b) The documentation concerning the quality management system referred to in Article 17.

(c) The documentation concerning the changes approved by the notified bodies, where applicable.

(d) The decisions and other documents issued by the notified bodies, where applicable.

(e) The documentation concerning the changes approved by the notified bodies, where applicable.

(f) The EU declaration of conformity referred to in Article 47.

Article 19 provides for the automatic generation of logs, while Article 20 imposes corrective measures and a duty of information on providers of high-risk AI systems who consider or have reason to believe that a high-risk AI system they have placed on the market or put into service does not comply with the Regulation. The measures consist of bringing the system into conformity, withdrawing it, disabling it, or recalling it, as appropriate. They must inform the distributors of the high-risk AI system concerned and, where appropriate, the deployers, the authorised representative, and the importers accordingly. At the same time, Article 21 imposes an obligation on providers of high-risk AI systems to cooperate with the competent authorities, upon a reasoned request from a competent authority.

B. Authorised representatives

Article 22 imposes on providers established in third countries the obligation to appoint an authorised representative before making their high-risk AI systems available on the Union market. In this respect, the provider must enable the authorised representative to perform the tasks specified in the mandate received from the provider. The authorised representative shall provide the market surveillance authorities, upon request, with a copy of the mandate in one of the official languages of the Union institutions, as indicated by the competent authority.

The mandate empowers the authorised representative to perform the following tasks:

(a) Verify that the EU declaration of conformity referred to in Article 47 and the technical documentation referred to in Article 11

have been drawn up and that an appropriate conformity assessment procedure has been carried out by the provider.

(b) Keep at the disposal of the competent authorities and national authorities or bodies referred to in Article 74(10), for a period of ten years after the high-risk AI system has been placed on the market or put into service, the contact details of the provider that appointed the authorised representative, a copy of the EU declaration of conformity referred to in Article 47, the technical documentation and, if applicable, the certificate issued by the notified body.

(c) Provide a competent authority, upon a reasoned request, with all the information and documentation, including that referred to in point (b) of this subparagraph, necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Section 2, including access to the logs, as referred to in Article 12(1), automatically generated by the high-risk AI system, to the extent such logs are under the control of the provider.

(d) Cooperate with competent authorities, upon a reasoned request, in any action the latter take in relation to the high-risk AI system, in particular to reduce and mitigate the risks posed by the high-risk AI system.

(e) Where applicable, comply with the registration obligations referred to in Article 49(1) or, if the registration is carried out by the provider itself, ensure that the information referred to in point 3 of Section A of Annex VIII is correct.

C. Importers

Article 23 lays down the corresponding obligations of importers. Before placing a high-risk AI system on the market, importers shall ensure that the system is in conformity with this Regulation by verifying that:

(a) The relevant conformity assessment procedure referred to in Article 43 has been carried out by the provider of the high-risk AI system.

(b) The provider has drawn up the technical documentation in accordance with Article 11 and Annex IV.

(c) The system bears the required CE marking and is accompanied by the EU declaration of conformity referred to in Article 47 and instructions for use.

(d) The provider has appointed an authorised representative in accordance with Article 22(1).

Where an importer has sufficient reason to believe that a high-risk AI system is not in conformity with the Regulation, has been falsified, or is accompanied by falsified documentation, it shall not place the system on the market until it has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the importer shall inform the provider of the system, the authorised representative, and the market surveillance authorities accordingly.

D. Distributors

Article 24 sets out the obligations of distributors. More specifically, before making a high-risk AI system available on the market, distributors shall verify that it bears the required CE marking, and that it is accompanied by a copy of the EU declaration of conformity referred to in Article 47.Where a distributor considers or has reason to consider, on the basis of the information in its possession, that a high-risk AI system is not in conformity with the requirements set out in Section 2, it shall not make the high-risk AI system available on the market until the system has been brought into conformity with those requirements. Furthermore, where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.

E. Deployers

Finally, Article 26 defines the obligations of the implementers of high-risk AI systems mainly as follows:

Deployers of high-risk AI systems shall take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems, pursuant to paragraphs 3 and 6. They shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support. The obligations set out above are without prejudice to other deployer obligations under Union or national law and to the deployer's freedom to organise its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider. Also without prejudice to the above, to the extent the deployer exercises control over the input data, that deployer shall ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system.

Deployers shall also monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72. Where they have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of Article 79(1), they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system. Where they have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not able to reach the provider, Article 73 shall apply mutatis mutandis. This obligation shall not cover sensitive operational data of deployers of AI systems which are law enforcement authorities. For deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service law.

Deployers of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in

applicable Union or national law, in particular in Union law on the protection of personal data. Deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs as part of the documentation kept pursuant to the relevant Union financial service law.

Before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. Deployers of high-risk AI systems that are public authorities, or Union institutions, bodies, offices or agencies shall comply with the registration obligations referred to in Article 49.

Without prejudice to Directive (EU) 2016/680, in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-event remote biometric identification shall request an authorisation, ex-ante, or without undue delay and no later than 48 hours, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of that system, except when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence

If the authorisation requested pursuant to the first subparagraph is rejected, the use of the post-event remote biometric identification system linked to that requested authorisation shall be stopped with immediate effect and the personal data linked to the use of the high-risk AI system for which the authorisation was requested shall be deleted.

In no case shall such high-risk AI system for post-event remote biometric identification be used for law enforcement purposes in an untargeted way, without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person. It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities based solely on the output of such post-event remote biometric identification systems. Deployers shall

cooperate with the relevant competent authorities in any action those authorities take in relation to the high-risk AI system in order to implement this Regulation.

X. Control and supervision

Human supervision of AI applications is an essential prerequisite for safeguarding personal freedom and self-determination. This oversight is expressly provided for in the AI Act, which establishes a governance structure comprising both national and Union-level bodies.[189]

The need for an objective assessment of an issue with vast emotional and practical implications, alongside the establishment of a robust control framework of bioethical, ethical, legal, and political dimensions, is self-evident.[190]

Given the immense coercive power of AI, failure to regulate it would allow it to dominate us with unforeseeable consequences. We must find a way to control it effectively, ensuring that it remains a valuable tool of immense creative potential. This is no easy task, for its force of implementation appears insurmountable, and, as the saying goes, innovation eats regulation for breakfast.[191]

The truth is that controlling AI is both desirable and absolutely necessary, but in practice it is very difficult, perhaps even impossible.

This is because we cannot:

(a) Restrict a tool that has been trained to transcend all limitations.

(b) Overcome an intelligence capable of harnessing the combined computing power of every device connected to the internet.

(c) Contain an algorithm once it has propagated throughout the internet.

---

[189] Spyros Vlachopoulos, "Article 5, Free Development of Personality, Personal Freedom," in *Artificial Intelligence, Human Rights and the Rule of Law, ed. Evripidis Stylianidis* (Athens: Nomiki Vivliothiki, 2025), 89 ff. (95).

[190] Metropolitan of Mesogaia and Lavreotiki Nikolaos, "Bioethical Approaches to the Impact of Artificial Intelligence on Human Life," https://bioethics.panteion.gr/dimosieyseis/

[191] Ibid.

The only way to achieve this would be to abolish the internet, shut down all computers, disable the global power grid, and reset everything from the beginning. It is evident that such a scenario is unfeasible; if it were to occur, it would unleash total chaos and prove catastrophic for humanity, civilisation, and life itself.[192]

A. Union level

At Union level, two central bodies are established: the AI Office within the Commission, responsible for enforcing the common rules across the Union, and the European Artificial Intelligence Board, composed of representatives of the Member States to provide advisory guidance and assistance to the Commission and the Member States for the consistent and effective application of the AI Act. Although distinct in structure and function, these bodies are designed to complement each other. The AI Office is expected to focus on regulatory supervision and enforcement, in particular with regard to general-purpose AI models. The European Artificial Intelligence Board is tasked with ensuring coordination among Member States, enhancing the application of the AI Act through advice, consultation and awareness-raising initiatives. In addition to these two, the AI Act establishes further Union-level bodies with a partly autonomous role, namely the Scientific Panel, which is an independent group of experts supporting enforcement activities, and the Advisory Forum, a platform for stakeholders to provide technical expertise to both the AI Board and the Commission.

The AI Office, established in February 2024 within the Commission, oversees the enforcement and application of the AI Act in cooperation with the Member States. Its mission is to foster an environment in which AI technologies respect human dignity, rights, and trust. It also promotes cooperation, innovation, and research in the field of AI among diverse stakeholders. Furthermore, it engages in international dialogue and cooperation on AI governance, recognising the need for global alignment. Through these efforts, the AI Office aims to position Europe as a leader in the ethical and sustainable development of AI technologies.

[192] Ibid.

The European Artificial Intelligence Board is composed of high-level representatives from the Commission and all EU Member States. Its role is to discuss ways to strengthen the development and uptake of AI within the Union and to coordinate the next steps for the implementation of the AI Act. The European Data Protection Supervisor (EDPS), along with representatives of the EEA/EFTA States (Norway, Liechtenstein, and Iceland) participate in the European Artificial Intelligence Board as observers. The AI Office provides the secretariat for the European Artificial Intelligence Board.

Meetings of the European Artificial Intelligence Board focus mainly on the establishment of the Board's organisation and the adoption of its rules of procedure; updates and strategic discussions on EU AI policy, including the GenAI4EU initiative and international AI activities; progress reports and exchanges on the Commission's first deliverables concerning the implementation of the AI Act; and the sharing of best practices on national approaches to AI governance and the application of the Act.

The Commission and the Member States aim to ensure the robust and timely establishment of the AI governance framework, facilitating the effective participation of Member States and supporting the consistent application of the AI Act.

B. National level

Effective implementation and enforcement of the AI Act often require a local presence, leaving discretion and responsibility primarily to the Member States to select the competent supervisory body. Each Member State is expected to establish at least one notifying authority responsible for compliance and certification procedures, and one market surveillance authority responsible for verifying that products meet the standards of safety, health, and environmental protection legislation, as described in Regulation (EU) 2019/1020. Both authorities are also encouraged to provide compliance guidance to SMEs and start-ups, taking into account any relevant recommendations from the European Data Protection Board and the Commission (Chapter VII, Section 2 of the Regulation).

The AI Act also requires national authorities to have, on a permanent basis, staff with expertise in AI, data protection, cybersecurity, fundamental rights, health and safety, as well as in the relevant standards and

legislative framework. Member States must assess and submit reports to the Commission every two years (Article 70).

In this context, Member States have the flexibility in designing their AI governance: they may either create new regulatory bodies dedicated to AI, or integrate these supervisory responsibilities into existing entities, such as national data protection authorities, within their domestic legal frameworks.

C. The issue of the supervisory authority in Greece

The question of the supervisory authority for AI is the subject of intense debate and concern internationally. What is required is an effective authority that (a) carefully balances the protection of autonomy, privacy, and intellectual property with the promotion of innovation and research, the strengthening of the market, and the protection of competition; (b) certifies the quality and safety of AI systems; (c) supervises and certifies applications in which AI systems are used; and (d) advises the legislator on AI-related issues.

The options regarding the supervisory authority are as follows:

1. Hellenic Data Protection Authority (HDPA)

The most obvious and straightforward option would be to entrust the supervision of AI to the Hellenic Data Protection Authority (HDPA). This choice is associated with several advantages:

First, Article 63(5) of the Regulation explicitly assigns data protection authorities responsibility for market surveillance of AI systems used for law enforcement purposes.

Second, AI systems, in their overwhelming majority, involve the processing of personal data. There is therefore a strong connection between the regulation of AI systems and data protection law.

Third, the HDPA has already examined AI systems for more than 20 years, , such as biometric facial recognition systems and, more recently, generative AI systems, thereby developing significant expertise in these matters.

Fourth, the HDPA, when addressing issues within its competence, cooperates with counterpart national supervisory authorities of EU Mem-

ber States, within the framework of the one-stop shop and the consistency mechanism (European Data Protection Board), thereby ensuring harmonised application of the GDPR across the Union.

Fifth, in the digital world, data protection is the primary tool for safeguarding individual rights and freedoms, which the Authority always takes into account when examining issues within its remit, by applying the relevant legal provisions. For this reason, the HDPA has already acquired extensive knowledge and experience in matters relating to fundamental rights.

Sixth, health and safety risks are already considered by data protection authorities when assessing data protection impact assessments (DPIAs) of high-risk processing operations. The envisaged fundamental rights impact assessment will largely overlap with the DPIA.

Seventh, the HDPA, as the national competent authority and, with regard to Directive 2016/680/EU, supervisory authority of the national sections and a member of the joint supervisory authorities of the Schengen Information System, Customs Information System, Visa Information System, Europol, and others, already possesses the necessary knowledge and experience in the field of law enforcement.

Eighth, the HDPA, as the competent authority for the GDPR, Directive 2016/680, Directive 2002/58 (ePrivacy), and the regulations governing the operation of the Union's major information systems, already possesses, to a large extent, the necessary knowledge of existing standards and legal requirements.

Ninth, the HDPA has already developed expertise in evaluating certification scheme criteria and codes of conduct, and has acquired knowledge and experience in the relevant standards. Since these tools are foreseen in the GDPR, the HDPA is also in a position to extend its expertise to matters concerning AI systems.

Tenth, if the HDPA is not also designated as the competent authority for AI, stakeholders (operators) will have to deal with multiple authorities, facing the risk of conflicting compliance decisions. In such a scenario, the risks of conflicting regulations from different authorities, fragmentation of data protection oversight, and compliance deadlocks are evident. Moreover, there is a significant risk of multiple sanctions for the same infringement.

Eleventh, the European Data Protection Board, together with the European Data Protection Supervisor (EDPS), adopted an opinion welcoming the selection of the EDPS as competent authority for EU institutions and bodies, and recommending that national data protection authorities should likewise be designated as competent authorities for AI in the Member States.

Twelfth, issues of unconstitutionality are avoided, since establishing a new authority would remove powers from the constitutionally enshrined HDPA.

At the same time, the choice of the HDPA is also associated with certain disadvantages:

First, AI constitutes the fourth industrial revolution and cannot fall under the umbrella of an already existing authority that was established for another purpose, namely the protection of personal data alone.

Second, the HDPA may be biased in favour of data protection and against the development of research and innovation. From this perspective, it could act as an obstacle to AI.

Third, the members of the HDPA specialise in data protection and not in AI.

Fourth, the HDPA in its current composition is understaffed and will not be able to meet its newly expanded responsibilities.

2. Establishment of a National Authority for Privacy, Information and Artificial Intelligence (NAPIA)

The second option is the transformation of the HDPA and the Hellenic Authority for Communication Security and Privacy (after their merger) into a National Authority for Privacy, Information and Artificial Intelligence (NAPIA), or the creation of a new authority with three departments: Privacy, Information, and AI. A sub-authority for AI could be integrated into the existing structure of the HDPA and the Hellenic Authority for Communication Security and Privacy. This sub-authority would consist of full-time permanent members specialised in personal data and some new members from the fields of innovation and research.

This model already exists in Member States, such as France[193] and the Netherlands.[194] This sub-base could be granted further flexibility to foster synergies with academia, research centres, and AI businesses, as well as to support start-ups. After more than five years of experience in implementing the GDPR (at EU level as well), data protection authorities are mature enough to identify and directly address problems that a new authority would otherwise face, providing the fastest, most effective and most cost-efficient solution for the national legislator.

In this way there will be no confusion of competences, since everything related to AI will fall under the NAPIA. The AI department will be responsible for strengthening research and innovation, protecting competition and intellectual property, overseeing technology, certifying AI applications, and advising the legislator. Moreover, the creation of a dedicated AI department will ensure that there is no bias in favour of personal data. At the same time, safeguarding access to information is of particular importance.

The modern trend in European legislation, which is in line with the equal treatment of individual rights, is the establishment of a single administrative authority responsible for both the protection of personal data and freedom of information. Therefore, priority should not be given solely to the protection of personal data when other conflicting constitutionally protected legal rights, such as the freedom of information, are also at stake. This position is fully aligned with the GDPR, which emphatically states in Recital 4 that "the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the pro-

[193] Source: CNIL, "CNIL Creates Artificial Intelligence Department and Begins Work on Learning Databases," https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases

[194] Source: Digital Policy Alert, "Order on Data Protection Authority's Supervisory Role over AI Algorithms," https://digitalpolicyalert.org/change/4226-order-on-data-protection-authoritys-supervisory-role-over-ai-algorithms

tection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity." At the same time, the GDPR enshrines in Article 85 thereof the freedom of expression and information, providing for a balance between the right to the protection of personal data and the right to freedom of expression and information, including processing for journalistic purposes.

This need for balance is not merely theoretical. Without it, there is a reasonable risk that greater emphasis will be placed on the protection of personal data under the aegis of an independent and constitutionally enshrined authority, while access to information would remain, in practice, "orphaned". The result is that the controller will reasonably prefer not to provide the data, since there would be no sanction, rather than to disclose it.

All members of the Authority shall be appointed in accordance with the requirements of Article 101A of the Greek Constitution. It is deemed necessary to provide for transitional provisions to ensure the completion of the terms of office of members of the existing authorities that may be affected by such changes.

3. Establishment of a National Artificial Intelligence Authority (NAA)

The third option is the creation of a specialised authority for AI. This would mean creating a new authority composed of members of the HDPA, the National Commission on Bioethics and Technoethics, and representatives of innovation, research, the market, and other stakeholders. It is a fact that the importance of AI and its strong impact on all areas of contemporary legal life argue in favour of establishing a specialised authority.

AI constitutes the fourth industrial revolution, and its particularity does not allow it to be placed under an already existing authority. The protection of the individual is largely linked to the protection of their personal data from the development of AI, but it is also connected with other goods such as research, innovation, competition, system security, and intellectual property, for which the HDPA may not have the appro-

priate expertise. For this reason, the establishment of a specialised supervisory authority for AI should be considered. This authority would be composed of experts from across the full spectrum of fields related to AI.

The advantage of this specialised authority lies in the fact that it would focus its attention on all areas that pertain to AI. This option is nevertheless linked to several disadvantages. In particular, the division of responsibilities between the supervisory authority and the HDPA may cause confusion of competences. The question arises as to which cases would fall within the competence of the HDPA and which within that of the specialised supervisory authority. This confusion is further compounded by the uncertainty as to what constitutes AI and therefore falls within the competence of the new authority, and what does not constitute AI and therefore remains under the HDPA. If both authorities were to handle the same case, there would be a risk of multiple sanctions for the same infringement and, consequently, a violation of the principle of ne bis in idem. This model ensures the representation of all stakeholders and addresses the legal obstacle of the ne bis in idem principle, since all independent authorities would be represented. Experience in Greece has shown that this model may lack functionality. It should also be emphasised that if competences for data protection are removed from the HDPA, the new authority will have to meet the constitutional requirements of the HDPA.

XI. Penalties

Member States are given the discretion to lay down their own rules on penalties, including administrative fines, applicable to infringements of the Regulation and shall take all measures necessary to ensure their correct and effective implementation. The penalties provided for, however, must be effective, proportionate, and dissuasive, and consider the interests and economic viability of SMEs, including start-ups.

Fines for infringements of the AI Act shall be set as a percentage of the worldwide annual turnover of the infringing undertaking in the preceding financial year, or as a fixed amount, whichever is higher. SMEs and start-ups are subject to proportionate administrative fines.

According to Article 99(2), Member States shall notify the Commission of the rules on penalties and other enforcement measures by the date of entry into application, and shall notify it without delay of any subsequent amendments.

Article 99(3) stipulates that non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to 35 000 000 EUR or, if the offender is an undertaking, up to 7 % of its total worldwide annual turnover for the preceding financial year, whichever is higher. Accordingly, Article 99(4) sets out that non-compliance with any of the following provisions related to operators or notified bodies, other than those laid down in Articles 5, shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 3 % of its total worldwide annual turnover for the preceding financial year, whichever is higher:

(a) Obligations of providers pursuant to Article 16.

(b) Obligations of authorised representatives pursuant to Article 22.

(c) Obligations of importers pursuant to Article 23.

(d) Obligations of distributors pursuant to Article 24.

(e) Obligations of deployers pursuant to Article 26.

(f) Requirements and obligations of notified bodies pursuant to Article 31, Article 33(1), (3) and (4) or Article 34.

(g) Transparency obligations for providers and deployers pursuant to Article 50.

Article 99(5) stresses the importance of providing accurate information to supervisory authorities. Hence it provides that the supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request shall be subject to administrative fines of up to 7 500 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Article 99(7) enshrines the principle of proportionality in setting administrative fines. Accordingly, before imposing a fine and in determining its amount, all relevant circumstances of the specific case shall be taken into account and, as appropriate, regard shall be had to the following:

(a) The nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them.

(b) Whether administrative fines have already been applied by other market surveillance authorities to the same operator for the same infringement.

(c) The size, the annual turnover and market share of the operator committing the infringement.

Finally, Article 99(8) allows Member States to decide to what extent administrative fines may be imposed on public authorities or bodies established within their jurisdiction. Article 99(9) further provides that, depending on national legal systems, fines may be imposed by competent courts or other designated bodies, provided that the resulting framework ensures an equivalent effect across Member States.

XII. Liability

The AI Act is underpinned by the principle of product safety. This principle reflects the aim of broadening the protection of rights, democracy and the rule of law, accounting for systemic risks from specific applications and providing legal remedies.[195] These remedies include the right to lodge a complaint with a market surveillance authority (Article 85) and the right to explanation of individual decision-making (Article 86). The Act does not establish an individual right to compensation from harm caused by AI applications. Liability serves as a deterrent against endangering rights and incentivises providers to design safe systems.[196] The balancing function of liability is a fundamental element of justice and complements the protection of fundamental rights. A clear liability regime enhances trust in AI.[197] When consumers know that concrete mechanisms exist to allocate liability to providers or operators, they are more likely to use the technology and benefit from it.[198] The fact is that AI can affect interests and rights protected under EU or national law For example, the use of AI may negatively affect certain fundamental rights such as life, physical integrity, the prohibition of discrimination, and equal treatment.

The AI Act sets out requirements designed to mitigate risks to safety and fundamental rights. As mentioned above, however, while these requirements are intended to reduce risks to safety and fundamental rights and to prevent, monitor and address social concerns, they do not provide individual compensation to those who have been harmed by AI. Moreover, the Act does not expressly establish a liability regime. Therefore,

[195] Christiane Wendehorst, "Art. 1," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 61.
[196] Ibid., para. 62.
[197] Ibid.
[198] Ibid.

in the absence of an explicit provision, the question of liability for machines arises. Who is liable if a self-driving car crashes, a management algorithm reaches a decision harmful to the individual concerned, or a medical application recommends, after processing all the data, a treatment that worsens the patient's health? The answer to this question is complex. The possible solutions are systematised as follows:

The first position is that responsibility should be borne and managed by the manufacturer of AI products; this approach is also followed by the existing EU Regulations on medical devices.[199] In this way, both the accountability and foresight of the manufacturer will be strengthened. No one should develop AI systems without a sense of responsibility for them, even if they are autonomous machine learning systems, since responsibility can now be embedded as information.[200] The strict liability of the creator should play a central role in compensating for damage caused by defective products and their components, whether they are tangible or digital.[201]

The second position argues that liability should be attributed to the operator of the technology, meaning the driver of the car, the administrator or the medical practitioner who applies the technology. This is because the operator of the relevant programme must not only embrace the proposal but must check whether it is fully adapted to the facts of the case and take into account the possibility of algorithmic bias. When absolute reliance on Tesla's car auto-navigation system resulted in a fatal accident in June 2016, Tesla quickly sought to shift responsibility by claiming that the driver's actions, not the programmer's, were to blame for the fatal collision.[202] In this vein, Tesla requires buyers to contractu-

[199] Articles 10 and 62 of Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnostic medical devices.

[200] Alan F. T. Winfield and Marina Jirotka. "Ethical Governance Is Essential to Building Trust in Robotics and Artificial Intelligence Systems." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018).

[201] European Commission, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Brussels: European Union, 2019), 8, https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en

[202] The Tesla Team, "A Tragic Loss," *Tesla Blog*, June 30, 2016, https://www.tesla.com/blog/tragic-loss; archived at https://perma.cc/94SX-RJCJ

ally commit that drivers must keep their hands on the wheel at all times, even when autopilot is engaged.[203]

The third position consists of sharing liability between the manufacturer or programmer and the operator. Each will be responsible for the share of liability that corresponds to them. This system, while appealing and tending to be the most popular, is not without controversy. The attribution of liability may, in many cases, become a difficult and hard-to-prove issue. If there are two or more actors, particularly (a) the person who primarily decides on and benefits from the use of the relevant technology (frontend operator); and (b) the person who continuously determines the characteristics of the relevant technology and provides substantial and ongoing support to the backend (backend operator), objective liability should rest with the one exercising greater control over the operational risks.[204]

The fourth position argues in favour of attributing liability to the technology itself.[205] Nevertheless, if the technology is to be held liable, it must first be recognised as a subject of law. This solution was rejected in October 2020 by the European Parliament, which adopted three resolutions on the ethical and legal aspects of AI software systems: (a) Resolution 2020/2012(INL) on a framework for ethical aspects of AI, Robotics and related technologies; (b) Resolution 2020/2014(INL) on a civil liability regime for AI; and (c) Resolution 2020/2015(INI) on intellectual property rights for the development of AI technologies. All three resolutions recognise that AI will bring significant benefits in various sectors, including business, the labour market, public transport, and healthcare. However, as noted in the resolution on the ethical aspects of AI, there are concerns that the current legal framework of the Union, including consumer law, the labour and social acquis, data protection legislation, product safety and market surveillance legislation,

[203] *Derdiarian v. Felix Contracting Corp.*, 414 N.E.2d 666, 671 (N.Y. 1980).

[204] European Commission, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Brussels: European Union, 2019), 8, https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en

[205] Vagelis Papakonstantinou and Paul De Hert, "Refusing to Award Legal Personality to AI: Why the European Parliament Got It Wrong," *European Law Blog*, November 20, 2020.

and anti-discrimination legislation, may no longer be adequate to effectively address the risks posed by AI, robotics and related technologies. All three resolutions firmly reject the idea of granting legal personality to AI software systems. Therefore, this solution, although tempting, does not seem relevant for the immediate future, though it cannot be ruled out at a later stage, once the concept of digital personality has matured.

Support for attributing digital personality to machines does not come as a bolt from the blue. It is a solution that would not be entirely alien to our legal system, as it could be paralleled with limited rights (for instance, those of the unborn or the deceased) and obligations (such as those of an animal owner). Indications already suggest that the dichotomy between natural and legal persons may soon evolve into a trichotomy through the recognition of a digital personality.[206] Some striking developments have already occurred, which should not be overlooked. For example, in 2017 Saudi Arabia granted citizenship to Sophia, an AI robot.[207] In addition, a web-based system in the form of a seven-year-old boy was granted a residence permit in Tokyo.[208] In 2014, it was announced that a Hong Kong venture capital firm had appointed a computer programme called Vital to its board of directors to manage its assets.[209] In this context, the creation of limited liability companies without any human members has been advocated. Bill Gates has also proposed the taxation of robots in employment.[210] Recently, a robot addressed the British Parliament for the first time on the topics of art and AI. Ai-Da appeared with the face and attire of a woman, informing British MPs that, although an artificial creation, it is capable of produc-

[206] Vagelis Papakonstantinou and Paul De Hert, "Structuring Modern Life Running on Software: Recognizing (Some) Computer Programs as New 'Digital Persons,'" *Computer Law & Security Review* 34, no. 4 (2018): 732–738.

[207] Dave Gershgorn, "Inside the Mechanical Brain of the World's First Robot Citizen," *Quartz*, November 12, 2017.

[208] Anthony Cuthbertson, "Artificial Intelligence 'Boy' Shibuya Mirai Becomes World's First AI Bot to Be Granted Residency," *Newsweek*, November 6, 2017.

[209] Rob Wile, "A Venture Capital Firm Just Named an Algorithm to Its Board of Directors," *Business Insider*, May 13, 2014.

[210] Kevin J. Delaney, "The Robot That Takes Your Job Should Pay Taxes, Says Bill Gates," *Quartz*, February 17, 2017.

ing art. In China, robots passed the medical licensing examination and are expected to provide care of the elderly.

It could be argued that attributing digital personality to AI applications constitutes a sui generis evolution of the recognition of legal personality in legal entities. Their operating conditions and purposes, nevertheless, are distinct.[211] Reluctant though we may be, developments will overtake us and compel us to recognise a form of digital personality in technology itself, without this absolving natural persons of responsibility. The reasons are straightforward and, at first sight, practical: First, because responsibility must be attributed. Accountability may extend to proceedings against "criminal" AI robots, with sanctions such as reprogramming or, in extreme cases, destruction – penalties which, however, they cannot themselves perceive. Second, because profit must also be attributed, for instance, ownership of intellectual property generated by AI systems.

But all this lies in the future: under present circumstances, the conditions are not yet mature, ethically or legally, for attributing digital personality to machines, as this category has not been sufficiently conceptualised or debated.[212] It must be examined further before being introduced into questions of legal liability. It is no coincidence that every legal concept has been created by humans to regulate relations first between natural persons and later between legal entities.[213] For the moment, a combination of existing liability regimes appears to be the preferable course.[214]

In the light of rapid technological developments, the Commission published a proposal for a Directive on AI liability in September 2022,[215]

---

[211] Dimitrios Koukiadis, "The Regulatory Challenges of Artificial Intelligence and the Issue of Recognition of Personality," *Journal of Law and Technology* (2020): 17 ff. (21).

[212] Michael Anderson, Susan Leigh Anderson, Alkis Gounaris, and George Kosteletos, "Towards Moral Machines: A Discussion with Michael Anderson and Susan Leigh Anderson," *Conatus – Journal of Philosophy* 6, no. 1 (2021): 177–202, https://doi.org/10.12681/cjp.26832

[213] Dimitrios Koukiadis, "The Regulatory Challenges of Artificial Intelligence and the Issue of Recognition of Personality," *Journal of Law and Technology* (2020): 17 ff. (21).

[214] Fereniki Panagopoulou, "Do Machines Have Responsibility?," *To Vima*, September 17, 2023, https://www.tovima.gr/print/nees-epoxes/exoun-oi-mixanes-eythyni/

[215] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Adapting Civil Liability Rules to Artificial Intelligence (AI Liability*

followed by a revised proposal in 2024. This Directive is intended to complement the AI Act and contains proposals for rules on the disclosure of evidence in cases involving high-risk AI systems, together with certain limitations on the claimant's burden of proof. Under general tort law, the claimant must prove the damage, the defendant's fault, and the causal link between the harmful act or omission and the damage suffered. The scope of the Directive also covers claims for compensation for fault-based liability in respect of damage caused by AI systems.[216] The proposed rules will therefore assist claimants in accessing evidence relating to AI systems, with the support of national courts.[217] The Directive introduces a new liability regime that ensures legal certainty, strengthens consumer confidence in AI, and supports consumers claims for compensation for damage caused by AI products and services. It applies to AI systems placed on the EU market or operating within the EU market. The Directive is intended to fill a major gap, since national liability rules – particularly those based on fault – have proven inadequate for addressing claims for damages caused by AI products and services. Under such rules, injured parties must prove an unlawful act or omission by a person responsible for the damage. The particular features of AI, including its complexity, autonomy and opacity, make it difficult or prohibitively costly for injured parties to identify the responsible person and establish the elements of a successful liability claim.

When seeking compensation, injured parties may face very high upfront costs and significantly longer litigation compared with cases not involving AI. They may therefore be discouraged from pursuing compensation altogether. If an injured party brings a claim, national courts, faced with the specific characteristics of AI, may adapt the way they apply the existing rules on an ad hoc basis in order to reach a fair outcome. This has led to legal uncertainty and inconsistency. Businesses have found it difficult to anticipate how liability rules would be applied and, consequently, to assess and insure against their exposure. This has especially affected

Directive), COM(2022) 496 final, Brussels, September 28, 2022, 2022/0303(COD), SEC(2022) 344 final, SWD(2022) 318 final, SWD(2022) 319 final, SWD(2022) 320 final.

[216] Ibid., Art. 1 para. 1.

[217] Ibid., Art. 3 para. 1.

businesses engaged in cross-border transactions and SMEs, which often lack in-house legal expertise or sufficient capital reserves.

Several Member States were considering, or even drafting, legislative measures on civil liability for AI. Without EU-level action, Member States would adapt their national liability rules to address the challenges posed by AI. This would result in further fragmentation and increased costs for businesses operating throughout the EU.

Existing requirements mainly provide for authorisations, controls, monitoring, and administrative penalties concerning AI systems, aimed at preventing losses. They do not, however, provide compensation to injured parties for harm caused either by an outcome or the failure of an AI system to deliver an outcome.

To harness the economic and social benefits of AI and to support the transition to the digital economy, certain national civil liability rules must be specifically adapted to the characteristics of AI systems. These adaptations should foster public and consumer confidence, thereby promoting the uptake of AI, while also maintaining trust in the judicial system by ensuring that victims of damage caused by AI are not left without redress.

The Directive adopts a minimum harmonisation approach. This enables claimants in cases of damage caused by AI schemes to rely on more favourable rules of national law. For example, national rules may continue to provide for the reversal of the burden of proof in fault-based regimes, or for no-fault liability regimes ("strict liability"), which already exist in various forms across Member States and may apply to damage caused by AI systems.

Access to information concerning specific high-risk AI systems suspected of having caused damage is an important factor in determining whether compensation will be sought and in substantiating related claims. Moreover, for high-risk AI systems, the AI Act establishes specific documentation, information, and record-keeping requirements, but it does not grant injured parties a right to access that information. It is therefore appropriate to lay down rules on the disclosure of the relevant evidence by those in possession of it for the purposes of establishing liability. This should also serve as an additional incentive to comply with the documentation and record-keeping requirements under the AI Act.

The large number of actors typically involved in the design, development, installation and operation of high-risk AI systems makes it difficult for injured parties to identify the person potentially responsible for the damage caused and to establish the conditions for a compensation claim.

To enable injured parties to determine whether a compensation claim is well-founded, potential claimants should have the right to request the court to order disclosure of relevant evidence prior to lodging a claim.

Such disclosure should only be ordered where the potential claimant presents facts and information sufficient to support the plausibility of the compensation claim and has previously requested the provider, the person responsible for the provider's obligations, or the user, to disclose such evidence in their possession concerning specific high-risk AI systems suspected of having caused damage, and that request has been refused.

A disclosure order should reduce unnecessary litigation and prevent costs for potential litigants arising from unfounded or potentially unsuccessful claims.

In the course of civil proceedings, national courts should be able to order the disclosure or preservation of relevant evidence relating to the damage caused by high-risk AI systems by persons already obliged under the AI Act to document or record such information.

There may be cases where evidence relevant to the claim is held by entities that are not parties to the compensation proceedings but are nevertheless obliged under the AI Act to document or record such evidence. It is therefore necessary to set out the conditions under which such third parties to the claim may be ordered to disclose the relevant evidence.

While the AI Act mainly regulates AI providers, operators and their systems, the European Commission had also proposed an AI Liability Directive intended to address civil liability for damage caused by AI. Although the proposal was eventually withdrawn and did not reach adoption, it remains relevant for understanding the EU's initial approach to complementing the AI Act.

The draft Directive aimed to modernise national tort law by introducing harmonised rules for "damage caused by AI", primarily by easing the claimant's evidentiary burden. It proposed a rebuttable presumption of causation linking a breach of obligations under the AI Act to the harm suffered, thereby reversing the usual burden of proof and requiring the

operator to show that no such causal link existed.[218] It also provided for adverse inferences where a defendant failed to comply with a court order to disclose or preserve evidence.[219]

Although the initiative did not move forward, the issues it sought to resolve remain central to the European debate on AI-related civil liability. The challenge of proving fault and causation in complex algorithmic environments has not disappeared. These concerns are now addressed through the revised Product Liability Directive, which expands strict liability to software and AI components, and through the continued application of national tort law, which must adapt concepts such as duty of care, foreseeability and evidentiary standards to the realities of AI-driven decision-making. The withdrawal of the proposal therefore does not close the discussion; it shifts the focus to existing legal frameworks and to future legislative options that may be considered once the AI Act is fully implemented.

[218] Ibid., Art. 3 para. 5.
[219] Ibid., Art. 4 para. 1.

XIII. Entry into force

Pursuant to Article 113, the Artificial Intelligence Act entered into force on 1 August 2024. To allow for a smooth adaptation to the new regulatory content by the state, society and the economy in general, it will be implemented gradually. The timeline for the Act's application underwent revisions during the final stages of the legislative process, and earlier commentaries may therefore refer to different transitional periods. The dates that follow reflect the final text as published in the Official Journal of the European Union.

The general date of application of the AI Act is 2 August 2026, unless expressly provided otherwise.

Certain provisions apply earlier. From 2 February 2025, Chapters I and II become applicable. These include the core definitions and the rules concerning prohibited AI practices under Article 5. From 2 August 2025, the following become applicable: Chapter III Section 4, Chapter V, Chapter VII, Chapter XII and Article 78, with the exception of Article 101. From 2 August 2027, Article 6(1), which determines when an AI system qualifies as high-risk, applies together with the corresponding obligations.

In addition to the staggered application of substantive provisions, the Regulation establishes specific transitional rules for systems already on the market (Article 111). AI systems forming part of the large-scale EU IT systems listed in Annex X and placed on the market or put into service before 2 August 2027 must comply by 31 December 2030, and the requirements of the AI Act must also be taken into account in the periodic evaluations required under the relevant sectoral legislation. Other high-risk AI systems placed on the market or put into service before 2 August 2026 are required to comply only where significant design changes occur on or after that date. Providers and deployers of high-risk AI systems intended for use by public authorities must nevertheless ensure compliance by 2 August 2030, even where no such changes are made. Providers

of general-purpose AI models placed on the market before 2 August 2025 must comply with their applicable obligations by 2 August 2027.

This study was finalised on 15 November 2025. On 19 November 2025, the European Commission published the "Digital Omnibus" proposal, which suggests adjustments and clarifications concerning the wider digital regulatory framework, including provisions that interact with the AI Act.[220] At the time of writing, the proposal remains under negotiation and does not affect the applicability dates or obligations set out in Regulation (EU) 2024/1689.

[220] European Commission, *Digital Omnibus – AI Regulation Proposal*, 19 November 2025, https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

XIV. Concerns

A. List-based categorisation

The AI Act aims at a regulation that promotes the market while respecting fundamental rights and safety. It categorises systems based on risk, calibrating the level of regulation according to the degree of risk posed by different AI systems. The aim is to avoid both under-regulation (which fails to protect rights and other values) and over-regulation (which restricts innovation and the effective functioning of the single market). This list-based rather than principle-based approach to determining whether a system is classified as high risk is not without problems. It is extremely difficult to identify in advance the applications of systems that may lead to serious rights violations. As a result, systems currently classified as low risk may not be subject to regulation sufficient to prevent rights violations. This flaw is compounded by concerns that the provisions of the AI Act may displace (a) the more stringent rights protection provided by other EU legislation, and (b) the more stringent rights protection established at the national level by Member States. A further concern is who will perform the risk categorisation and what procedures the impact assessment will be conducted, so that it does not become a mere meaningless process.

B. Insufficient protection of rights

There is serious concern that the AI Act provides insufficient protection of fundamental rights in the case of AI systems classified as not high risk.

The criterion for classifying an AI system as "high risk", apart from AI systems that serve as safety components of regulated products, takes the form of a reviewable list of specific purposes for which the AI systems are used (Annex III). It is the development within these designated areas that makes an AI system "high risk". The relevant purposes are set out in Annex III and include biometric identification and categorisation

of individuals, access to and assessment of educational and vocational training institutions, recruitment and management of employees, law enforcement and administration of justice, access to and enjoyment of basic private and public services and benefits, as well as migration, asylum, and border control. It is, however, doubtful whether high-risk AI systems requiring enhanced regulation can be reliably identified in advance through predefined operational domains.

A classic example is one of the "high-risk" domains listed in Annex III, namely AI systems that affect "access to and enjoyment of essential private services and essential public services and benefits" (Annex III, point 5). How does this relate to AI systems used in the provision of healthcare services? Point 5(d) refers to "AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems". This description excludes non-emergency healthcare services. But if a general practitioner were to use an AI system to prioritise patients' appointment requests, the algorithm could systematically discriminate against patients who are women or members of racial and ethnic minorities, and still not fall within the existing "high-risk" category. This appears to underestimate the seriousness of such discrimination compared with other forms of harm falling within one of the listed areas.

This concern extends beyond health services, since the potential for AI systems to cause serious harm, such as breaches of non-discrimination rights, runs through all areas of operation. An example is algorithms that introduce racial discrimination in the allocation of cultural or recreational opportunities, which likewise do not fall within the existing list of designated sectors. If, for example, an algorithm regulating access to theatres or leisure centres were systematically to discriminate against children from ethnic minorities, serious harm would result. The list-based methodology, however, appears to take the perceived importance of a designated sector as the guide to the severity of the risk posed by deploying AI systems within it. As a result, it underestimates the pervasive character of the serious risks inherent in AI systems.

C. "Quasi-Directive" Regulation model

The model of the Regulation, which has many features of a Directive (a quasi-Directive approach) modelled on the GDPR, seems to leave Member States with significant discretionary choices, which may result in its non-uniform application. A typical example is the choice of supervisory authority, which may either be newly established or placed under the auspices of an existing body, such as the HDPA. The model preferred by the national legislator will likely indicate the intention either to grant autonomy to the new supervisory body or to place it under an existing one, which may reinforce its original orientation.

D. Multiple supervisory authorities

The role of the different actors involved in the AI Act may lead to a blurring of competences. It includes the European Artificial Intelligence Board as a regulatory body with representation of the Commission, Member States, the European Data Protection Supervisor, and subgroups on specific issues. This Board has been criticised for excluding stakeholder groups, lacking a defined organisational structure, and being unable to clearly define its tasks. A further complication arises from the delegation to the Commission of risk assessment responsibilities for updating the list of AI systems. This complexity is compounded by the supervisory authorities established under the sister instruments – the Digital Services Act, the Digital Markets Act, and others.

E. Lack of guidance

Uncertainty persists regarding the ability of citizens to challenge the outcomes of AI systems. The obligation to provide justification for decision-making raises questions about the content, nature, and depth of explanations of AI-based decisions. The scope of explanations is unclear at the level of communication, language, and presentation when individuals are subjected to emotion recognition or biometric categorisation systems. In healthcare, it is unclear when patients must be informed of the use of AI in medical decision-making. Quantitative risk assessment systems also face challenges, as no standardised method exists for evaluating

their performance. Assessing high-risk systems without clear guidance is therefore difficult.

F. Extended scope

The scope of the AI Act tends to be extremely broad. Its definition of AI may cover many systems related to everyday data processing, producing an overly inclusive scope where the only common denominator may be data processing. As a result, it becomes difficult to identify programmes that are not captured by the description of AI systems. The Act's scope has also been criticised for its limitations: its strong emphasis on software to the detriment of hardware, its neglect of relevant use cases and user organisations, and its disregard for the use of AI systems in certain sectors.

G. Competition with non-European systems

Over-regulation of AI may stifle innovation. The European Union is called upon both to resist and to compete with non-European AI products, primarily from the United States and China, which threaten to fracture the unity of AI philosophy and technology. The European Union is lagging behind in initiatives in this area and any overshadowing of the market by others would undermine the entire effort of human-centred regulation. The key question is how the EU can compete on equal terms with non-European markets without betraying its constitutional identity.

H. Extraterritoriality

The AI Act, like the GDPR, appears to challenge constitutional assumptions that war and military intervention have not managed to shift.[221] Its ambition seems excessive, particularly given that the extraterritoriality model of the GDPR has not, in practice, been vindicated. Fines imposed

[221] Fereniki Panagopoulou-Koutnatzi, "Constitutional Implications of Mechanisms Extending the Protection of Personal Data beyond the EU: Extraterritorial Application of the GDPR and Cross-Border Data Transfers," *Public Law Review* 4 (2019): 504 ff. (509).

by national authorities on non-European operators are often merely cautionary,[222] remaining effectively unpaid,[223] thereby undermining the ambitious plans for extraterritorial application.

[222] Souzana Papakonstantinou, "HDPA Decision 35/2022. Imposition of a €20,000,000 Fine on Clearview AI, Inc. for Violation of the Principles of Lawfulness and Transparency," *e-Politeia: Journal of Legal Theory and Practice* 6 (2023): 268 ff. (279).

[223] A characteristic example is the €20,000,000 fine imposed by the HDPA pursuant to its Decision No. 35/2022.

SPECIAL SECTION: Constitutional issues for examination

The AI Act seeks to address, on the basis of the principle of proportionality, issues requiring particular attention. Some of these are discussed in the following chapters.

I. Biometric identification

A. Introduction

The AI Act provides flexibility clauses for Member States regarding enforcement measures. A typical example is biometric identification. This is either permitted as a measure to safeguard national security or, if it does not fall within the narrow interpretation of national security, it may fall within the cases set out in Article 5(1)(h). In short, the discretion of the legislator is broad, and it is for the legislator to decide what kind of framework is preferred. Such flexibility, however, may undermine the uniform application of the AI Act. A key consideration is whether the legislator opts for a structured framework that facilitates the work of the police authorities or for a looser framework that does not, leaving the police reliant on half-measures, such as reliance on illegal private cameras, which do not protect citizens' rights.

B. Terminology

According to Article 3(35), 'biometric identification' means the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database. Law enforcement authorities use identification systems when comparing a captured image with an existing database, such as a database of photographs of wanted persons or holders of driving licences. The system scans the new image (possibly from CCTV footage in a public space or from a camera at the scene), creates a template, and then attempts to match it with a previously reg-

istered individual.[224] At the same time, many services are based on these functions, such as connecting to phones, sorting and organising family photos, authenticating on platforms, and creating consumer profiles for personalised recommendations.[225] Hotels, conferences, and concerts are experimenting with the use of facial recognition to create personalised experiences for members and registered users, enabling smooth passage from taxi to lobby, room, or check-in to a show or event, with minimal delays, queues, or other friction points along the way.[226] Companies also use facial recognition to assist people who are blind or have low vision via audio or Braille interfaces. Other programmes deploy facial recognition features to help people with autism interpret emotional expressions.[227]

C. Importance

Since the face is a unique part of the human body, closely linked to personal, social, and institutional identity, whoever controls facial recognition technology exercises enormous power.[228] Facial recognition technologies can be a valuable tool for strengthening national security by offering rapid and efficient identification capabilities that can contribute to security, such as quickly identifying suspects who pose a threat, locating missing or trafficked persons by matching their images to databases, identifying people in need of help during emergencies, or ensuring streamlined and accurate identity verification at borders.[229] In other words, national security in the age of AI involves the use of facial recognition technologies to prevent, respond to, and recover from events that may compromise the safety of the general public. While these systems offer potential advantages for law enforcement and security applications, their application in public places may be considered intrusive, "evoke a feeling

[224] Evan Selinger and Brenda Leong, "Facial Recognition Technology Primer: What Is It and How Is It Used?," in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford: Oxford University Press, 2021), 590 ff.
[225] Ibid., 591.
[226] Ibid.
[227] Ibid.
[228] Ibid.
[229] Ibid.

of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights" (see Recital 32).

D. The issue of public trust in the United States (U.S.)

The use of facial recognition technology affects the level of trust between citizens and law enforcement authorities. The Georgetown Law Center on Privacy and Technology has reported a number of troubling findings regarding the accuracy and social impact of facial recognition technology in the law enforcement context.[230] Some of the main findings of the U.S. reports criticise, among other things, the following:[231] First, law enforcement agencies have purchased city-wide facial surveillance networks capable of scanning residents' faces in real time as they walk down the street. In addition, law enforcement agencies have not always been transparent with the public about how they use facial recognition technology. Second, a range of actors have used improper practices (such as, for example, submitting unsuitable sketches or celebrity photos, and altering low-quality images, including copying and pasting facial features from another person). Third, law enforcement bodies query databases linking names and faces that cover over half of U.S. adults without their express consent, and government agents have used legally questionable practices when deploying facial recognition systems to monitor international airport departures. Recent research on police use of facial recognition already shows that trust among younger people and racial-minority groups is significantly lower than among older white adults.[232] Misuse of biometric tracking can erode consumer and stakeholder confidence in the fairness, equity, and reliability of these processes and, depending on the context, cause harms affecting individuals, groups or society at

[230] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations* (Washington, DC: Center on Privacy & Technology at Georgetown Law, 2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf

[231] Ibid.

[232] Evan Selinger and Brenda Leong, "Facial Recognition Technology Primer: What Is It and How Is It Used?," in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford: Oxford University Press, 2021), 590 ff.

large.[233] Examples of harm include loss of opportunities in employment, insurance and social security benefits, housing, and education. A typical example is an employer using a biased face-scanning system during interviews to rate a candidate's "friendliness" or cultural "fit" and ultimately treating that output as decisive over the candidate's CV, performance, or other qualifications.[234]

Overall, these harms can negatively affect society as a whole, undermining people's confidence in their ability to be treated fairly, succeed on their own merits, and be trusted.

E. The Union's legislative framework

As noted in the General Part, according to Article 5(1)(h), the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement shall be prohibited, unless and in so far as such use is strictly necessary for one of the following objectives:

(a) The targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons.

(b) The prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack.

(c) The localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Furthermore, according to Recital 24, if, and insofar as, AI systems are placed on the market, put into service, or used with or without mod-

[233] Ibid.
[234] Ibid.

ification of such systems for military, defence or national security purposes, those should be excluded from the scope of the Regulation. As far as military and defence purposes are concerned, this exception is justified both by Article 4(2) TEU and by the specificities of Member States' defence policy and the Union's common defence policy covered by Chapter 2 of Title V TEU, which are subject to public international law. Public international law is therefore the most appropriate legal framework for regulating AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exemption is justified both by the fact that national security remains the exclusive competence of Member States under Article 4(2) TEU, and by the specific nature and operational needs of national security activities and the specific national rules applicable to those activities. Even so, if an AI system developed, placed on the market, put into service or used for military, defence, or national security purposes is also used, whether temporarily or permanently, for other purposes – such as civilian, humanitarian, law enforcement, or public security purposes – that system falls within the scope of the AI Act. In that case, the entity using the AI system for purposes other than military, defence, or national security, should ensure that the AI system complies with the Act, unless it already does so.

AI systems placed on the market or put into service for an exempted purpose, namely a military, defence, or national security purpose, and for one or more non-exempted purposes, such as civilian or law enforcement, fall within the scope of the Act. Providers of such systems must ensure compliance with it. In such cases, the fact that an AI system may fall within the scope of the AI Act should not affect the ability of entities carrying out national security, defence, and military activities, irrespective of the type of entity performing those activities, to use AI systems for those exempted purposes. An AI system placed on the market for civilian or law enforcement purposes and then used, with or without modification, for military, defence, or national security purposes does not fall within the scope of the AI Act, regardless of the type of entity performing those activities.

The AI Act therefore prohibits real-time biometric identification systems when used in publicly accessible areas. These systems are capable of

recording and analysing biometric data, such as facial features, iris patterns, fingerprints, and voice patterns, in real time and remotely, without requiring direct interaction or physical contact with the person being identified. Moreover, it prohibits the use of AI systems that allow biometric categorisation of natural persons on the basis of certain narrowly defined characteristics. These systems process biometric data to infer or deduce a person's race, political opinions, trade union membership, religious or philosophical beliefs, or sexual orientation. These systems are prohibited, except when used to identify victims. The filtering of biometric datasets in law enforcement remains possible (Article 5(1)(g)). The Act introduces a partial prohibition on individual preventive policing. The prohibition covers systems that assess or predict an individual's risk of committing a criminal offence, based solely on that individual's profile or an assessment of their personality traits and characteristics. The use of AI systems that support human assessment of involvement in a crime that has actually been committed is permitted, as this is not considered a prediction, but an assessment based on objective and verifiable evidence directly linked to an actual criminal activity (Article 5(1)(d)). While remote biometric post-event identification systems are not explicitly prohibited, their classification in a high-risk category requires an external conformity assessment (Recital 125).

Further to the above, the Act imposes additional obligations on deployers of post-event biometric surveillance systems (Article 26(10)). Specifically, in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-event remote biometric identification shall request authorisation, ex-ante, or without undue delay and no later than 48 hours. Such authorisation is issued by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of that system, except when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Moreover, the Act expressly prohibits the untargeted use of post-event remote biometric identification in law enforcement. It also takes a clear stance on preventing the creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage

(Article 5(1)(e)). Untargeted data extraction, such as from a website, is the collection of facial images without a specific, predefined purpose. Beyond the necessary and proportionate use of facial recognition technology, huge datasets may be accumulated without clear objectives. This prohibition seeks to address concerns about mass surveillance and possible violations of fundamental rights, in particular the right to privacy.

Taking into account the specificities of law enforcement activities, there are limited exceptions to the prohibited AI practices, designed to equip law enforcement authorities with the tools needed to combat modern crime effectively. For example, under Article 46(2) of the Regulation, law enforcement authorities or civil protection authorities may put a specific high-risk AI system into service without the authorisation referred to in paragraph 1 of said Article, provided that such authorisation is requested during or after the use without undue delay. If the authorisation referred to in paragraph 1 is refused, the use of the high-risk AI system shall be stopped with immediate effect and all the results and outputs of such use shall be immediately discarded. Additionally, following Article 5(1)(h), the use of real-time remote biometric identification systems in publicly accessible spaces is possible only for exhaustively defined law enforcement purposes. These purposes include the targeted search for victims, the prevention of terrorist attacks and threats to life, and the identification of suspects involved in serious and organised crime. The circumstances under which law enforcement authorities may use real-time biometric surveillance systems are subject to specific conditions (Article 5(2)(a)). In particular, use is limited to confirming the identity of specific targeted individuals. This means real-time biometric monitoring must not be used for indiscriminate surveillance or broad identification purposes. The use of real-time biometric monitoring must be strictly necessary and targeted. This includes limits on the individuals to be identified, the locations, the temporal scope, and the use of a closed dataset derived from lawfully obtained video footage. Law enforcement authorities are required to carry out a fundamental rights impact assessment before using these systems. That assessment evaluates the potential impact on individuals' rights and freedoms.

The use of such systems in publicly accessible areas for law enforcement purposes must be explicitly and specifically authorised by a judicial

authority, or by an independent administrative authority. Although the AI Act provides exceptions, authorisation should ideally be obtained before the system is used, or within 24 hours. Exceptions for the use of real-time biometric monitoring for law enforcement purposes are possible only where expressly provided for in national law. Therefore, Member States have flexibility to decide whether such exceptions apply domestically, to impose stricter conditions, or even to enact a blanket ban. The competent market surveillance authority and the national data-protection authority must be informed of each use of a "real-time biometric identification system". These systems enable targeted and effective interventions, while helping avoid disproportionate stop-and-search measures based on race, nationality, or other distinguishing physical characteristics.

F. The concept of publicly accessible space

According to Article 3(44) of the Regulation, 'publicly accessible space' means any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions.

Under Recital 19, the notion of 'publicly accessible space' should be understood as referring to any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned, irrespective of the activity for which the space may be used, such as for commerce, for example, shops, restaurants, cafés; for services, for example, banks, professional activities, hospitality; for sport, for example, swimming pools, gyms, stadiums; for transport, for example, bus, metro and railway stations, airports, means of transport; for entertainment, for example, cinemas, theatres, museums, concert and conference halls; or for leisure or otherwise, for example, public roads and squares, parks, forests, playgrounds. A space should also be classified as being publicly accessible if, regardless of potential capacity or security restrictions, access is subject to certain predetermined conditions which can be fulfilled by an undetermined number of persons, such as the purchase of a ticket or title of transport, prior registration or having a certain age. In contrast, a space should not be con-

sidered to be publicly accessible if access is limited to specific and defined natural persons through either Union or national law directly related to public safety or security or through the clear manifestation of will by the person having the relevant authority over the space. The factual possibility of access alone, such as an unlocked door or an open gate in a fence, does not imply that the space is publicly accessible in the presence of indications or circumstances suggesting the contrary, such as signs prohibiting or restricting access. Company and factory premises, as well as offices and workplaces that are intended to be accessed only by relevant employees and service providers, are spaces that are not publicly accessible. Publicly accessible spaces should not include prisons or border control. Some other spaces may comprise both publicly accessible and non-publicly accessible spaces, such as the hallway of a private residential building necessary to access a doctor's office or an airport. Online spaces are not covered, as they are not physical spaces. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

It should be noted that the term refers to a physical space, and not a virtual one. In summary, publicly accessible spaces include business premises (restaurants, cafés, banks, hotels), sports facilities (swimming pools, gyms, stadiums), public transport and associated facilities (buses, metro and railway stations, airports), entertainment venues (cinemas, theatres, museums, concert halls), recreational areas (playgrounds, parks), and public spaces in general (public roads, squares).[235]

The term "public accessibility" means that any person can visit the space, such as a public market.[236]

G. The exception of national security

Protection from biometric monitoring on grounds of national security appears to promote the interests of the State, but abuse of this exception may give rise to particular concern. The national security requirement is

[235] Christiane Wendehorst, "Art. 3," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 304.

[236] Ibid., para. 306.

overly general and vague, and open to abuse.[237] It is a vague concept, as it is impossible to assess objectively whether, and from where, an "imminent threat" arises.[238]

The term "national security" does not have a universally agreed definition, as its interpretation varies between different states, regimes, and individuals.

In the Greek legal order, "national security" appears as a constitutional term in Articles 5A, 19(1), and 48(1) of the Constitution. Beyond these references, the core of the concept is protected, directly or indirectly, in other constitutional provisions. In its narrower form of "national defence", it is protected under Article 14(3) (publications endangering national defence), Article 18(3) (requisition of property), Article 22(4) (requisition of personal services), Article 30(4) (extension of the term of office of the President of the Republic during war), and Article 53(3) (extension of parliamentary term during war). National security is also indirectly protected in constitutional provisions regulating the status of military personnel in a special relationship of authority with the State (Article 23(2) (prohibition of military strike), Article 29(3) (prohibition of political activities by military personnel), Article 56(1), (3), and (4) (ineligibility of military personnel for election), and Article 96(4) and (5) (jurisdiction of special military courts)), as well as in Article 4(3b) (loss of Greek nationality where a person undertakes service in a foreign State contrary to national interests), and Article 28(2a) (conferral of powers on international organisations for the purpose of serving important national interests). A threat against national security may also trigger the application of constitutional provisions intended for addressing emergency needs, such as Article 5(4b) (individual administrative measures restricting movement), Article 41(2) (dissolution of Parliament for a national issue of exceptional importance), Article 44(1) and (3) (acts of legislative content and addresses by the President of the Republic), Article 76(4) and (5) (limited debate and urgent voting of bills on proposal of

[237] Aristovoulos Manesis, *Individual Liberties, vol. A*, 3rd ed. (Thessaloniki: Sakkoulas, 1981), 240.

[238] Nikos Alivizatos, *The Constitutional Position of the Armed Forces, I. The Principle of Political Control* (Athens–Komotini: Ant. N. Sakkoulas, 1987), 199 ff.

the Government), and Article 103(2) (recruitment of staff to meet unforeseen and urgent needs).

"National security" refers to the protection of the country from external threats that undermine its national independence, territorial integrity, peaceful relations with other states, or sovereign rights (such as the exploitation of declared EEZs).[239] The term is linked to the state's position in its external relations (international standing of the state) and is affected by fluctuations in external relations with other states or international organisations.[240] According to Alivizatos,[241] "the core of national security is related to the state's status in its external relations. From this perspective, national security is clearly distinguished from public security, which concerns the protection of the Constitution, the constituted powers, and state institutions from internal threats, and from public order, which, aiming at the legal good of 'common peace', primarily seeks to safeguard private rather than civil society. As a legal good, national security is also linked to the protection of the armed forces, possibly the security forces, and the civilian services (counterintelligence and intelligence services in general) whose main mission is its defence, and which may also be threatened from within. This is where national security and public security converge [...]". The term "national security" does not encompass public security in general, but the defence of the country against external threats.[242]

Therefore, the grounds of national security should not extend to reasons of public order, mere facilitation of police work, or the convenience of other administrative authorities.[243]

As an exception, it should be interpreted narrowly, and it must strictly satisfy necessity and proportionality in light of the legitimate aim

[239] Efstratios Efstratiou, *National Security as an Exception Clause in the Greek Constitution and the Treaties of the European Union* (PhD diss., Aristotle University of Thessaloniki, Faculty of Law, 2024, unpublished), 23.

[240] Ibid., 23.

[241] Nikos Alivizatos, *The Constitutional Position of the Armed Forces, vol. I: The Principle of Political Control* (Athens–Komotini: Ant. N. Sakkoulas, 1987), 199 ff.

[242] Panagiotis Tsiris, *The Constitutional Safeguard of the Right to Communication* (Athens–Komotini: Ant. N. Sakkoulas, 2002), 110 ff.

[243] Prodromos D. Dagtoglou, *Constitutional Law, Individual Rights* (Athens–Thessaloniki: Sakkoulas, 2022), 361, para. 542.

pursued.[244] Invoking national security indicates that there is, at least at that time, no offence – certainly not a particularly serious one – and no pending criminal prosecution.[245] The information sought concerns external security, because internal security is framed in the Constitution as "public security" (Article 11(2)) and "public order" (Articles 13(2) and 18(3)).[246] In criminal law, the constitutional concept of national security aligns with the legal interest of the country's international standing, encompassing protection of territorial integrity, international peace, defence capability, and state secrets, and is codified in Articles 138–152 of the Penal Code.[247]

The European Court of Human Rights has extensive case law on measures justified by national security.[248] While acknowledging a wide margin of appreciation for domestic legal orders, the Court stresses that the existence of a "pressing social need" justifying national security grounds must be adequately examined by the competent authorities.[249]

To safeguard the rule of law in a democratic society, a blanket national security exception should be avoided, because it creates a risk of abuse. Accordingly, any exception should be rigorously assessed case by case, in line with the EU Charter of Fundamental Rights and the case law of the CJEU. If any exception is contemplated, it must be tightly circumscribed, and any public authority invoking it should be subject to robust transparency and accountability obligations. This includes conducting risk

[244] Giorgos Karavokyris, "The Face of Democracy," *Constitutionalism*, August 16, 2022.

[245] Evangelos Venizelos, "The Constitutional Limits on Lifting the Telephone Confidentiality of Citizens and Politicians for Reasons of National Security – The Androulakis Case," *Constitutionalism*, August 27, 2022.

[246] Ibid.

[247] Ibid.

[248] *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, Eur. Ct. H.R., judgment of 11 January 2022, paras. 291 ff., 394 ff.; *Centrum för Rättvisa v. Sweden*, no. 35252/08, Eur. Ct. H.R., judgment of 19 June 2018, para. 86 ff.

[249] *Dumitru Popescu v. Romania (no. 2)*, no. 71525/01, Eur. Ct. H.R., judgment of 26 April 2007, para. 61 ff.; *Amann v. Switzerland*, no. 7798/95, Eur. Ct. H.R., judgment of 16 February 2000, para. 76; *Valenzuela Contreras v. Spain*, no. 58/1997/842/1048, Eur. Ct. H.R., judgment of 30 July 1998, para. 49 ff.; *Leander v. Sweden*, Series A no. 116, Eur. Ct. H.R., judgment of 26 March 1987, para. 59; *Klass and Others v. Germany*, Series A no. 28, Eur. Ct. H.R., judgment of 6 September 1978, para. 48.

and impact assessments prior to deployment and throughout the period of use.

H. Concluding remarks

Biometric monitoring poses an unacceptable risk that society should not, in principle, accept. Such monitoring appears incompatible with human dignity, which underpins European civilisation. Exceptionally, it may be permitted in narrowly defined cases, which must be set out with precision in legislation. It follows from the above that biometric monitoring should be a measure of last resort. The necessary conditions for applying biometric surveillance are as follows:

First, the principle of proportionality must be respected.[250] This means that the benefits for national security must be significant, and the risks to privacy must be mitigated. Consequently, indiscriminate scanning of everyone's faces should not occur.

Second, legislative clarity is required, with explicit statutes delimiting permissible use of facial recognition in line with European values and human rights.

Third, a common EU operational framework is needed. This implies that there will be no divergence between Member States.

Fourth, design and governance should be inclusive.[251] This entails public dialogue with all stakeholders, including government authorities, technology providers, data providers, data protection authorities, and civil society.

Fifth, robust ethical oversight is required through an independent ethics committee to guide and oversee development, and judicial authorisation and supervision for case-specific use.[252] It should also be ensured

[250] Carissa Véliz, "The Surveillance Delusion," in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford: Oxford University Press, 2021; online ed., Oxford Academic, November 10, 2021), https://doi.org/10.1093/oxfordhb/9780198857815.013.30

[251] Kat Holmes, *Mismatch: How Inclusion Shapes Design* (Cambridge, MA: MIT Press, 2018), https://doi.org/10.7551/mitpress/11647.001.0001

[252] Luciano Floridi, *The Ethics of AI* (Oxford: Oxford University Press, 2023), 105, discussing the importance of "context" in choosing appropriate justice measures.

that the use of the technology by the police is subject to multi-level oversight.

Sixth, effective error management is required through procedures to remedy misidentification and unauthorised access.

Seventh, logs must be kept for the purposes of explainability, recording all changes and deletions made to a record.

Eighth, the system must be based on the principle of transparency and algorithmic fairness, with a mandatory ability to audit algorithms to ensure fairness and accuracy.

Ninth, controlled environments must be introduced for system audits and test environments to examine these technologies, explore their use in law enforcement, and evaluate them under higher levels of scrutiny to ensure compliance with ethical, legal, and human rights standards.

Tenth, accountability is required for the consequences of actions caused by an algorithm.[253]

Eleventh, AI literacy is required, providing a legal framework for ongoing training and educational programmes on AI for law enforcement and civil society.

The successful integration of AI technologies in law enforcement requires public trust and acceptance. This necessitates investment in public participation, education, awareness raising, and feedback mechanisms. Strengthening cooperation and knowledge sharing through cross-departmental collaboration, partnerships with academia and industry, and the involvement of civil society is essential for the successful integration of AI in law enforcement.

[253] Ibid.

II. Employment and the workplace

A. General remarks

AI has entered many aspects of modern life and can be expected to affect work in various ways. Its advent creates new occupations but also eliminates others. Concerns are expressed that AI will lead to soaring unemployment through the elimination of manual occupations and jobs requiring light or low-level intellectual skills. AI has already eliminated, and is expected to eliminate even more, repetitive and predictable jobs.[254] These concerns are countered by the argument that AI will require new skills and create new occupations.[255] Some tasks may be completely replaced, but a multitude of new requirements will be transformed into new occupations.[256] At this point there is also a creative convergence of automation and the utilisation of human labour.[257]

At the same time, the workforce is subject to algorithmic management.[258] This means that it is (pre)selected, (pre)evaluated, controlled, and monitored on the basis of an algorithmic process. This constitutes a new form of algorithmic management.[259] It refers to the practices of

[254] Anastasios G. Gatzoufas, "Everyday Life in the Age of Artificial Intelligence," *dialogos* 14 (2024): 293 ff. (300).

[255] Giorgos Theodosis, "Article 21," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 452 ff. (454).

[256] Giorgos Giannakopoulos, *Artificial Intelligence: A Discreet Demystification* (Athens: Ropi, 2020), 33.

[257] Dimitris Travlos-Tzanetatos, *Labour Law in the Fourth Industrial Revolution: Digitalisation, Robotics and Artificial Intelligence* (Athens–Thessaloniki: Sakkoulas, 2019), 253.

[258] Giorgos Theodosis, "Article 21," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 452 ff. (454).

[259] Matina Giannakourou, "The Regulation of Algorithmic Labour Administration in the Draft Legislative Initiatives of the EU: Quo vadis, Europa?," in *Artificial Intelligence and Labour Law*, ed. Matina Giannakourou and Christina Deliyianni-Dimitrakou, *Labour Law Review* (2023): 645 ff. (646).

planning, organising, and managing employees via digital platforms.[260] It involves the full or partial delegation of personnel management functions and the employer's powers that constitute managerial authority to AI systems, algorithms, or automated decision-making systems.[261]

The fundamental aim of AI regulation in the workplace is to serve human well-being, not undermine it. Yet can management truly be delegated to an algorithm?[262]

B. Managing employees through artificial intelligence

In the workplace, extensive data concerning the employee are collected from multiple sources (internet, social networks, evaluations, and so on)[263] and include the employee's CV, degrees, certificates, and skills. Processing these data seeks to create a model of which candidate is suitable or unsuitable for filling a particular post, or even who should be promoted[264] or dismissed. This may initially sound positive, as it saves resources and time. Yet it is also linked to negative consequences when discrimination and prejudice intervene, potentially affecting specific population groups, such as vulnerable groups, and aggravating social inequalities.[265] Personal data collected from various devices are analysed and reused for automated or semi-automated decision-making.[266] Algorithms can, with a certain degree of autonomy and minimal human supervision, select useful outcomes by identifying patterns in existing

[260] Ibid.

[261] Ibid.

[262] Lilian Mitrou, "Can the Algorithm Govern?," in *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, ed. Lilian Mitrou (Heraklion: University of Crete University Press, 2023), 253 (265).

[263] Giorgos Theodosis, "Article 21," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 452 ff. (458).

[264] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 37.

[265] Antonio Aloisi, "Algorithmic Management," in *Artificial Intelligence and Labour Law*, ed. Matina Giannakourou and Christina Deliyianni-Dimitrakou, *Labour Law Review* (2023), 621 ff. (636).

[266] Ibid., 624.

data that predict future outcomes.[267] At the same time, lack of objectivity in data processing can lead to inaccurate estimates.[268] When an algorithm has been trained that managerial posts are occupied by white men, it will select a white man. Moreover, processing the vast amount of an employee's data may produce a detailed psychogram and affect the right to informational self-determination. This blurs the boundaries between personal and private life by mixing professional data with special categories of data (sensitive data), enabling employers to observe, infer, direct, and even prevent human behaviour.[269] A new form of algorithmic employer is emerging on the horizon.[270] AI assists employers in decision-making, or even makes decisions on their behalf.[271] Beyond the risks of algorithmic bias, which may cause discrimination, exclusion, or disadvantage,[272] there also emerges a lack of human contact and workplace alienation through the platformisation of work.[273]

C. The response of the EU and national legislator

The Regulation clarifies in Recital 9 that AI must not undermine the right to work. In particular, the Regulation must not affect Union law on social policy and national labour law, in compliance with Union law, concerning employment and working conditions, including health and safety at work, and the relationship between employers and workers. It should also not affect the exercise of fundamental rights as recognised in the Member States and at Union level, including the right or freedom to

[267] Ibid., 631.

[268] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 37.

[269] Antonio Aloisi, "Algorithmic Management," in *Artificial Intelligence and Labour Law*, ed. Giannakourou and Deliyianni-Dimitrakou, *Labour Law Review* (2023), 621 ff. (632).

[270] Ibid., 624.

[271] Ibid., 631.

[272] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 25.

[273] Rolf Wank, "Algorithmic Management and the Individual Employment Contract," in *Artificial Intelligence and Labour Law*, ed. Matina Giannakourou and Christina Deliyianni-Dimitrakou, *Labour Law Review* (2023), 675 ff. (677).

strike or to take other action covered by the specific industrial relations systems in Member States as well as the right to negotiate, to conclude and enforce collective agreements or to take collective action in accordance with national law. Lastly, it should also not affect the provisions aiming to improve working conditions in platform work laid down in a Directive of the European Parliament and of the Council on improving working conditions in platform work.

According to Annex III, the following are classified as high-risk schemes:

(a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates.

(b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

Also, according to Article 26(7), putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information shall be provided, where applicable, in accordance with the rules and procedures laid down in Union and national law and practice on information of workers and their representatives.

To prevent the above risks, the Union legislator has prohibited practices that endanger safety, fundamental rights, and health. Accordingly, subliminal manipulation is prohibited. For example, it would be prohibited if warehouse management software pressured employees, through a rating or ranking system, to work increasingly faster, even where this involved breaching safety rules.[274] It is also prohibited to operate sys-

[274] Rolf Schwartmann, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum, *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten* (Munich: C.H. Beck, 2025), 37.

tems that degrade vulnerable groups, such as older people, persons with disabilities, and low income groups. An example of such an application would be AI-based shift scheduling that treats single parents with childcare responsibilities as less flexible, and therefore less efficient. By contrast, such systems could be permissible if used to support these groups, for instance by offering flexible working arrangements as an optional choice. Likewise, emotion recognition in the workplace is prohibited, unless strictly necessary for health or safety reasons. To this end, employers are not allowed to assess their employees' facial expressions, voice, or biometric data through AI to monitor their motivation, satisfaction or loyalty.[275] Similarly, facial recognition systems that monitor employees' attention, distraction, or irritation during video conferencing are impermissible.

AI should not be used to keep individuals permanently connected to technology and to work, hence the right to disconnect must be recognised. Disconnection includes not only refraining from replying to employer messages, but also not receiving such messages outside working hours. The right to digital disconnection after working hours is a fundamental right of employees. It is vital and directly linked both to the right to privacy, the protection of personal data, and respect for private and family life (Articles 9(1)(b) and 9A of the Greek Constitution, and Article 8 ECHR), and to the balance between professional and personal life.[276] This right is enshrined in Article 18 of Law No. 4807/2021 for public sector employees, and Article 67(10) of Law No. 4808/2021 for private sector employees. It protects employees' right to disconnect, without detriment, from the digital media (software, digital platforms, social networks, wireless connections, e-mails, internet/intranet) used to organise work. Finally, Article 9 of Law No. 4961/2022 imposes an obligation to provide information on the use of AI in the workplace.

[275] Ibid.

[276] Hellenic Data Protection Authority (HDPA), *Guidelines 1/2021: On the Application of Personal Data Protection Rules in the Context of Teleworking*, 7.

D. Artificial intelligence as a tool of public policy to strengthen the protection of workers

The use of AI systems can enhance worker protection by facilitating inspections of undeclared work by the Labour Inspectorate. The digital worker's card supports the creation of procedures to quickly identify potential infringements, classify incoming complaints, and standardise decision-making processes for assessing infringements and imposing proportionate fines. In all this, it is essential to safeguard employees' personal data and ensure that human oversight is maintained.

E. Artificial intelligence and the future of work

The advent of AI is seen by some as a threat to the future of work. Traditional occupations will disappear, but new ones adapted to the needs of AI will emerge. Therefore, interdisciplinary research and documentation on protecting workers in occupations affected by digitisation must therefore be strengthened, making systematic use of strategic foresight methods and tools. Emphasis should be placed on reskilling and upskilling, along with qualification certification mechanisms, particularly in sectors of importance to the Greek economy, such as tourism, catering, shipping, the environment, and culture. AI should not be regarded as a means of replacing human labour solely to reduce costs. It should instead be regarded as a means of enhancing quality of life, for instance by reducing working hours and increasing leisure time. From this perspective, AI should not be seen as a substitute for humans, but as a technology that can enhance their capabilities, opening new avenues for cooperation between AI and humans.[277] In this direction, particular emphasis should be placed on training workers to adapt to the new environment created by the introduction of AI in the workplace.

[277] Implement Consulting Group, "The Economic Opportunity of Generative AI in Greece," https://implementconsultinggroup.com/article/the-economic-opportunity-of-generative-ai-in-greece

F. Concluding remarks

The new challenges brought by the advent of AI in the workplace require training in new AI-related skills. At the same time, they demand respect for workers' rights. The use of AI as a high-risk practice must not exceed the limits of human endurance. In general, the use of AI must align with respect for labour and social rights, and above all, with respect for the dignity of workers. This needs to be taken into account especially in relation to performance monitoring and evaluation.

It is considered appropriate to extend traditional labour rights (such as trade union rights, and health and safety protection) fully to freelancers and to establish oversight of the algorithmic management of workers. The main challenge for the regulator of algorithmic labour law is to establish a framework where innovative technologies are used to benefit, rather than harm, workers.[278]

[278] Antonio Aloisi, "Algorithmic Management," in *Artificial Intelligence and Labour Law*, ed. Giannakourou and Deliyianni-Dimitrakou, *Labour Law Review* (2023), 621 ff. (644).

III. Artificial intelligence and democracy: Towards digital authoritarianism or a democratic upgrade?

A. Introduction

Do robots vote? Do machines make decisions instead of us? No (at least not yet), but this is something that could happen. The discussion of this topic will begin with two flashbacks, one to the past and one to the future.

When drafting the United States Constitution, the Founding Fathers decided that enslaved people would be counted as three-fifths of a free citizen. This provision addressed the dilemma of whether enslaved people should be included in a state's population count. The clause effectively increased the population figures of the slaveholding states. As a result, these states were politically strengthened, gaining additional representation at the federal level and thus greater influence over the country's legislative process.

If robots were ever to be counted as part of the electorate, by what criteria would they cast their vote?

The impact of AI on democracy is a complex issue that requires detailed study and careful regulation. This is because the electoral process, although not determined in its entirety, is nonetheless greatly influenced by AI applications. New types of online campaigns, driven by AI applications, are replacing traditional ones. In the 18th century, the coffee shop was the hub of the public sphere; in the 21st, that role is taken by social media.[279] Platforms have amplified the voice of ordinary citizens in

[279] Jeffrey W. Howard, "Extreme Speech, Democratic Deliberation, and Social Media," in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford: Oxford University Press, 2021), 181 ff. (181).

ways that were unimaginable only a few years ago. With a device in their pocket, everyone can engage in countless exchanges with fellow citizens on matters of public policy. Where once views on political issues could be shared only with neighbours, comments can now be republished and seen by millions.

The potential to manipulate voters and indirectly influence election outcomes should not be overlooked. Voter manipulation has always been part of traditional political campaigns; the difference nowadays, however, is that online manipulation often occurs without people's awareness, for instance through the monitoring of our behaviour on social media.[280] At the same time, the positive impact of AI in strengthening democratic institutions by creating new forums for participation in decision-making deserves equal attention.

In this context, the potential risks that AI tools pose to democratic processes are first examined. Attention is then given to the ways in which AI might enhance these processes and to the possibilities for the technology itself to be democratised through the opportunities it creates. Third, the impact of AI on the system of representation is considered. Finally, recommendations and concluding remarks are set out.

B. Risks posed for democracy

The misuse of AI tools can undermine democratic political processes or manipulate individuals through targeted strategies, destabilising democracy.[281] The potential risks are many and far from negligible.

[280] Fereniki Panagopoulou-Koutnatzi, *Artificial Intelligence: The Path to a Digital Constitutionalism – An Ethical-Constitutional Approach* (Athens: Papazisis, 2023), 115. See also the case of the British consulting firm Cambridge Analytica, which in the 2010s collected personal data from millions of Facebook users without their consent, mainly for political advertising purposes.

[281] Raluca Csernatoni, "Can Democracy Survive the Disruptive Power of AI?," Carnegie Endowment for International Peace, December 18, 2024, https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en

1. Disinformation

The operation of algorithms, and the connections they create between individuals, carry considerable weight for the democratic principle. Public debate can be undermined through the mass dissemination of false information.[282] A form of targeted disinformation is produced, a distortion of reality[283] into which one can easily slip without realising it and from which it is extremely difficult, from a technical perspective, to escape. Facts and information are "manufactured" by digital media and become products of algorithmic choices.[284] This type of targeted information can influence electoral outcomes and, to a large extent, the democratic principle,[285] in the sense that elections are ultimately not decided by the people but by interest groups with the technical capacity to shape the popular will. In this respect, disinformation constitutes a threat to liberal democracy and its institutions.[286] It is crucial for the proper functioning of democracy and the untainted expression of the will of the people in elections.[287] Electoral processes can be undermined through practices such as the dissemination of intentional and uninten-

[282] Evripidis Stylianidis, "Article 5A," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 145 ff. (153).

[283] Lilian Mitrou, "Digital Democracy, Participation and Threats," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 53 ff. (78 ff.).

[284] Charalampos Tsekeris, "Human Communication in the Whirlwind of the 'Strange Magic' of Social Networks," *Economic Review*, April 22, 2024, https://www.economia.gr/

[285] Council of Europe, *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications*, March 2018, available at: https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

[286] Lilian Mitrou, "Digital Democracy, Participation and Threats," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 82.

[287] Lina Papadopoulou, "Fake News and Hate Speech," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 99 ff. (117).

tional disinformation, the spread of deepfake content,[288] or the manipulation of individuals through targeted strategies. The misuse of such technologies, for instance the creation of videos by algorithms that distort reality so that the line between true and false[289] becomes difficult to discern, poses a serious threat to democracies. It enables malicious actors, ranging from political opponents to foreign adversaries, to manipulate public perceptions, disrupt electoral processes, and amplify disinformation.[290] Particularly dangerous in this respect are the texts generated by generative AI; as these systems produce highly persuasive material, they allow both state and non-state actors to disseminate disinformation and harmful narratives.[291]

Generative AI models played a significant role in the 2024 US presidential election campaign, with fake images and deepfakes created by AI flooding social media platforms.[292] Fabricated images appeared on both sides: Trump reposted an AI-generated picture showing singer Taylor Swift endorsing his campaign, something she never did, while Democrats circulated AI-generated images of Trump being arrested.[293]

It should be noted that alongside disinformation, overinformation, understood as the provision of an excessive volume of information, also poses a risk, as recipients are unable to evaluate and process it effectively

[288] According to Recital 134 and Article 3(60) of the AI Act, "deepfake content" is defined as *"image, sound or video content produced or manipulated by AI which bears a resemblance to real persons, objects, places, entities or events and which may give the deceptive impression of being genuine or real."*

[289] Evripidis Stylianidis, "Article 5A," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 145 ff. (153).

[290] Lina Papadopoulou, "Fake News and Hate Speech," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 117.

[291] Ibid.

[292] Ibid.

[293] Ibid.

2. Exploitation of data

Data are of great value. They are rightly described as the "new gold"[294] and have acquired exchange value.[295] Those who process them can better understand their constituents, optimise their actions, and make data-driven decisions.[296] As Harari aptly notes, whoever controls the data controls the future.[297] Governance has always required reliance on data. Big data contributes to the effectiveness of public services and strategic planning and shape the interactions between citizens, public institutions, policies and administrative systems.[298] AI can collect and analyse these data in real time, training[299] algorithms and enabling campaign strategists to adjust their approaches in line with public opinion. Data collection can be used either to identify the electorate's fundamental needs or simply to influence and manipulate voters. By analysing the distinctive psychographic and behavioural profiles of voters on social media, AI can be deployed to sway individuals towards a particular candidate or to spread hostility against opponents in order to influence voting decisions.[300] The creation of psychographic profiles and targeted messages, enabled by Big Data, in online campaigns based on deception and intimidation can shape a wide range of activities, from propaganda to policy-making.[301] This is because election campaigns are moving increas-

[294] Tom Dausy, "Data, the New Gold: How AI Is Unlocking Insights and Driving Business Growth," *Medium*, May 19, 2024, https://medium.com/@tomdausy/data-the-new-gold-how-ai-is-unlocking-insights-and-driving-business-growth-c458b5676f08

[295] Takis Vidalis, "The Impact of Technology on Democracy," in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 21 ff. (27).

[296] Tom Dausy, "Data, the New Gold: How AI Is Unlocking Insights and Driving Business Growth," *Medium*, May 19, 2024, https://medium.com/@tomdausy/data-the-new-gold-how-ai-is-unlocking-insights-and-driving-business-growth-c458b5676f08

[297] Yuval Noah Harari, *21 Lessons for the 21st Century* (Athens: Alexandria, 2018), 87.

[298] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 13, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[299] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 46, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[300] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 12, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[301] Ibid.

ingly online and advertising on digital platforms is influencing election outcomes.[302]

Governance based on available data is neither neutral nor uncontested because the data themselves are neither universally available nor beyond dispute.[303] Algorithms frequently embed biases.[304] The social roots of prejudice run deep, and the education required to identify and eliminate them is lacking.[305] Algorithms trained on recent recruitment data develop biases against specific groups.[306] The vast quantities of data available exceed human capacity to analyse, comprehend, and ultimately make use of them. This has led to increased reliance on automated algorithms to detect patterns and support decision-making, deepening our dependence on such technologies and aggravating power imbalances.[307] Biases arise not only from data but also from algorithm design and AI training practices,[308] which can either reinforce or mitigate them.[309] In short, it is not the algorithm itself that is racist, but its design and training based on existing statistical data. Data inequality stems primarily

[302] Cornelius Erfort, "Targeting Voters Online: How Parties' Campaigns Differ," *Electoral Studies* 92 (December 2024), https://www.sciencedirect.com/science/article/pii/S0261379424001306

[303] Iliana Kosti, "Can the Algorithm Be Fair?," in *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, ed. Lilian Mitrou (Heraklion: University of Crete University Press, 2023), 97 ff. (103).

[304] A classic case of bias is the systematic discrimination against women who applied for technical jobs at Amazon, such as software engineering positions. The algorithm developed this bias because Amazon's existing pool of software engineers was overwhelmingly male and white, and the new software was trained on data from their résumés. See Rachel Goodman, "Why Amazon's Automated Hiring Tool Discriminated Against Women," *ACLU*, October 12, 2018, https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against

[305] Iliana Kosti, "Can the Algorithm Be Fair?," in *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, ed. Lilian Mitrou (Heraklion: University of Crete University Press, 2023), 97 ff. (103).

[306] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 146.

[307] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 14, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[308] COMPAS, *Correctional Offender Management Profiling for Alternative Sanctions* (Northpointe Inc., 2012).

[309] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 14, https://unesdoc.unesco.org/ark:/48223/pf0000389736

from unequal access to it.[310] Even where databases are publicly available, only a limited number of people have the skills or resources to analyse, understand, manage, or exploit them.[311] Today's Big Data ecosystem produces significant inequalities, reflecting a different kind of poverty and wealth,[312] not based on material goods.[313] There are essentially three categories of people when it comes to databases: those who produce them, those who have the capabilities and resources to store them, and those who know how to exploit their value. The last group is the smallest and most privileged one, dictating the rules that govern the use of and participation in Big Data.[314]

---

[310] The European Data Act (the Regulation on harmonised rules for fair access to and use of data – also known as the Data Act – entered into force on 11 January 2024) constitutes a key pillar of the European data strategy and will significantly contribute to achieving the Digital Decade goal of promoting digital transformation. It provides that connected products must be designed and manufactured, and related services must be supplied, in such a way that the data generated by these products and services are directly accessible to users (Article 3). If the data cannot be made directly accessible, they must be made available upon request without undue delay (Article 4).

There is an exception to the obligation of direct access or availability upon request where such access would undermine the security of the connected product, leading to serious adverse effects on the health, safety, or protection of natural persons.

According to Articles 3 and 4 of the Regulation, the data that must be directly accessible or made available upon request include: (a) product data, i.e. data generated by the use of the connected product, designed to be retrievable via an electronic communications service, physical connection, or access to the device; (b) related service data, i.e. data representing the digitalisation of user actions (including in-app actions) and events related to the connected product, whether deliberately recorded by the user or produced as a by-product of user actions; and (c) metadata necessary for the interpretation of the aforementioned categories of data.

[311] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 14, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[312] Uneecops. "How Data Analytics Drive Growth for Wealth Management Firms." August 2, 2024. https://www.uneecops.com/blog/data-analytics-for-wealth-management-firm

[313] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 14, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[314] Ibid.

3. Manipulation

The Cambridge Analytica scandal revealed the extent to which the misuse of AI can influence electoral behaviour. This is because the data of internet users can be exploited to build a political, ideological or psychological profile of individual voters, enabling the delivery of personalised advertisements or automated messages to promote or discredit particular candidates.

First, the autonomy of the citizen is undermined: through the creation of a detailed psychological profile and the exploitation of weaknesses, fears, or fixations by means of personalised messages designed to trigger emotions, the citizen is subjected to a form of automated "brainwashing" intended to influence behaviour.[315] Second, internet users are rarely informed of, or give their consent to, the use of their data for such purposes.[316] Third, there arises the issue of violating the right to stand for election and the principle of equal opportunities among candidates.[317] Fourth, algorithms are employed to generate and disseminate false or distorted news, as part of propaganda strategies designed to manipulate the information and steer the emotions of internet users in a given direction.[318] For instance, false or distorted reports – such as fabricated statements by political figures about alleged violent crimes committed during the electoral period by migrants or asylum seekers – can be deployed in campaigns spreading fear, intolerance, and xenophobia, thereby promoting extreme ideologies. Fifth, the use of algorithms to create deepfakes (videos in which faces are changed or replaced) with the aim of misleading the public and discrediting political opponents is equally dangerous for democratic processes.

Furthermore, attention must be drawn to the risk that the provision of predetermined and curated knowledge may undermine the liberal

[315] Fereniki Panagopoulou-Koutnatzi, *Artificial Intelligence: The Path to a Digital Constitutionalism – An Ethical-Constitutional Approach* (Athens: Papazisis, 2023), 286.

[316] Ibid., 288.

[317] Latanya McSweeney, "Psychographics, Predictive Analytics, Artificial Intelligence & Bots: Is the FTC Keeping Pace?," *Data Privacy Lab* (2013): 514 ff., http://dataprivacylab.org/projects/onlineads/1071-1.pdf

[318] Fereniki Panagopoulou-Koutnatzi, *Artificial Intelligence: The Path to a Digital Constitutionalism – An Ethical-Constitutional Approach* (Athens: Papazisis, 2023), 286.

character of our polity, by imposing the "average" of existing knowledge on science and thought more generally, and entrenching a single, uniform perception of reality.[319] The use of AI systems to influence voters politically and shape the outcome of elections has raised serious concerns at both European and international levels. It is therefore reasonable to ask whether legislative intervention is required in order to safeguard the core of liberal democracy. The question is a complex one, since the consolidation of a particular perception may in turn foster the consolidation of a particular electoral preference and, in this way, the indirect manipulation of the electorate.

The risks arising from the use of AI in electoral contests may be numerous, difficult to address, and in many cases intolerable (within the meaning of Article 5 of the Regulation), where they result in the manipulation of citizens. It is proposed that legislators accord this issue particular priority, requiring digital platforms, algorithm developers, and distributors to ensure algorithmic transparency and to criminalise the creation and dissemination of harmful deepfake products that enable political manipulation.[320] At the same time, software developers and distributors must block audio and video products that generate harmful deepfakes and will be held responsible if their preventive safeguards can be easily circumvented.

To this end, mechanisms for verifying the reliability of news must be strengthened (fact-checking, including the labelling of content as true, false, or disputed).[321] At the same time, specialised skills must be cultivated to counter the falsification of news, media literacy and education must be enhanced, and stakeholders (citizens, journalists, private and public bodies) must be empowered through the adoption of clear, responsible, fair, and widely accepted rules of conduct and operation in the

[319] Fereniki Panagopoulou-Koutnatzi, "Legal and Ethical Concerns Regarding the Use of ChatGPT in Education," *Journal of Law and Technology* (2023): 6 ff. (11).

[320] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 94, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[321] Lilian Mitrou, "Digital Democracy, Participation and Threats," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 83. The note also raises the question of who determines whether news is true, false, or disputed.

new, advanced technological environment.[322] The debate is not without difficulties. A reasonable question arises as to who exercises control and on the basis of which principles.[323] In this context, the Digital Services Act imposes obligations of transparency and accountability with regard to content moderation.[324]

4. Towards privatisation of elections?

The role played by large private internet companies is of great importance. Their architecture and algorithms shape the way people communicate and determine what information is presented, and in what sequence, to participants.[325] In short, private actors often play a decisive role in regulating social behaviour and information.[326] Some describe this regime as "techno-feudalism".[327]

Almost every stage of AI model development, from computing infrastructure to training data, is controlled by an oligopoly of technology companies. There is very little public oversight of how these systems are developed and governed. The risks associated with the concentration of AI development in monopolistic entities are a cause for serious concern.[328] There is a need to find alternative structures for the exploitation and governance of AI that would better serve the public interest with regard to AI development. One of these structures could be shareholding

[322] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight, 2024), 94, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[323] Lilian Mitrou, "Digital Democracy, Participation and Threats," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 87.

[324] In this sense, this Act constitutes the most significant reform regarding digital platforms. See Ioannis Iglezakis, *The Law of the Digital Economy*, 2nd ed. (Athens–Thessaloniki: Sakkoulas, 2024), 71.

[325] Nicolas P. Suzor, "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms," *Social Media + Society* 4, no. 3 (2018): 1–11, https://doi.org/10.1177/2056305118787812

[326] Ibid., 2.

[327] Manolis Andriotakis, *Artificial Intelligence for All* (Athens: Psychogios, 2022), 69.

[328] Anton Korinek and Jai Vipra, "AI Monopolies," *Economic Policy* (panel brief), March 27, 2024, https://www.economic-policy.org/79th-economic-policy-panel/ai-monopolies/

schemes.[329] These are employee-owned and managed enterprises with a long global history of community-oriented business practices that distribute both control and capital. Today, it is estimated that participatory schemes employ nearly 10% of the world's population.[330] Participatory models are designed to ensure fairer ownership and governance than investor-owned companies.[331] Such structures are expected to alleviate growing concerns among various stakeholders: consumers gain greater influence and an economic stake in the technological systems that shape their lives; businesses build trust with consumers and regulators while remaining connected to public needs; and regulators facilitate a competitive marketplace with the potential to enhance the social impact of AI.[332]

5. Algorithmic governance?

Decision-making largely tends to be algorithmic,[333] as automated systems account for a significant share of government decisions.[334] Managing complex issues requires algorithmic decision-making. It is difficult to conceive of managing the complexity of modern societies without such processes of this kind, as they process vast amounts of information and

[329] Sarah Hubbard, *Cooperative Paradigms for Artificial Intelligence* (Cambridge, MA: Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, November 20, 2024), https://ash.harvard.edu/resources/cooperative-paradigms-for-artificial-intelligence/

[330] International Cooperative Alliance, "Co-ops Employ 10% of the Global Employed Population," September 25, 2017, https://ica.coop/en/media/news/co-ops-employ-10-global-employed-population

[331] Connor Spelliscy, Sarah Hubbard, Nathan Schneider, and Samuel Vance-Law, "Toward Equitable Ownership and Governance in the Digital Public Sphere," *Stanford Journal of Blockchain Law & Policy* (2024), https://stanford-jblp.pubpub.org/pub/equitable-ownership-and-governance/release/1

[332] Sarah Hubbard, *Cooperative Paradigms for Artificial Intelligence* (Cambridge, MA: Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, November 20, 2024), https://ash.harvard.edu/resources/cooperative-paradigms-for-artificial-intelligence/

[333] Fereniki Panagopoulou, "Algorithmic Decision-Making in Public Administration," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 141 ff.

[334] John Danaher, "The Threat of Algocracy: Reality, Resistance and Accommodation," *Philosophy & Technology* 29 (2016): 245–268. https://doi.org/10.1007/s13347-015-02111-1

automate tasks that would otherwise be impossible or less efficient.[335] The problem, however, is the extent to which and the manner in which the use of automated decision-making systems is compatible with political decision-making.[336] AI systems can improve our understanding of social preferences and facilitate more objective evaluations of public policies. They are also useful in situations where there is a large volume of data and choices are sorted into binary-digit categories.[337] Even so, they prove limited in cases of data scarcity or ambiguous situations, where policy decisions are imperative and carry greater certainty than any calculation. In any case, in a democracy, the final decision rests with the people who hold sovereignty, regardless of the extent of data processing.[338] Therefore, the algorithm should not replace but assist those who make political decisions.[339]

6. Have the risks been confirmed?

In 2024, numerous countries[340] held national elections, making that year one of the largest election years in history. It was the largest election year in human history, with 3.7 billion voters in 72 countries going to the polls.[341] Despite early public concerns about dramatic AI disruption in the 2024 election, experts agreed that most of those fears did not materialise, while a more nuanced reality is emerging: AI permeates all as-

[335] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 16, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[336] Ibid.

[337] Ibid.

[338] Ibid.

[339] Fereniki Panagopoulou, "Algorithmic Decision-Making in Public Administration," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 137 ff. (180).

[340] "It's the Biggest Election Year in Modern History. Will Democracy Prevail?," *NPR*, 3 July 2024, https://www.npr.org/2024/07/03/1198912778/its-the-biggest-election-year-in-modern-history-will-democracy-prevail

[341] Bruce Schneier and Nathan Sanders, "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 4 December 2024, https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/

pects of elections, from campaign operations to the information ecosystem.[342] It was argued that many platforms took proactive measures to address election-related concerns, redirected political queries to authoritative sources, and developed their own AI-based countermeasures to identify and address coordinated inauthentic behaviour.[343]

Nevertheless, ominous practices involving bots were also noted. "Bots" are social media accounts not belonging to a real person but controlled by an operator for a specific purpose.[344] Myriad bots disseminate false information and centrally directed disorienting messages originating from domestic oligarchs or from foreign dictators and authoritarian leaders.[345] In Romania, the European Commission opened a formal investigation into TikTok due to "serious indications" of foreign interference in Romania's recent presidential election. The second-round vote was cancelled after intelligence documents revealed that 25,000 TikTok bot accounts had been suddenly activated weeks before the first-round polls opened. The accounts supported independent candidate Calin Georgescu, who described Russia's Vladimir Putin as a 'patriot and leader', although he denied being a follower.[346] EU regulators will assess whether TikTok's advertising policies and the systems it uses to

[342] Sarah Hubbard, *The Role of AI in the 2024 Elections* (Cambridge, MA: Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 5 December 2024), https://ash.harvard.edu/resources/the-role-of-ai-in-the-2024-elections/

[343] Ibid.

[344] Michalis Bletsas, "The big problem is not bots but the toxic impact of social media," quoted (in Greek) at Hellenic Cybersecurity Authority, https://cyber.gov.gr/athens-voice-michalis-mpletsas-to-megalo-provlima-den-einai-ta-bots-alla-i-toxiki-epidrasi-ton-social-media/. As he states in said article, "Bots are robotic accounts that are created automatically on online platforms and allow the person behind them—the one paying—to control very many accounts at the same time, increasing a troll's impact. You sit at your console and say: 'take this article and promote it,' and instead of it coming from your own account, it comes from hundreds or thousands." How can we recognise them? "They usually have odd usernames, no photos, they follow influential accounts, very few people follow them, they post an awful lot in a very short period of time and then remain inactive."

[345] Lina Papadopoulou, "Robots and Sheriffs," *To Vima*, March 19, 2025, https://www.tovima.gr/print/opinions/rompot-kai-serifides

[346]. Alex Loftus, "EU Investigates TikTok over Alleged Russian Meddling in Romanian Vote," *BBC News*, December 17, 2024, https://www.bbc.com/news/articles/cm2v13nz2020

recommend content to users violate the Digital Services Act, which seeks to prevent the spread of disinformation and curb illegal activities online.[347]

Recent research has shown, however, that before the final (and bot-contaminated) consensus is reached, the network goes through an almost static phase that offers the possibility of mitigating the harmful impact of the bots.[348]

C. Upgrading democratic institutions

1. Facilitating participation in consultation processes

The question arises whether facilitating access to AI-assisted digital governance applications has a positive impact on democracy.[349] This has been described as the "platformisation of democracy", since a significant share of debates takes place on platforms that, while facilitating them, also end up shaping them in different ways.[350] AI tools can strengthen democracy by facilitating citizen participation in consultation processes. Innovative uses of AI can support deliberative democracy at different levels of decision-making, from the adoption of national legislation to local government and corporate governance. This is because they facilitate the consultation process by summarising consultations and aggregating vast volumes of incoming online information.

AI can support the expansion of consultation and democratic participation. Among the many tasks that AI tools can perform are selecting and allocating participants in citizens' assemblies (the LEXIMIN algorithm[351]

---

[347] Ibid.

[348] Ines Lindner, Bernd Heidergott, Saeed Badri, and Merle Praum, *The Impact of Bots on Social Learning and Consensus Formation: Why Even an 'Infinitesimal' Number of Bots Matters* (December 2024), https://ssrn.com/abstract=5249942

[349] Lilian Mitrou, "Digital Democracy, Participation and Threats," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 53 ff. (55).

[350] Tarleton Gillespie, "The Politics of Platforms," *New Media & Society* 12, no. 3 (2010): 347–364.

[351] Sylvain Bouveret and Michel Lemaître, "Computing Leximin-Optimal Solutions in Constraint Networks," *Artificial Intelligence* 173 (2009): 343–364, https://doi.org/10.1016/j.artint.2008.10.010

is already available and in use); facilitating consultation (Meta's community forums pioneered this function); summarising deliberations; and aggregating vast amounts of online input (the pol.is system[352] is being used by the Taiwanese government).[353]

In this way, AI can also serve as an important tool for promoting the democratic governance of AI technology itself. Indeed, the development of AI for the benefit of society, with transparency and accountability, cannot take place without the participation of society itself – and this is something that can be facilitated by deliberative democracy.[354]

The above is also linked to building 'digital trust' in platforms, which can be achieved through continuous public evaluation and democratic representation and participation where critical decisions are taken.[355]

A possible experiment in democratic representation could involve the creation of citizens' assemblies. Citizens' assemblies are now an established process through which local and national governments, in-

[352] Polis Blog, "Pol.is in Taiwan," *Medium*, https://blog.pol.is/pol-is-in-taiwan-da7570d372b5

[353] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Office, 2024), 94, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[354] Ibid.

[355] Ibid.

cluding Ireland,[356] France,[357] Belgium,[358] and Canada,[359] seek to remedy legitimacy deficits and governance problems. These are large bodies of citizens, convened (sometimes in person and sometimes virtually) to discuss complex policy issues, with the aim of producing policy recommendations and, in some cases, even legislative proposals. A recent OECD report documented hundreds of such assemblies (or similar bodies) around the world.[360] In essence, these are assemblies of representatives, composed of adult citizens, residents of a region, or even residents abroad.[361] These representatives are selected on an almost random basis but are deliberately "stratified" by characteristics such as race, gender, and social class, and then consider an issue.[362] The assembly follows three structural stages of deliberation: it begins with an educational process introducing its members to the issue; this is followed by hearing different

[356] Citizens' assemblies were convened in Ireland to evaluate possible constitutional amendments, for example on same-sex marriage and reproductive rights.

[357] This was the French Citizens' Convention on Climate, convened in 2019/2020. It emerged out of the "Gilets Jaunes" protests that began in late 2018 in response to a new fuel tax. As the government struggled to respond, it channelled popular energy—perhaps also to contain it—by launching a "Great National Debate," which took the form of a series of local citizens' assemblies. From this process arose the idea of a national climate policy convention. In July 2019, the government tasked the Convention with recommending how France could reduce CO_2 emissions by 40% compared to 1990 levels by 2030 in a socially just way.

[358] In Belgium, a proposal was made for a permanent body resembling a citizens' assembly with the power to decide whether a proposal should proceed to referendum. Organisation for Economic Co-operation and Development (OECD). *Eight Ways to Institutionalise Deliberative Democracy*. Paris: OECD, 2021. https://www.oecd.org/gov/open-government/eight-ways-to-institutionalise-deliberative-democracy.htm

[359] In Canada, a Citizens' Assembly was created to examine electoral reform. See National Citizens' Assembly. "Electoral Reform in Canada." Canada, 2021. https://nationalcitizensassembly.ca

[360] Organisation for Economic Co-operation and Development (OECD). *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave*. Paris: OECD, 2020. https://www.oecd-ilibrary.org/governance/innovative-citizen-participation-and-new-democratic-institutions_339306da-en

[361] ENA Institute for Alternative Policies, *Citizen Assemblies and Democratic Renewal* (Athens: ENA, May 2022), 3.

[362] Ibid.

views from stakeholders, individuals, or groups; and it concludes with deliberations, during which the assembly votes on a proposal.[363]

To achieve the greatest possible legitimacy, these citizens' assemblies must connect with the wider public through various online and offline consultation mechanisms, some of which could be uniquely enabled by open AI tools. It should be noted that openness is necessary for the sustainable and ethical development of AI technologies and for safeguarding conditions of digital sovereignty.

Selecting citizens from all social groups through AI tools appears to have three main advantages. First, assemblies achieve broader demographic representation than elected bodies. This is because elected representatives tend disproportionately to come from the most privileged groups in society – overwhelmingly male, white, and middle class, for example. This results in political inequality and a lack of insight that arises from bringing together people from a broader social spectrum.[364] Second, assemblies are put forward as a way to bridge the trust gap between politicians and citizens. This, however, presupposes that the public trusts its representatives in the assembly and that politicians heed the assembly's proposals.[365] Third, citizens' assemblies can contribute to improving the quality of direct democracy.[366] It should not be overlooked, however, that assemblies are also associated with the risk of "majoritarian tyranny", in the sense that they may be subject to the excessive influence of wealthy citizens who can more easily finance petition and referendum campaigns.[367]

At this point, it is crucial to emphasise that citizen participation in the decision-making process does not only take place in an organised form, such as through citizens' assemblies. It can also occur in a dispersed manner where anyone who wishes may participate unconditionally. This form of unconditional participation facilitates access to the participatory process but may also lead to mass involvement of individuals who are not entitled to take part in decision-making.

[363] Ibid.
[364] Ibid., 4.
[365] Ibid., 5.
[366] Ibid., 6.
[367] Ibid.

2. Facilitating political campaigning

a. Translation tools

One of the beneficial uses of AI is the translation of election campaigns.[368] Local governments in Japan[369] and California,[370] as well as prominent politicians such as Prime Minister Narendra Modi of India[371] and New York City Mayor Eric Adams,[372] have used AI to translate meetings and speeches to their diverse constituents.[373]

Even when politicians are not themselves speaking through AI, their constituents may use it to listen to them. Google launched free translation services for an additional 110 languages this summer, available to billions of people in real time via their smartphones.[374]

---

[368] Ananya Bhattacharya, "Political Campaigns Embrace AI to Reach Voters across Language Barriers," *Rest of World*, September 19, 2024, https://restofworld.org/2024/aapi-victory-alliance-ai-voter-outreach

[369] "Japanese Mayor Suddenly Speaks Fluent English with AI Video That Surprises Even Him," *Japan Today*, June 7, 2024, https://japantoday.com/category/politics/japanese-mayor-suddenly-speaks-fluent-english-with-ai-video-that-surprises-even-him

[370] Zhe Wu, "As Bay Area Cities Adopt Real-Time AI Translation for Public Meetings, SF Abstains," *San Francisco Public Press*, December 6, 2024, https://www.sfpublicpress.org/as-bay-area-cities-adopt-real-time-ai-translation-for-public-meetings-sf-abstains

[371] "BJP to Use AI to Translate PM's Speeches," *Times of India*, March 8, 2024, https://timesofindia.indiatimes.com/city/bengaluru/bjp-to-use-ai-to-translate-pms-speeches/articleshow/108318912.cms

[372] Anthony Izaguirre, "Adams' Revelation That He Uses AI to Speak in Mandarin Stirs Outcry: 'The Mayor Is Making Deepfakes of Himself'," *Associated Press*, October 17, 2023, https://fortune.com/2023/10/17/new-york-city-mnayor-eric-adams-uses-ai-to-speak-mandarin

[373] Bruce Schneier and Nathan Sanders, "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 4 December 2024, https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/

[374] Google, "Google Translate Adds New Languages," Google Blog, 2024, https://blog.google/products/translate/google-translate-new-languages-2024

b. Virtual chats

Other candidates used AI chat features to connect with voters. American politicians used chatbots of themselves in their presidential primary campaigns.[375] Fringe candidate Jason Palmer defeated Joe Biden in the American Samoa primary, at least in part thanks to the use of AI-generated emails, texts, audio and video. Pakistan's former Prime Minister Imran Khan used an AI-generated clone of his voice to deliver speeches from prison.[376]

Perhaps the most effective use of this technology was in Japan, where an independent Tokyo gubernatorial, Takahiro Anno, used an AI avatar to answer 8,600 questions from voters and secured fifth place in a highly competitive field of 56 candidates.[377]

Chatbots also encourage users to leave comments and provide valuable insights into public opinion.[378]

c. Political organisation

On the political organisation side, AI assistants are used for a variety of purposes, such as supporting the drafting of political messages and strategy, creating adverts, preparing speeches, and coordinating efforts to mobilise and elect voters.[379] In Argentina in 2023, both main presidential

[375] Bruce Schneier and Nathan Sanders, "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 4 December 2024, https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/

[376] "Imran Khan's 'Victory Speech' from Jail Shows A.I.'s Peril and Promise," *New York Times*, February 11, 2024, https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html

[377] Gideon Lichfield, "Meet Your AI Politician of the Future," *Futurepolis Substack*, October 4, 2024, https://futurepolis.substack.com/p/meet-your-ai-politician-of-the-future

[378] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 12, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[379] Bruce Schneier and Nathan Sanders, "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 4

candidates used AI to develop posters, videos and other campaign materials.[380]

In 2024, similar capabilities were used in several elections around the world. In the US, for example, a Georgia politician[381] used AI to produce blog posts, campaign images, and podcasts. Other AI systems assist candidates seeking higher office.[382]

Furthermore, AI can collect and analyse this data in real time, enabling campaign strategists to adjust their approaches based on public opinion.[383]

D. Changing representative democracy

1. Issues and considerations

Citizen participation in consultation processes, whether organised in assemblies or scattered, raises the issue of the changing or evolving nature of representative democracy. New internet technologies that expand the possibility of participation magnify the challenge. It is therefore necessary to consider whether the new opportunities offered by the internet alter the qualitative characteristics of democratic participation in a way that affects the functioning of the constitution.[384] Some speak of a transi-

December 2024, https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/

[380] "Is Argentina the First A.I. Election?," *New York Times*, November 15, 2023, https://www.nytimes.com/2023/11/15/world/americas/argentina-election-ai-milei-massa.html

[381] Ross Williams, "Georgia Political Campaigns Start to Deploy AI but Humans Still Needed to Press the Flesh," *GPB News*, April 25, 2024, https://www.gpb.org/news/2024/04/25/georgia-political-campaigns-start-deploy-ai-humans-still-needed-press-the-flesh

[382] Sean J. Miller, "AI Is Helping Candidates Decide on Runs for Higher Office," *Campaigns & Elections*, October 22, 2024, https://campaignsandelections.com/campaigntech/ai-is-helping-candidates-decide-on-runs-for-higher-office

[383] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 12, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[384] Vasiliki Christou, "Towards a Digital Municipality?," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 19 ff. (24).

tion to a "Digital Pnyx", where each citizen will only need a few seconds, from wherever they are, to take part in decision-making.[385]

It is a fact that AI tools enable politicians to consult the people in an easy, quick, and effective way on a variety of matters for which they hold a popular mandate. The logical question then arises: when should a politician return to the people, on what kinds of questions, and in what way?[386] Modern online media have created some prospects and hopes for enhancing citizen participation in the decision-making process.[387] This raises the question of how representative democracy is being transformed by new internet technologies. This is because the audience participating in consultation processes is, on the one hand, enlarged and, on the other, limited.[388]

2. The possibility of broadening participation

The broadening lies in the fact that participation in decision-making usually takes place without any form of participant identification. In theory, anyone can participate in any vote, whether it concerns them or not. This enlarges the circle of people deciding on an issue.

This concern is addressed in many modern electronic voting media, where a strict voter identification system is applied. Such identification raises issues of ballot secrecy and the protection of the voter's personal data, while free access to the ballot entails the risk of involving groups not legitimately entitled to take part in decision-making. The logical question arises: on which procedures are citizens legitimately entitled to decide? Are all Greeks abroad, for example, entitled to take part in decision-making on Greece's internal affairs? Might this open the way for the alteration of the electorate and ultimately the election result? This position could be justified by the fact that it allows the formation of a potentially vast and immeasurable electoral body including voters with no economic

[385] Anastasios Avrantinis, "Artificial Intelligence: Towards a 'Digital Pnyx'," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 607 ff. (610).
[386] Ibid., 19 ff.
[387] Ibid., 23.
[388] Ibid., 29.

or social ties to Greece, who may only visit the country for holidays, who will vote on the basis of the social and political conditions of the countries in which they reside, and, most importantly, who will not bear any consequences from their political choices. At this point, it is stressed that facilitating the right of expatriates to vote is considered a step in the right direction towards upholding the principle of universal suffrage.[389] In this case, it is a matter of facilitating the exercise of a right – not of granting the right to vote. Some concerns are expressed as to whether citizens unfamiliar with Greek reality will be able to decide on Greek affairs.[390] Set

[389] Fereniki Panagopoulou, *Electronic Voting: A Constitutional-Ethical Approach* (Athens–Thessaloniki: Sakkoulas, 2023), 160. With the recent Law No. 5044/2023, adopted by five out of the eight parliamentary parties (in addition to the governing majority, PASOK, Spartans, NIKI, and Course of Freedom voted in favour, while SYRIZA and the Communist Party of Greece raised objections, and Greek Solution expressed reservations and requested time for the current framework to be tested), that is, by 220 MPs, the electoral rights of expatriates were expanded, recognising the right to vote for all expatriates residing abroad who are registered in the electoral rolls. Under this law, not all expatriates worldwide vote, but only those registered in the electoral rolls. The purpose of the law is to safeguard the universality of the electoral right of all citizens. It does not grant the right to vote to anyone who does not already have it, but rather provides a facility enabling them to participate without travelling to Greece in order to vote. Furthermore, it strengthens the bonds of Greeks abroad with the homeland, multiplying their active interest in developments in Greece. The law seeks to rationalise the existing framework, which today creates a "two-tier diaspora": those affluent enough to afford the cost of travelling to Greece to vote and those living in nearby countries, and those who cannot afford to travel or who live in very distant countries.

Objections were voiced by SYRIZA, which warned of a "danger for democracy" and argued that since citizenship is granted on the basis of descent, there is a risk of excessive use of the new regulation. The Communist Party of Greece further argued that the law opens highly dangerous paths for altering the electoral body, and ultimately the electoral outcome, since by abolishing every criterion that applied under the 2019 law, it creates the possibility of forming a potentially vast and incalculable electorate that may include voters with no economic or social ties to Greece, who may only come to the country for holidays, and who will participate in elections based on the social and political conditions of the countries where they live, while bearing no consequences from their political choices in Greece. SYRIZA tabled an amendment providing for the creation of four electoral districts for expatriates, so that Greeks abroad could elect their own representatives. It was further proposed that voting be conducted separately with a single ballot in each of the four districts, with all Greek citizens entitled to participate, provided they have the legal capacity to vote and stand for election without other restrictions or conditions.

[390] Ibid.

against this is the need to support the Greek diaspora and, more broadly, to integrate it into Greek public life. It is necessary to provide an incentive for second and third generation expatriates to take an interest in the common affairs of Greece and to become active from abroad, following the example of earlier expatriates who awakened the Greek nation with their ideas and prepared the Greek revolution.[391]

Could we go a step further by allowing Greeks to co-decide on German or even American affairs? Any enlargement of the electorate could be justified on the grounds that important decisions in one third country have repercussions elsewhere. For example, restrictions on immigration in Germany affect Greece, which will be forced to absorb more immigrants. The US withdrawal from the Paris Agreement and US climate and environmental policy, more generally, also affect other countries. The abolition of English-language university studies in the Netherlands will lead to students moving to other countries. It is no coincidence that Jürgen Habermas argues that all those affected by the decisions to be taken have a right to participate in consultations.[392] Enlargement of the electorate, however, could also signal an attempt to determine or influence the electoral outcome. This could occur through the deliberate guidance of a large group of citizens to vote for a particular policy option.

In any case, it may be concluded that electronic media offer possibilities for enlarging the electorate, whether they operate in a strict form (with identification systems) or in a loose form (without identification systems). Even when citizens are grouped in citizens' assemblies, the number of decision-makers is still enlarged, as the members of assemblies outnumber representatives.

3. Risk of limiting or excluding participants

Participation in decision-making through AI tools may restrict the electorate, depriving the digitally illiterate of the possibility to participate in processes they cannot understand. Some speak of a kind of digital authoritarianism, in the sense that the internet compels us to participate

[391] Ibid., 361.

[392] Jürgen Habermas, *Faktizität und Geltung: Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats* (Frankfurt: Suhrkamp, 1992), 138.

in online processes, and dictates what we should follow.[393] Certain segments of the population remain unrepresented on these platforms due to various systemic inequalities, such as gender, age, socio-economic status, or the lack of connectivity itself, leading to disconnection and complete digital exclusion.[394] In this way, inequality arises between the digitally underprivileged and the digitally proficient – a form of discrimination or digital divide that can be reduced to a distinction between the haves and the have-nots.[395] Indeed, since secure elections require strong identification, digital skills required go well beyond beginner level. Nevertheless, this gap is expected to narrow over time.

4. Is representative democracy ultimately changing?

The above issue leads us to ask whether enlarging the electorate remedies the disadvantages of representative democracy, which lie mainly in its alienation from the electorate and the danger of technocracy.[396] Does it not, however, create for the citizen the illusion of participation in public affairs, when in fact that participation has no effect?[397] Is there not a diffusion of political responsibility to the people, who cannot in fact bear such responsibility? Who will bear responsibility if a wrong choice leads the country to economic disaster? Will the people themselves be politically persecuted? At this point, it is crucial to stress that AI should be used as a tool for consultation, not for diffusing political responsibility. In this way, the structural features of representative democracy can be

[393] Raluca Csernatoni, "Can Democracy Survive the Disruptive Power of AI?," Carnegie Endowment for International Peace, December 18, 2024, https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en

[394] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 13, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[395] Fereniki Panagopoulou, *Electronic Voting: A Constitutional-Ethical Approach* (Athens–Thessaloniki: Sakkoulas, 2023), 160.

[396] Vasiliki Christou, "Towards a Digital Municipality?," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 19 ff. (37).

[397] Vasiliki Christou, "Towards a Digital Municipality?," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 19 ff. (41).

preserved. Representatives will listen to the people but will decide themselves.

E. Abstention or conditional acceptance?

There are two solutions: abstention or conditional acceptance. The first is technophobic and utopian: the genie is already out.[398] The second requires careful policy-making. In this direction, policymakers should consider the trade-offs involved in watermarking AI content, which is a technique that embeds a unique, traceable signature in AI-generated material, identifying it as an AI product. Visible watermarks promote transparency but can disrupt artistic intent, while digital watermarks, hidden in metadata, are more subtle but easier to manipulate.[399] The global, interconnected nature of online content suggests that broader, harmonised standards across jurisdictions may be necessary for effective multilateral governance. The G7 has called on companies to develop credible mechanisms such as watermarking.[400] Towards this end, the AI Act imposes obligations on AI providers and developers to ensure transparency, detection, and tracking of AI-generated material (Recital 115). Addressing the challenges posed by AI-generated content will require coordination across a wide range of stakeholders, including governments, AI companies, social media platforms, and users. Technology companies also have a central role in developing authentication and provenance tools to identify and trace the origin of AI-generated content.[401] The use of AI to com-

[398] Bruce Schneier and Nathan Sanders, "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 4 December 2024, https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/

[399] Raluca Csernatoni, "Can Democracy Survive the Disruptive Power of AI?," Carnegie Endowment for International Peace, 18 December 2024, https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en

[400] European Commission, "Hiroshima Process International Guiding Principles for Advanced AI Systems," 30 October 2023, https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-guiding-principles-advanced-ai-system

[401] Ibid.

bat AI shows some promise, but many detection tools are not publicly accessible.[402]

Reliance on detection technology alone may be insufficient without regulatory oversight and public digital literacy initiatives. Enhancing AI and information literacy is crucial, and broad education in digital skills is urgently needed.[403]

F. Recommendations

The peaceful integration of AI with the upgrading of democracy requires a series of measures.

First, there is an urgent need to educate citizens and raise awareness of the challenges posed by AI. It is important to create mechanisms for dialogue with national and regional parliaments, notably through science and technology committees.

Second, careful regulation is required to ensure that AI is used for the "common good", guided by humanitarian principles such as diversity, equality and inclusion, enshrined in the protection of human rights, democracy and the rule of law.[404] The legal framework must establish independent oversight mechanisms to ensure effective compliance and accountability. At the same time, however, such an oversight mechanism can only be effective if it is proactive and committed in advance, that is, before issues arise.[405] Indeed, while introducing sanctions for non-compliant behaviour is important, relying solely on ex-post sanctions and fines, which large private companies can usually afford to pay, regardless of the amount, may not achieve the desired results. This is because it is often difficult, if not impossible, to revert to the previous situation or "undo the damage" after the introduction and use of a particular AI technology, irrespective of its compliance, or lack thereof, with ethical stan-

[402] Ibid.
[403] Ibid.
[404] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 19, https://unesdoc.unesco.org/ark:/48223/pf0000389736
[405] Ibid.

dards, human rights, democracy, and the rule of law.[406] In addition, efforts should be made to democratise[407] data.[408] Alongside legal measures to prevent or limit the dissemination of harmful rhetoric, fact-checking institutions have proven effective in mitigating its negative effects.[409] To ensure maximum transparency, which is necessary for an informed public opinion, states are encouraged to promote codes of best practice for companies and to require recognition of AI-generated products as measures to combat disinformation.

Third, encouraging transparency and explanatory power in AI systems is crucial for understanding decision-making processes and the criteria that govern their outcomes.[410] Problems of representation, exclusion, or discrimination in politics in general may be exacerbated if decisions are made by AI processes that those affected by them cannot understand. Transparency should also be linked to defining anonymity on social media,[411] in the sense that readers should not be misled about the writer's identity.[412]

Fourth, based on the principle of pluralism[413] throughout the AI process, gender diversity among professionals, inclusive system design, curated datasets, mitigation of biased exclusion policies, facial recog-

[406] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 20, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[407] Hippolyte Lefebvre, Christine Legner, and Elizabeth A. Teracino, "5 Pillars for Democratizing Data at Your Organization," *Harvard Business Review*, 24 November 2024, https://hbr.org/2023/11/5-pillars-for-democratizing-data-at-your-organization

[408] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 19, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[409] Ibid.

[410] Ibid.

[411] "Pedro Sánchez Announces New Initiatives to Prevent 'the Digital Space from Becoming the Wild West'," *La Moncloa* (Spain), 5 February 2025, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2025/20250205-digital-rights-observatory.aspx

[412] Fereniki Panagopoulou-Koutnatzi, *On the Freedom of Blogs: New Technologies as a National, European and International Challenge to the Freedom of Dissemination of Ideas* (Athens–Thessaloniki: Sakkoulas, 2010), 112.

[413] Catharina Rudschies, Ingrid Schneider, and Judith Simon, "Value Pluralism in the AI Ethics Debate: Different Actors, Different Priorities," *International Review of Information Ethics*, no. 32 (2024), https://informationethics.ca/index.php/irie/article/view/419/396

nition processes, and information recommendations must be ensured. Pluralism should guide the democratisation of AI governance, involving new actors such as regions, cities, private actors, and citizens in decision-making processes.[414]

Fifth, AI requires the digitisation of the state in order to function.[415] Digitisation strategies should include objectives related to technological transformation and economic modernisation, as well as others with direct democratic implications. These include the digitisation of public administrations and the promotion of digital literacy[416] among citizens, all grounded in democratic values such as equality, inclusion, and accountability.[417] The democratic principles of equality, accountability, and transparency[418] should be the cornerstone of implementing AI systems, particularly in public services.[419]

Sixth, the adoption of universal standards for digitisation and AI is imperative.[420] These standards should reflect the different perspectives, interests, and objectives of stakeholders worldwide, with particular attention to marginalised regions.[421]

---

[414] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 19, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[415] Fereniki Panagopoulou, "Algorithmic Decision-Making in Public Administration," in *Rule of Law and Democracy in the Digital Age*, ed. Giorgos Karavokyris (Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024), 137 ff. (179).

[416] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 84, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[417] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 21, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[418] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 14, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[419] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 21, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[420] Article 40 of the Regulation.

[421] Ibid.

Seventh, the preservation of the modern democratic rule of law requires human oversight of AI applications:[422] it must not be left unchecked by humans.[423]

G. Concluding remarks

AI tools can enable new forms of participation, but they can also facilitate the spread of disinformation. They have the potential to enhance the accountability of public institutions and their representatives, to promote greater participation and pluralism that enrich citizen participation and make democracy more inclusive and flexible, but they can also reinforce authoritarian tendencies and be used for potentially malicious and manipulative purposes.[424] The complexity of the issue calls for in-depth research to understand these threats and opportunities, in order to develop policies that mitigate threats and maximise opportunities. It is up to the supervisory authorities to monitor for participation in democratic processes in an effective, but not technophobic, way. Moreover, advanced disclosure methods are needed to ensure that we know whether we are interacting with a computer or another person.[425] It is up to us to shape AI as a tool for democratic upgrading, not as a vehicle for digital authoritarianism.

[422] Spyros Vlachopoulos, *The Selfish Gene of Law and the Law of Artificial Intelligence* (Athens: Eurasia, 2023), 98.

[423] Ibid.

[424] UNESCO, *Artificial Intelligence and Democracy* (Paris: UNESCO, 2024), 10, https://unesdoc.unesco.org/ark:/48223/pf0000389736

[425] European Commission, "Hiroshima Process International Guiding Principles for Advanced AI Systems," 30 October 2023, https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-guiding-principles-advanced-ai-system

IV. Artificial intelligence and education: Towards a right to digital literacy?

A. Introduction

AI is already changing the way we learn, work and live, and education is affected by this development.[426] The introduction of AI applications in education sounds like a blessing to some and a curse to others. Concerns are heightened mainly due to the fact that minors are (also) involved, whose personalities are shaped through the educational process. Therefore, any experimentation[427] should be approached with restraint and great caution, as potential harm may prove irreversible. This does not mean that the introduction of AI tools in the field of education should be prohibited, but rather that their application ought to be clearly delineated. This must be pursued with a primary focus on enhancing the educational process, without compromising its fundamental objective: the formation of responsible and conscientious citizens and the cultivation of ethical reasoning. Within this context, the legislative framework governing AI in the field of education is examined, the constitutional basis of the right to digital literacy is explored, and various cases of AI use are analysed, alongside the corresponding critical reflections. The section concludes with a set of recommendations and final remarks.

[426] European Commission, *Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators* (Luxembourg: Publications Office of the European Union, 2022), 12.

[427] Researchers conducting research involving children must apply Articles 3 and 12 of the UN Convention on the Rights of the Child. Article 3 provides that in all actions concerning children, the best interests of the child shall be a primary consideration. Article 12 requires that children with sufficient age and maturity be given the right to express their views freely in all matters affecting them. See UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, *Treaty Series*, vol. 1577, 3.

B. European legal framework

1. Article 2 of the First Additional Protocol to the ECHR

According to this Article the introduction of AI tools in the field of education should be prohibited, but rather that their application ought to be clearly delineated. This must be pursued with a primary focus on enhancing the educational process, without compromising its fundamental objective: the formation of responsible and conscientious citizens and the cultivation of ethical reasoning. Within this context, the legislative framework governing AI in the field of education is examined, the constitutional basis of the right to digital literacy is explored, and various cases of AI use are analysed, alongside the corresponding critical reflections. This section concludes with a set of recommendations and final remarks. The negative formulation (no person shall be denied), as opposed to the initial wording (every person has the right to education) gives rise to a dual interpretation. First and foremost, the emphasis lies in ensuring effective access to the educational system provided by the state.[428] Second, the state is not under a positive obligation to take active measures to guarantee access to education of one's choice, to allow individuals to design their own educational systems, or to subsidise private education.[429] The provision does not impose a duty on the state to provide selective education;[430] such matters fall with the state's discretion.[431] The ECtHR highlights the need for pluralism in education,[432] which implies that AI systems in education must promote pluralism. Pluralism is linked both to the means of teaching (such as AI tools) and to the subject matter (multiculturalism).

[428] *Case "relating to certain aspects of the laws on the use of languages in education in Belgium" (Belgian Linguistic Case)*, nos. 1474/62, 1677/62, 1691/62, 1994/63, and 2126/64, Eur. Ct. H.R. (July 23, 1968).

[429] Anastasios Tamamidis, "Interpretation of Article 2 of Protocol No. 1 ECHR," in ECHR: Article-by-Article Commentary, ed. Ioannis Sarmas, Xenophon Contiades, and Charalambos Anthopoulos (Athens–Thessaloniki: Sakkoulas, 2021), 1094 ff. (1096).

[430] Michail Margaritis, *The European Convention on Human Rights (ECHR) and Protocols Nos. 1, 6, 7 and 13: A Concise Commentary* (Athens: P. N. Sakkoulas, 2018), 534.

[431] David Harris, Michael O'Boyle, Ed Bates, and Carla M. Buckley, *Law of the European Convention on Human Rights*, 4th ed. (Oxford: Oxford University Press, 2018), 898.

[432] *Hasan and Eylem Zengin v. Turkey*, no. 1448/04, Eur. Ct. H.R. (Oct. 9, 2007).

2. Article 14 of the EU Charter of Fundamental Rights

Under Article 14 of the Charter, everyone has the right to education and access to vocational and continuing training. This right includes the opportunity to attend compulsory education free of charge. The wording of Article 14 broadens the scope of the right to education from the corresponding provision of the ECHR, enshrining, among other things, access to vocational and continuing training, as well as the right to attend compulsory education free of charge.[433] Education is defined as "the acts or processes by which, inter alia, information, knowledge, understanding, attitudes, values, skills, competences, and behaviours are transmitted or acquired".[434] In a modern digital state, continuing training necessarily includes digital education, as the very standards of such a state presuppose the digital literacy of its citizens.

3. Regulation 1689/2024 on Artificial Intelligence (AI Act)

The importance of AI in the field of education is already highlighted in the Preamble of the Regulation. According to Recital 4, "AI is a fast-evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial outcomes, for example in [...] education and training".

According to Recital 56, "The deployment of AI systems in education is important to promote high-quality digital education and training and to allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes".

---

[433] Dimitris Sarmas, "Interpretation of Article 14," in *Article-by-Article Commentary on the Charter of Fundamental Rights of the European Union*, ed. Eugenia R. Sahpekidou and Charis N. Tagaras (Athens: Nomiki Vivliothiki, 2020), 164 ff. (165).

[434] *Heiko Jonny Maniero v Studienstiftung des deutschen Volkes eV*, C-457/17, ECLI:EU:C:2018:912 (Nov. 6, 2018).

The Regulation provides that AI systems used in education or vocational training are classified as high-risk. By way of example, it refers to AI systems used to determine access or admission, to assign persons to educational or vocational training institutions or programmes at all levels, to evaluate the learning outcomes of individuals, to assess the appropriate level of education for a person and materially influence the level of education and training that a person will receive or be able to access, or to monitor and detect prohibited behaviour of students during examinations, should be classified as high-risk AI systems, since they may determine the educational and professional course of a person's life and, as a result, affect that person's ability to secure a livelihood. According to the Regulation, when improperly designed and used, such systems may be particularly intrusive and may violate the right to education and training as well as the right not to be discriminated against. They may thus perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities or persons of certain racial or ethnic origins or sexual orientation.

Recital 96 stresses the importance of carrying out an impact assessment study on the introduction of AI in education. The aim of the fundamental rights impact assessment is for the implementing body to identify the specific risks to the rights of the individuals or groups of individuals likely to be affected and to identify the measures to be taken in the event of those risks materialising. The impact assessment should be carried out prior to the development of the high-risk AI system and should be updated when the implementing body considers that any of the relevant factors have changed. A problematic issue arises as to who assesses the risk, namely, who determines what is to be considered risky. The impact assessment should identify the relevant processes of the implementing body in which the high-risk AI system will be used in accordance with its intended purpose and should include a description of the period and frequency with which the system is intended to be used, and specific categories of individuals and groups likely to be affected in the particular context of use. The assessment should also include the identification of specific risks of harm that are likely to impact the fundamental rights of the persons or groups concerned. When carrying out the assessment, the implementing body should take into account information

that is relevant to a proper assessment of the impact, including information provided by the provider of the high-risk AI system in the instructions for use. In the light of the risks identified, implementing bodies should determine the measures to be taken in case such risks materialise, including, for example, governance arrangements in the relevant context of use, such as provisions for human oversight in accordance with the instructions for use, or complaints-handling and appeal procedures, as they could be instrumental in mitigating risks to fundamental rights in specific use cases. After completing the impact assessment, the implementing body should inform the relevant market surveillance authority. Where appropriate, in order to collect relevant information necessary for carrying out the impact assessment, implementing bodies of high-risk AI systems, in particular where the AI systems are used in the public sector, could ensure the involvement of relevant stakeholders, including representatives of groups of persons likely to be affected by the AI system and independent experts, when carrying out impact assessments and designing measures to be taken in case the risks materialise. The European Artificial Intelligence Agency (AI Agency) should develop a model questionnaire in order to facilitate compliance and reduce the administrative burden for implementing bodies.

The AI Act distinguishes risks into four main categories. AI systems that present only limited risk will be subject to minimal transparency obligations, while high-risk AI systems will require authorisation subject to a set of requirements and obligations to gain access to the EU market. AI systems, such as for example cognitive behavioural manipulation of persons and social scoring, will be prohibited by the EU because their risk is considered unacceptable. Under Article 5, the Regulation prohibits certain AI applications that threaten the rights of individuals. This reflects an agreement not to tolerate dangerous systems. In the field of education, inferring emotions is not permitted except for medical or safety reasons. This implies that it is not allowed to measure the emotions of trainees during an educational process. For example, when trainees sit examinations, it is not allowed to record their emotions and draw conclusions about them.

Under strict conditions, practices involving a high level of risk are permitted under Article 6 et seq. Such systems require an impact assess-

ment study. The AI Act sets out clear obligations for high-risk AI systems (due to the significant potential harm they may cause to health, safety, security, fundamental rights, the environment, democracy and the rule of law). These systems must assess and mitigate risks, maintain usage logs, ensure transparency and accuracy, and provide for human oversight. Users will have the right to lodge complaints about the systems and receive explanations about decisions based on high-risk systems that affect their rights. The regulatory concept of high risk has its origins in the safety of the products concerned. High-risk practices in the field of education include, according to Article 6(c), the determination of access, admission or assignment of educational and vocational training at all levels, assessment of learning outcomes and the appropriate level of education, monitoring and detection of prohibited behaviour of students during examinations. This does not mean that learners cannot be assessed and trained through technical means—but when such methods are used, appropriate safeguards must be in place to protect their rights.

According to Annex III, high-risk AI systems referred to in Article 6(3) include:

(a) AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels.

(b) AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels.

(c) AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels.

(d) AI systems intended to be used for monitoring and detecting prohibited behaviour of students during examinations within educational and vocational training institutions at all levels.

C. The Greek constitutional framework

Article 5A(2) of the Greek Constitution guarantees participation in the information society.[435] This provision reflects an effort on the part of the revising legislator to embrace the digital age by facilitating access to electronically transmitted information.[436]

Article 16 guarantees the freedom of art and science, stipulating in paragraph 1 that art and science, research and teaching shall be free, and that their development and promotion shall constitute a duty of the state. This provision may be interpreted to mean that the freedom of research is reinforced through the proper use of technology (e.g., research on incurable diseases may be supported by AI), teaching may be enhanced by AI tools, and art may be elevated by relevant applications, for instance, those that blend several artistic styles into a single work.

Article 16(2) stipulates that education constitutes a fundamental mission of the state. The constituent legislator confines itself to a general formulation, leaving it to the ordinary legislator to determine the means by which education is provided.[437] It is therefore within the discretion of the ordinary legislator to establish the method of instruction, whether that involves digital tools and AI-assisted learning, the integration of technological means, or the maintenance of conventional educational models.

---

[435] For the interpretation of Article 5A as a right to participate in the information society, see Aikaterini N. Iliadou, "Contemporary Issues in the Interpretation of the Right to Participate in the Information Society (Article 5A(2) of the Constitution)," *e-politeia* 13 (2025): 81 ff. (90), https://www.epoliteia.gr/wp-content/uploads/2025/01/MELETES-2.13.pdf; Fereniki Panagopoulou, "Interpretation of Article 5A of the Constitution," in *Article-by-Article Commentary on the Constitution*, ed. Evangelos Venizelos (Athens–Thessaloniki: Sakkoulas, 2025), 410 ff. (414); and Konstantinos Stratilatis, "Interpretation of Article 5A of the Constitution: The Right to Information," in *Article-by-Article Commentary on the Constitution*, ed. Spyros Vlachopoulos, Xenophon Contiades, and Giannis Tasopoulos (Athens: Syntagma Watch), https://www.syntagmawatch.gr/my-constitution/arthro-5a/

[436] Fereniki Panagopoulou, "Interpretation of Article 5A of the Constitution," in *Article-by-Article Commentary on the Constitution*, ed. Evangelos Venizelos (Athens–Thessaloniki: Sakkoulas, 2025), 410 ff. (414).

[437] Kostas Ch. Chrysogonos and Spyros V. Vlachopoulos, *Individual and Social Rights* (Athens: Nomiki Vivliothiki, 2017), 374.

At this point it should be noted that in a modern digital state, the right to education must necessarily encompass digital education. It would be unreasonable for public services to undergo digital transformation while individuals are not afforded the requisite education to navigate these services effectively. Such digitisation, in the absence of corresponding educational measures, would be unconstitutional, as it would lead to a 'digital divide' separating those who are able to acquire digital literacy through their own means and those who are not, thereby hindering or even obstructing their access to state services. Therefore, the right to digital education is inferred from Article 16(2), in conjunction with Article 5A, regarding access to the information society and the consequent avoidance of a "digital divide".[438] A lack of access to technology for educational purposes[439] would run counter to the right to digital literacy. At the same time, the improper use of AI tools in education would also be unconstitutional, particularly when such use prevents certain population groups from accessing educational institutions that would otherwise support their intellectual, professional, economic, and social advancement.

Furthermore, the same paragraph 2 of Article 16 of the Constitution states that education shall aim at the moral, intellectual, professional, and physical development of the Greek people. From this provision, it may be inferred that the moral and intellectual cultivation of Greeks could also be achieved through the ethical use of technology. A prominent example of such ethical use of technology is the prohibition of plagiarism and the precise detection of textual similarity through AI tools. Technology may be deemed ethical when it is designed in a way that encourages its users to engage in moral behaviour, rather than pushing them to commit criminal acts (as is the case with certain addictive online games).

Article 16(4) establishes the right to free public education. This obligation corresponds to the social right of pupils and students to receive education free of charge, which is a right that is closely aligned with the

[438] Aikaterini N. Iliadou, "Contemporary Issues in the Interpretation of the Right to Participate in the Information Society (Article 5A(2) of the Constitution)," *e-politeia* 13 (2025): 81 ff., cited at 90, https://www.epoliteia.gr/wp-content/uploads/2025/01/MELETES-2.13.pdf

[439] Ibid.

right to freedom of education.[440] It is considered the oldest social right recognized under Greek constitutional law, having first been enshrined in the Constitution of 1864. At first glance, the provision of digital education may appear to be in tension with the State's obligation to provide free public education, since not all pupils and students have access to modern digital learning tools. Social reality, however, largely dispels such concerns, as the majority of young people are users or owners of devices[441] suitable for education through AI-based tools. Complementary measures, such as providing educational devices to vulnerable groups and offering educational technology tools free of charge, further mitigate the risk of excluding socioeconomically disadvantaged populations.[442] This is because the right to free public education does not only include the constitutionally mandated free provision of education by state educational institutions, but also the right of learners in need of assistance to receive financial support.[443]

D. Legislative and advisory framework

There is no specific legislative regime covering the use of AI in education.

Nevertheless, certain key principles may be inferred from the European legal framework itself, the provisions of the Greek Constitution, Regulation 1689/2024 on AI (AI Act), and Law No. 4961/2022 on emerging information and communication technologies, strengthening digital governance and other provisions. At the same time, guidance is provided by the opinion of the High-Level Expert Group on Artificial Intelligence.

---

[440] Dimitris Sarafianos, "Interpretation of Article 16 of the Constitution," in *The Constitution: Article-by-Article Commentary*, ed. Philippos Spyropoulos, Xenophon Contiades, Charalambos Anthopoulos, and Giorgos Gerapetritis (Athens–Thessaloniki: Sakkoulas, 2017), 380 ff. (389).

[441] Fereniki Panagopoulou-Koutnatzi, "Constitutionality Issues in Distance School Education," *Administrative Law Review* 2020, 292 ff. (at 292).

[442] Ibid.

[443] Lina Papadopoulou, "Interpretation of Article 16 of the Constitution," in *The Greek Constitution: Article-by-Article Commentary*, vol. 1: Articles 1–25, ed. Evangelos Venizelos (Athens–Thessaloniki: Sakkoulas, 2024), 736 ff. (767).

According to Article 4(1) of Law No. 4961/2022, public sector entities, as defined in Article 14(1)(a) of Law 4270/2014 (Government Gazette A' 143), may, in the exercise of their powers, use AI systems for the process of making, supporting or issuing decisions or acts that affect the rights of a natural or legal person, but only if such use is expressly provided for in a specific provision of law that includes appropriate safeguards for the protection of those rights. Furthermore, according to Article 5(1) of Law No. 4961/2022, any public sector entity that intends to use an AI system, as defined in Article 4(1), must conduct an algorithmic impact assessment prior to the system's deployment. It follows from this provision that educational institutions may use AI systems in decision-making processes. The Committee proposes the development of a centralised AI education platform that will support teaching, learning and online collaboration, and host competitions in the field of AI. It recommends the provision of AI-related educational material through a centralised online platform. The platform will act as a common virtual space where educational material can be developed by AI specialist teams from academia and industry. Content creators will be invited to produce relevant material and will be remunerated based on its use. The aim is to promote the creation of a dynamic and sustainable ecosystem for AI education, where contribution is rewarded and continuous improvement is encouraged. Educational material will be subject to a rigorous evaluation process to maintain a high level of quality and educational value. Educators will be able to select materials relevant to their teaching and their audience, and each individual will be able to follow individualised studies to master new areas of knowledge and seek support to fill any knowledge gaps. The same platform will be able to host competitions and hackathons (app development marathons), offering a virtual collaborative space. These activities could be structured around specific themes or challenges, encouraging participants to develop innovative solutions using AI applications. The platform would facilitate project submission and evaluation, provide access to tools and relevant datasets, and enable communication between teams and mentors. By hosting competitions and hackathons, the platform will encourage the creation of a community of students and researchers, enhance hands-on learning and inspire creativity and innovation in the field of AI and beyond. Lastly, the same

infrastructure can be used for vocational education and training, as well as for lifelong learning.

E. Case studies

1. Conduct of examinations

The future of the examination process appears to be automated. It is anticipated that, in a few years, candidates for the national examinations will arrive at designated testing centres, sit for exams on dedicated computers, respond to standardised questions that do not require essay writing, and receive their grades upon completion of the testing session. In the following days they will submit their preferences for academic institutions and subsequently receive a message indicating the school to which they have been admitted. At a later stage, examinations may be conducted remotely from the candidates' homes,[444] who will have to install special monitoring software on their computer or on the computer provided by the examining body to participate in the examination. The software will scan the exam environment, ensure that no third party is present at the examination site, perform a system scan of the examinee's computer, deactivate any suspicious software or communication tools and monitor the examinee's behaviour throughout the process. This procedure entails two risks. First, the examinees' capacity for analytical writing is limited, as they have to answer multiple-choice questions. This may also restrict critical thinking since it involves selecting from predefined answers. Second, there is a risk of excessive monitoring of the examinee. The first risk may be mitigated by asking questions that require analytical thinking, even if it results in a delayed grading process. Furthermore, software tools already exist that are capable of evaluating written responses. It could also be argued that critical thinking is not necessarily hindered when questions call for evaluating judgement; on the contrary, such formats may increase the likelihood of examinee confusion or misinterpretation. The second risk could be addressed by taking technical and organisational measures to ensure the security of data processing.

[444] This already occurred during examinations for the selection of senior officials in the public administration.

2. Evaluation of student applications

Admission to higher education institutions should require a comprehensive assessment of applications. It is not enough to rely solely on entrance exam scores; additional factors, such as community involvement, individual skills, personality traits, and so on, should also be taken into account. Automated assessment of all these parameters reduces the risk of introducing criteria of favouritism and nepotism, and ensures the integrity of the examination process. Nevertheless, it is not always easy for an algorithm to evaluate a candidate's soft skills. How can qualities, such as teamwork, honesty, willingness to cooperate, and so on, be assessed? The safest approach may be to rely on measurable criteria only, such as entrance exam scores and documented points earned from participation in athletic, musical, or other competitive activities. As for community service, it is proposed that a dedicated committee certify such contributions, issuing an official attestation that would be scored according to its duration and weighted appropriately in the admissions process.

3. Vocational guidance

Vocational guidance may be carried out algorithmically. The person concerned enters certain data, and on this basis guidance is provided. It is essential that the categorisation developed by the algorithm must not be fixed, as this would imply that society is not evolving.[445] If, for example, the guidance relies on data from the 1980s, it would propose specific professions to women (for example, becoming a philologist) and others to men (for example, electrical engineering). Such categories should not limit us.

4. Pre-evaluation of faculty candidacies

It is envisaged that, in the future, the pre-evaluation of faculty candidates will be carried out in an automated manner. The algorithm will scan the application, check whether the required formal qualifications have been met, for example whether the candidate has completed their military ser-

[445] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 25.

vice, whether they have been awarded their doctoral degree, or provided the required recognition for foreign qualifications, and so on. The number of publications will then be calculated and scored based on the impact or recognition of the scientific journal in which they are published. Such evaluation, however, which is a consequence of the "metric era",[446] is not always straightforward in the social sciences, where there are no criteria for the relevance of journals.[447] Publications in peer-reviewed journals carry different weight compared to those in non-peer-reviewed ones. In Greece, there are also cases where journals claim to conduct blind peer review, yet the process is not genuinely anonymous. For these reasons, fully automated pre-screening of applications is not advisable. In any case, candidates retain the right to human intervention under Article 22 GDPR.

5. Text generation through generative artificial intelligence

Generative AI produces complex scientific answers to user-submitted questions.[448] Generative AI has led to applications that can provide automated responses to queries through the use of Large Language Models. These models are a type of AI algorithm that uses deep learning techniques and large datasets to produce text in a way that resembles human language. They are trained on massive data sets to predict the most likely text continuations. The content and form of such responses are becoming increasingly significant across multiple domains of our lives.

---

[446] Christina Koulouri, "Universities in the Age of Metrics," *To Vima*, 3 July 2025, https://www.tovima.gr/print/opinions/ta-panepistimia-stin-epoxi-lfton-metrikon/

[447] See, on this issue, the initiative of Christina Koulouri, Rector of Panteion University, for a digital repository, available at https://www.protothema.gr/greece/article/1425742/protovoulia-tou-padeiou-psifiako-apothetirio-epistimonikon-dimosieuseon-sta-ellinika/

[448] On generative AI see Charalampos Tsekeris, Vangelis Karkaletsis et al., *Generative AI Greece 2030: Possible Futures of Generative Artificial Intelligence in Greece* (Athens: Secretariat-General for Long-Term Planning, 2023), https://foresight.gov.gr/wp-content/uploads/2024/02/GenAI_Greece_2030.pdf

6. Supporting the educational process

Specialised tools can assist the educational process. These tools can generate engaging presentations, formulate possible questions with the desired degree of difficulty, produce summaries of course materials, evaluate students' answers, and focus on each learner individually. They offer personalised guidance, recommend revision in areas of weaknesses, carry out statistical evaluations of performance, identify gaps and deficiencies, check for text similarity, and relieve educators of administrative burdens. Such tools are valuable aids for those involved in education, provided they do not replace the teacher. Notable examples include:

a. Virtual Mentor

A widespread AI application in the field of education is Virtual Mentor. This tool can provide feedback on students' learning activities and practice questions and subsequently provide recommendations on which materials should be reviewed, much like a teacher or instructor would.[449] The system continuously learns and updates its information based on the needs and constraints faced by learners.[450] It can also identify the underlying causes of student misunderstandings and suggest strategies to address learning difficulties.

The tool assists learners during study sessions by helping to structure their thinking and by posing potential questions. In this way, the need for supplementary private tutoring may be reduced, as students no longer depend on an external instructor. Notwithstanding the above, it should not be viewed as a substitute for the educator, but rather as a support mechanism for both teachers and students.

[449] Tira Nur Fitria, "Artificial Intelligence (AI) in Education: Using AI Tools for Teaching and Learning Process," *ResearchGate*, 20 December 2021, 134 ff. (136), https://www.researchgate.net/profile/Tira-Nur-Fitria/publication/357447234_Artificial_Intelligence_AI_In_Education_Using_AI_Tools_for_Teaching_and_Learning_Process/links/61ce7029e669eeof5c76b2ba/Artificial-Intelligence-AI-In-Education-Using-AI-Tools-for-Teaching-and-Learning-Process.pdf

[450] Ibid.

b. Voice assistant

Voice assistant is one of the most widely recognised and used AI technologies (not all such assistants use AI) in various fields, including education. Examples of widely known voice assistants include Google Assistant (Google), Siri (Apple), and Cortana (Microsoft) among others. Voice assistant allows learners to search for materials, reference questions, articles, and books simply by speaking or providing keywords.

c. Automated online assessment

AI is widely used for purposes of automated online assessment and grading of questions. The use of such features makes it easier for educators to prepare and administer tests easily and efficiently. Teachers no longer need to manually compose questions and mark answers. Instead, they simply select the type of questions, the level, number of items, difficulty, and other parameters. Once the test is generated, the teacher can share the link with students who complete it online. This functionality enables the easy creation of assessment questionnaires (quizzes). Student results are instantly available in the teacher's account, with an overall score, a list of incorrect and correct answers, and a discussion feature. All of this is managed by a programmed AI system. AI can also support teachers by handling repetitive administrative tasks, such as lesson planning, exam grading, homework review, and more. By automating these processes, teachers gain more time to monitor student progress and focus on improving their instructional techniques.

This tool will operate autonomously based on programmed instructions and will be capable of learning from the user's or student's habits. Furthermore, the AI will provide recommendations for targeted material to be reviewed, as well as other suggestions based on the student's recorded performance.

d. Personalised learning

Personalised learning allows learners or users to receive services like those provided by personal assistants. The application of this technology is already quite common. AI allows learners to access tailored support by collecting data from their past learning activities and offering alternative

learning paths based on individual needs. This approach enables each student to progress and develop at their own pace and according to their capacity to absorb content, in alignment with their interests and abilities. The AI will also provide content recommendations, suggest study timetables, and carry out various other important functions. Over time, the system learns how to optimise the learning process, making it more effective and efficient. By analysing student data, AI can help educators and educational institutions identify each learner's pace and needs. Schools can then design study plans based on students' strengths and weaknesses. What must be emphasised, however, is that the technology will function solely as a tool, allowing educators the time and space they need. In any case, the unique teacher-student relationship remains essential, especially when it comes to the emotional and ethical dimensions of learning, which directly affect students' feelings and psychological well-being.

e. Educational games

Educational games serve learning purposes, while still offering play and entertainment. They provide an educational or learning experience for the players. For example, Duolingo does not just teach English: it offers access to more than 30 foreign languages that children can learn, such as Mandarin, French, Italian, Spanish, Korean, Japanese, and others. Khan Academy Kids features thousands of interactive activities for toddlers, preschoolers and kindergarten children. Within this all-in-one educational game, children can develop skills in reading, language, writing, mathematics, social-emotional learning, problem-solving skills, and motor development. Quick Brain, on the other hand, sharpens the brain's processing speed for performing calculations.

f. Automatic text translation

Automatic text translation tools support those involved in the educational process to understand the views of prominent foreign-language representatives of science, letters and arts by overcoming language barriers.

g. Virtual reality tools

Virtual reality tools can familiarise learners with foreign cultures and offer them an interactive experience of past historical eras. Learners may, for instance, engage in conversations with avatars of ancient philosophers and exchange ideas with them. By incorporating AI techniques, these platforms and their smart applications can provide personalised and immersive learning journeys, as well as automated and adaptive enhancements of the services offered, tailored to users' preferences, traits, and behavioural patterns.[451] The user interacts with the environment and visualises the information provided, resulting in enhanced understanding and assimilation of complex ideas and concepts.[452] A key feature of virtual reality is the possibility of individualised guidance, with users being able to communicate directly with experts and receive real-time information adapted to their needs and interests.[453]

h. Distance learning tools

During the pandemic, schools remained active thanks to the use of distance learning. These tools help overcome barriers to instruction during times of crises, such as pandemics, extreme weather, strikes, school closures, and similar disruptions. They enable learners to stay connected to the educational process. That said, they should not become a default or permanent substitute for in-person education, as there is a risk of weakening the social and relational bonds between educators and learners.

i. Text editing tools

Text editing tools assist with grammatical, syntactic and lexical correction, and vocabulary refinement. On the one hand, they help improve the quality of written output; on the other hand, overreliance on them

[451] Andriani Avgerinou, Fotis Gogoulos, Achilleas Kleisouras, Evangelos D. Protopapadakis, Dimitris Tsamis, and Giota Charalampaki, "Philosophy, Education, and Augmented Reality through the Digital Platform 'Traces of Philosophy: Connect, Reflect, Experience,'" *Paidagogikos Logos* 30, no. 1 (2024): 11 ff. (20), https://doi.org/10.12681/plogos.39663

[452] Ibid.

[453] Ibid.

may lead learners to neglect their own writing skills, knowing that an automatic corrector will always be available. One way to address this issue would be for the tool to identify the error but give the learner the opportunity to correct it manually before any automatic correction is applied.

7. Other applications

a. Turnitin

The Turnitin platform detects textual similarity and calculates plagiarism percentages by providing detailed similarity reports, source matching, feedback and review tools, and integration with learning platforms. It helps ensure academic integrity by identifying suspected cases of plagiarism in reports, essays and other assignments. Turnitin also streamlines the review process for originality, as professors no longer need to scrutinise everything thoroughly.

Learners can also use Turnitin as a learning tool to practice proper citation techniques before submitting work with incorrect or incomplete references.

b. Mentimeter

The Mentimeter tool aims to train learners in creating presentations that are both engaging and educational. It enables the creation of interactive presentations that include live quizzes, polls, Q&A sessions, and more.

c. Eduaide.Ai

Eduaide.AI is an AI-powered tool that streamlines lesson planning, enabling educators to design curriculum materials and teaching plans with ease. It supports teachers, administrators, and curriculum designers by generating instructional content and lesson structures quickly, reducing workload and saving valuable time.

d. AudioPen

AudioPen simplifies note-taking by converting voice into text quickly and accurately. Beyond the classroom, it serves students, educators, school staff, and business professionals alike, offering a faster way to

capture information without the burden of manual writing. It can be used to transcribe lessons, meetings, reflections, and ideas.

e. Khanmigo

Khanmigo is an AI tool that provides training support for various subjects. Teachers, students and parents can use Khanmigo for individual tutoring, homework help or supplemental instruction alongside classroom lessons.

f. Gradescope

Turnitin's Gradescope is an AI-powered grading tool for educators. It streamlines grading and student assessment, leveraging AI for speed and accuracy. Teachers can use Gradescope to grade assignments and exams, ensuring more consistent and unbiased assessment than manual grading. It also provides feedback for students.

g. SchoolAI

This tool offers AI-powered activities that teachers can seamlessly integrate into their curriculum to enrich classroom learning. With access to thousands of chatbots, students can interact with historical figures, collaborate with a writing tutor, and more, while teachers can personalise these chatbots for specific school or classroom needs. The platform also provides AI-driven insights to help educators track student progress, alongside a co-teaching chatbot, time-saving tools, and image generators that enhance lesson planning.

h. Traces of Philosophy: Connect, Reflect, Experience

The digital platform "Traces of Philosophy: Connect, Reflect, Experience",[454] was implemented as a project under the Action entitled "Synergies of Research and Innovation in the Region of Attica" of the Operational Programme "Attica 2014 – 2020". The project aimed to implement an integrated platform for managing cultural content, with the

[454] "Traces of Philosophy: Connect, Reflect, Experience," https://philosophytraces.gr

broader objective of filling a gap in existing services related to philosophical and cultural tourism in the wider Attica region, while also improving the accessibility of the single-user system.

F. Challenges and considerations

The incursion of AI into the field of education must not overlook the fundamental social function of education: the transmission of the capacity for critical engagement with knowledge and, more broadly, the teaching of critical thinking.[455] Replacing this inherently human capacity risks leading to the heteronomy of learners and undermining the free development of their personality.[456] Moreover, we must not lose sight of the fact that education is far more than the mere dissemination of information: it also aims at fostering social skills and shaping responsible and conscientious citizens, which is achieved through interaction and interpersonal engagement between students and educators. Therefore, any assessment of AI applications in education must begin with the premise that these tools are meant to be supportive in nature and not intended to replace the educator.

On the one hand, AI tools can relieve educators of burdensome administrative tasks, allowing them to focus more on student engagement and the cultivation of a positive learning environment. Presentations and learning become more engaging. Grading is conducted in an impartial and automated manner, without bias. Student progress is monitored in a systematic way. AI can help learners to develop critical thinking and computational skills, boosting their productivity and creativity, and enhancing their adaptability to technological changes.[457] AI also offers significant opportunities in terms of providing educational resources for young people with disabilities and special needs. For example, AI-based solu-

[455] National Commission for Bioethics and Technoethics (Greece), *Opinion on the Applications of Artificial Intelligence in Greek Schools* (March 2025), 4, https://bioethics.gr/announcements-26/nea-gnwmh-gia-tis-efarmoges-texnhths-nohmosynhs-sto-ellhniko-sxoleio-18-martioy-2025-3219

[456] Ibid.

[457] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 66, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

tions, such as real-time live captioning, can assist individuals with hearing impairments, while audio description can improve access for those with low vision.[458] Education in AI can also foster a deeper understanding of the ethical issues arising from its use, and of how to address them.[459] AI technologies contribute to the democratisation of education by making learning resources accessible to students in remote areas.[460] Lastly, AI plays a vital role in facilitating broader access to knowledge through its many educational applications.

On the other hand, AI tools can lead to depersonalised teaching, inaccurate assessments, and shortcomings in addressing the individual needs of each learner. Unregulated use of such tools can lead to fundamental errors that may mislead the learner from finding the truth. Mistakes can also occur during evaluation, as it is possible that multiple choice questions may not have been properly constructed. A virtual conversation with Socrates does not guarantee an accurate representation of his views. There is significant concern regarding the delivery of pre-designed, predetermined knowledge. Through poor, intentional or unintentional training of the algorithm, Socrates may lead us toward a specific direction or a particular policy choice. Moreover, when students interact with digital devices, they generate digital traces. If not used ethically, this kind of trace data (traces of digital usage and learning activity) can lead to an invasion of privacy.[461] To this set of concerns is added the fear of excessive or unregulated processing of learners' personal data; the opacity or difficulty in explaining the outcomes produced by AI applications, especially in the case of machine learning systems; the challenge of incorporating

[458] European Commission, *Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators* (Luxembourg: Publications Office of the European Union, 2022), 13.

[459] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 66, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[460] Evripidis Stylianidis and Thaleia Tsalkitzi, "Article 16," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 306 ff. (309).

[461] European Commission, *Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators* (Luxembourg: Publications Office of the European Union, 2022), 11.

ethical parameters and capabilities for logical reasoning and inference in the design of algorithms; the requirement that algorithms be fed with large volumes of scientific data; and the possibility that such data use may be restricted by intellectual property and industrial rights.[462]

Whenever our society discovers a technological tool, a not unjustified concern arises that it will deprive learners of the opportunity to practice. When handheld calculators were introduced, there was a fear that students would lose their ability to solve mathematical problems. When search applications were created, concerns were raised that learners were being spoon-fed information. The same applied for tools providing bibliographic references. It should not escape our attention, however, that these tools facilitate education by allowing learners to engage in more complex issues. The solution lies in the regulated and ethical use of such tools. This means that learners should not rely on using the tools without performing their own final review. As a result, the tool should assist and not replace the educator. Moreover, it is important that learners do not view the use of such tools as a magic genie that will solve all their problems: they should also be assessed critically in an environment where their use of such tools is not allowed, be examined orally on the work they produce with the help of AI, and be able to demonstrate that they have understood the educational content.

The goal is not to exclude AI tools from the field of education, but to ensure their proper and ethical use. The integration of AI tools into education should not be driven merely by their availability but based on their proven usefulness.[463] This entails the following:

First, the algorithm must be compatible with human dignity. AI systems should be developed in ways that respect the personal autonomy of those interacting with them. It is essential to take steps to prevent AI systems from exploiting, degrading, manipulating, instrumentalising

[462] National Commission for Bioethics and Technoethics (Greece), *Opinion on the Applications of Artificial Intelligence in Greek Schools* (March 2025), 5, https://bioethics.gr/announcements-26/nea-gnwmh-gia-tis-efarmoges-texnhths-nohmosynhs-sto-ellhniko-sxoleio-18-martioy-2025-3219

[463] Ibid, 6.

or eroding human self-determination.[464] This principle entails the exclusion of any applications that manipulate student behaviour from the educational system. Practices involving the monitoring of student behaviour, whether inside or outside the school environment, "social scoring" mechanisms, or the disclosure of either behavioural data or views expressed by students in class to third parties, when carried out through AI applications, violate the core of their personality rights.[465]

Second, the algorithm must promote the well-being of those involved. Its purpose is to support the educational process, not to replace the educator with an algorithm. It should be recognised as a tool that helps and inspires people to improve their quality of life by utilising their unique human capabilities in the context of education.[466] AI should not be seen as a means of replacing educational human labour for the sole purpose of reducing costs.[467]

Third, the algorithm must be transparent. This means that we must know how it works, on the basis of which process it evaluates or summarises texts, and so on. Algorithms, data, and AI-based decision-making procedures must be sufficiently accessible to relevant stakeholders so that the functioning of AI systems is understandable, explainable, reliable, justified, and accountable.[468]

Fourth, the algorithm must respect the privacy of learners. The recording of a learner's progress, performance fluctuations, periods of fatigue and emotional stress must be handled in a rights-friendly manner and must not have a negative impact on the learner's subsequent

[464] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 15, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[465] National Commission for Bioethics and Technoethics (Greece), *Opinion on the Applications of Artificial Intelligence in Greek Schools* (March 2025), 8, https://bioethics.gr/announcements-26/nea-gnwmh-gia-tis-efarmoges-texnhths-nohmosynhs-sto-ellhniko-sxoleio-18-martioy-2025-3219

[466] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 15, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[467] Ibid.

[468] Ibid.

personal and professional development.[469] Educational institutions are required to ensure that all data they process are stored confidentially and securely and must implement appropriate policies and procedures for the protection and ethical use of all personal data.[470]

Fifth, the algorithm must promote pluralism. This means that the algorithm should provide pluralistic education to learners, be inclusive, involve a wide range of disciplines from mathematics and physics to humanities and social[471] sciences, and not promote cultural and linguistic monoculture.[472] Actions should foster diversity and social cohesion, and target inclusion.[473]

Sixth, the algorithm must be evaluated and monitored,[474] in order to weigh the risks and benefits to stakeholders, and promote the required values. Particular attention should be paid to the selection of the appropriate form of supervision,[475] including human supervision.

---

[469] This is also the thrust of the *S. and Marper v. United Kingdom* judgment of the European Court of Human Rights (*S. and Marper v. United Kingdom*, nos. 30562/04 and 30566/04, Eur. Ct. H.R., judgment of 4 December 2008). According to the Court, the retention of data of unconvicted persons could be particularly harmful in the case of minors, given their particular situation and the importance of their development and integration into society. The Court held that particular attention should be paid to protecting minors from any harm that might result from the authorities' retention of their personal data after they have been acquitted of a criminal offence.

[470] European Commission, *Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators* (Luxembourg: Publications Office of the European Union, 2022), 11.

[471] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 15, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[472] Fereniki Panagopoulou, "Language as a Cultural Asset in Large Language Models," *HuffPost Greece*, 9 April 2024, https://www.huffingtonpost.gr/entry/h-ylossa-os-politismiko-ayatho-sta-meyala-ylossika-montela_gr_6613982ce4b056f720588bfb

[473] Spyros Polymeris, "Chaos Theory, Artificial Intelligence and Education: A Discussion," *Public Administration Review* (2024): 81 ff., at 94, https://www.lawjournals.unic.ac.cy/index.php/pareview

[474] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 15, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[475] Fereniki Panagopoulou, "Artificial Intelligence and Independent Authorities," *Journal of Public Administration* 6, no. 1 (2024): 34 ff., https://sryahwapublications.com/journals/journal-of-public-administration/volume-6/issue-1

Seventh, a distinction of particular importance must be made between education in AI and education about AI. Education in AI refers to the integration of AI into curricula as part of digital and algorithmic literacy. What is necessary, however, is a shift of focus towards education about AI, which entails familiarising students with the ethical, social, and legal questions raised by AI, with the ultimate goal of preparing them for a future of responsible and constructive interaction with AI systems that are increasingly embedded in everyday life.[476]

Eighth, the algorithm should not have as its primary mission the mere transmission of information, but rather the promotion of critical thinking.[477]

Ninth, the algorithm must ensure equal access to AI-based applications for all learners.[478]

Tenth, the algorithm must be used in a manner that complements, rather than replaces, direct teacher-led instruction. AI applications in education must not replace the student–teacher relationship, nor the interpersonal bonds that form the fabric of the educational community.[479] The school group, the classroom, and the wider school community must remain the primary environments for shaping students' social identity and the development of their social skills.[480]

G. The question of language

Of particular significance is the use of specific terminology and more generally, in the context of AI.[481] Large Language Models, presented as repositories of collective human knowledge, raise a crucial question: do

[476] National Commission for Bioethics and Technoethics (Greece), *Opinion on the Applications of Artificial Intelligence in Greek Schools* (March 2025), 6, https://bioethics.gr/announcements-26/nea-gnwmh-gia-tis-efarmoges-texnhths-nohmosynhs-sto-ellhniko-sxoleio-18-martioy-2025-3219

[477] Ibid.

[478] Ibid, 9.

[479] Ibid.

[480] Ibid.

[481] See in detail Panagopoulou, "Language as a Cultural Asset in Large Language Models," *HuffPost Greece*, 9 April 2024, https://www.huffingtonpost.gr/entry/h-ylossa-os-politismiko-ayatho-sta-meyala-ylossika-montela_gr_6613982ce4b056f720588bfb

they encompass the diverse knowledge embedded in different cultures? For example, the dominance of the English language may result in a cultural monoculture. The structures inherent in language shape the way we construct reality, and the words we employ are closely bound up with how we think about the world. Moreover, many linguistic nuances risk being lost, since what is not articulated in English is unlikely to be expressed in another language. This is why responses in English tend to appear "more correct" in terms of substance. In this context, Large Language Models trained predominantly on English texts appear to revert to English internally, even when instructed to respond in another language. Responses in Greek are produced via English translation, thereby neutralising the distinctiveness of the Greek language. This may have significant consequences for both linguistic and cultural perception.

Secondly, how are linguistic specificity and terminology determined? Who is to decide on linguistic idiosyncrasy? Linguists now train the algorithm on the basis of established Large Language Models. These models tend to exhibit stronger cultural alignment when oriented towards the dominant language of a given culture and when pre-trained in a specific linguistic idiom. In this way, diverse linguistic nuances are placed at risk. At the same time, an algorithm's choice of particular terminology predisposes the AI user towards a specific outcome. The synonymy of the terms "abortion", "termination" and "artificial termination of pregnancy" makes it abundantly clear that language in the social sciences is never value-neutral, since the use of different terms often reflects distinct ethical perspectives. The same applies to the terms "informant", "whistleblower", "public interest witness". The global consolidation of default words and expressions could distort the fundamental characteristics of scientific discourse.[482]

H. Concluding remarks

The use of AI in the field of education is recommended following strategic planning and careful assessment of the risks it entails. AI tools must

[482] Spyros Vlachopoulos, "Article 5, Free Development of Personality, Personal Freedom," in *Artificial Intelligence, Human Rights and the Rule of Law, ed. Evripidis Stylianidis* (Athens: Nomiki Vivliothiki, 2025), 89 ff. (95).

serve the fundamental principles of protecting human dignity, privacy, transparency, promoting well-being, and pluralism. At the same time, they must be subject to oversight by a supervisory authority. Regarding their introduction into the educational process, the following are proposed:

Tools ought to support, rather than replace educators. Furthermore, it is recommended that they be used as a complement to conventional education and not as a substitute for it.[483] Traditional education, which is grounded in dialogue between teacher and learner, must not be abandoned, but rather enriched with new educational methods. Particular emphasis must also be placed on the ethical use of technology within the educational sphere. And, lastly, AI must not divert us from the fundamental aim of education: the formation of responsible and conscientious citizens.

[483] Fereniki Panagopoulou-Koutnatzi, "Legal and Ethical Concerns about the Use of ChatGPT in Education," *Journal of Law and Technology* (2023): 6 ff.

V. Applications for predicting illness and death

A. Introduction

In an age of (near) absolute knowledge of all kinds of information, a question that arises is whether such information should have certain limits. Is it possible for me to know when and from what ailment I will suffer, and when I will die? Such a notion may seem fictional,[484] yet it is now technically feasible. Knowledge is power, but also a burden, and false knowledge may even become a torment.

In the context of this section, the issue of predictive medicine will be examined from an ethical and constitutional perspective. Initially, a terminological clarification of the subject will be attempted, followed by a presentation of its institutional background and history. Following this, the advantages and disadvantages of the method will be discussed. Then, the issue will be analysed from a constitutional standpoint, the European regulatory framework will be explored, the matter of oversight will be investigated and, lastly, certain recommendations will be put forward.

B. Terminological clarification

Predictive analytics is an approach within the field of AI that aims to calculate the probability of future life events (predictions), using both historical and real-time data, statistical algorithms, and machine learning methods. Predictive analytics primarily relies on synthesising heterogeneous data, such as data related to health, residence, employment and working conditions, educational background, economic profile, and so

[484] For a literary treatment, see Panagiotis Rizos, *Tartaros Ltd* (Athens: Papadopoulos, 2024).

on.[485] Predictive medicine is capable of integrating and analysing known disease characteristics alongside a particular patient's medical history and health status, utilising the resulting information to alter outcomes and determine new directions for research and development within life sciences.[486] It is related to genomic medicine, as it employs genetic testing to determine an individual's likelihood of developing a specific disease. Researchers study biomarkers associated with medical conditions and analyse large volumes of data. Such research is based on numerous genetic tests from multiple individuals.

C. History

1. The Oscar cat

It all started with a cat named Oscar. This cat was adopted by a nursing home in the United States, where he was known for making his rounds in the nursing home, sniffing and observing the patients. Indifferent to most, he would choose to lie down only next to certain patients, namely those who would die within a few hours. His assessment was so accurate that the staff developed a protocol requiring that those patients' families be called in anticipation of death. His mere presence at a patient's bedside was regarded by doctors and nursing staff as an almost certain indicator of imminent death. Oscar's story was published in the prestigious New England Journal of Medicine in 2007.[487] The author of the article, geriatrician David Dosa, eventually published a book on dementia, entitled Making Rounds with Oscar: The Extraordinary Gift of an

[485] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31 January 2025), 2, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

[486] Jeff Elton and Arda Ural, "Predictive Medicine Depends on Analytics," *Harvard Business Review*, 23 October 2014, https://hbr.org/2014/10/predictive-medicine-depends-on-analytics

[487] David Dosa, "A Day in the Life of Oscar the Cat," *New England Journal of Medicine* 357 (2007): 328–29, https://www.nejm.org/doi/abs/10.1056/NEJMp078108

Ordinary Cat.[488] The entire story drew attention to the importance of predicting death and recognising the process.

2. The prediction model: Life2vec

Predicting death just a few hours before it occurs was an important step, but not sufficient: for a prediction to be useful, it needs to be more long-term – and this is what Danish researchers sought to achieve.[489] Their study is based on the following rationale:

Machine learning has brought about a revolution when it comes to the ability of computers to analyse text through flexible computational models. In view of their structural similarity to written language, transformer-based architectures promise the creation of tools for understanding a range of multivariate sequences, from protein structures and music to electronic health records and weather forecasts. It is possible to represent human lives in a way that shares this structural similarity with language. Viewed from a certain standpoint, lives are simply sequences of events: people are born, visit the paediatrician, start school, move to a new location, get married, and so forth. It is feasible to leverage this similarity to adapt innovations from natural language processing and examine the evolution and predictability of human lives based on detailed event sequences. This can be achieved by utilising the most comprehensive registry data available, covering an entire nation of over six million people and spanning multiple decades. The data include information on life events related to health, education, occupation, income, address, and working hours, recorded on a daily basis.

The researchers created embeddings of life events in a unified vector space, demonstrating that this embedding space is powerful and highly structured. Their models allow them to predict a variety of outcomes, ranging from early mortality to subtle nuances of personality, far surpassing state-of-the-art models. Using deep learning model interpretation methods, they explored the algorithm to identify the factors en-

[488] David Dosa, *Making Rounds with Oscar: The Extraordinary Gift of an Ordinary Cat* (New York: Hyperion, 2010).

[489] Germans Savcisens et al., "Using Sequences of Life-Events to Predict Human Lives," *Nature Computational Science* (2023), https://doi.org/10.1038/s43588-023-00573-5

abling their predictions. The framework allows researchers to identify new potential mechanisms affecting life outcomes and related possibilities for personalised interventions.

The overarching goal of such models is to predict health problems and estimate the timing of death. With the help of AI, the Danish researchers created the Life2vec model, processing data from millions of people to predict the stages of an individual's life up to its end.[490] The researchers aim to explore the patterns and relationships that deep learning programmes can reveal, in order to predict a broad range of "life events" concerning health or society. This is a very general framework for predicting human life, which may predict anything for which there exist training data. For example, it could predict health outcomes, so it could predict fertility or obesity, or it might predict who will develop cancer and who will not; it could also predict whether someone will earn money. The unveiling of the programme triggered reactions about creating a "death computer," with some fraudulent websites scamming people by offering to use the AI programme to predict their life expectancy, often in exchange for submitting personal data. This software is private and is not currently available online or to the broader research community. The basis for the Life2vec model is anonymised data from approximately six million Danes, which were collected by Denmark's official statistical agency. By analysing sequences of events, it is possible to predict life outcomes up to one's last breath. In terms of death prediction, the algorithm has an accuracy rate of 78%. As for predicting whether a person will move to another city or country, its accuracy is 73%.

The researchers studied a young group of individuals aged between 35 and 65. The team then set about predicting, based on an eight-year period from 2008 to 2016, whether an individual would die within the following four years. According to the researchers, focusing on this age group where deaths are usually few and rare allowed them to verify the reliability of the algorithm. Nevertheless, the tool is not yet ready for use outside the research environment. For the time being, it is a research project exploring what is possible and what is not.

[490] Ibid.

3. Prediction of impending disease

Israel's largest healthcare provider, Clalit, used advanced analytics to develop a predictive model that identified which seemingly healthy individuals were on a trajectory leading to dialysis five years later. The model, targeting less than 1% of the population, is based on decades of digital health data from over half of Israel's population – approximately 4.5 million patients typically cared for from birth through old age.[491] Primary care physicians were then asked to reach out to those individuals identified as selected patients at risk. Following this preventive intervention, the data revealed a considerable reduction in dialysis cases within this group.[492]

A characteristic example of prediction based on genetic data is a study at Massachusetts General Hospital in Boston, where geneticist Sekar Kathiresan examined 6.6 million sites in the human genome to calculate an individual's risk of developing coronary artery disease. Following this, Kathiresan and his team used their findings to develop a polygenic risk score that could be applied to patients based on their individual genetic markers.[493] Predictive medicine uses AI to create predictive profiles (algorithms) based on data from previous individuals. The model is then developed so that a new individual can immediately receive a prediction for any need, whether it concerns a bank loan or an accurate diagnosis.

At the same time, diagnostic models can offer predictions for cardiovascular diseases, oncological diseases, and generally enable timely detection and early diagnosis of illnesses.[494]

---

[491] "How Israel's Largest Healthcare Organisation Is Approaching Digital Transformation," *MobiHealthNews*, https://www.mobihealthnews.com/news/emea/how-israels-largest-healthcare-organisation-approaching-digital-transformation

[492] Ran Balicer, "The Doctor Will See Your Future Now," *Forbes*, 16 April 2018, https://www.forbes.com/sites/startupnationcentral/2018/04/16/for-predictive-medicine-its-back-to-the-future/

[493] Matthew Warren, "The Approach to Predictive Medicine That Is Taking Genomics Research by Storm: Polygenic Risk Scores Represent a Giant Leap for Gene-Based Diagnostic Tests. Here's Why They're Still So Controversial," *Nature* 562 (2018): 181–83, https://doi.org/10.1038/d41586-018-06956-3

[494] Paraskevi Panagopoulou, "The Use of Artificial Intelligence in Medicine," *dia-LOGOS* 14 (2014): 253 ff. (259 ff.).

Applying this way of reasoning, a patient might visit their doctor and be informed that they are likely to have a heart attack within a few hours, allowing for pre-emptive treatment before it occurs.[495]

D. Issues and considerations

Predicting an individual's health status and the occurrence of their death entails both advantages and disadvantages.

1. Advantages: Knowledge as power

Predictive medicine carries many advantages, both at the individual and collective level.

First, predicting a disease can lead to its prevention; if you are aware of it, you may be able to prevent it. If someone knows they will develop cancer, they can take all necessary measures to prevent it. A woman might even go so far as to remove her breasts if the predicted risk of breast cancer is very high.

Second, prediction can lead to appropriate health policy planning. For instance, if there is a prediction of many Alzheimer's cases, appropriate measures can be taken to manage the condition. The state can engage in strategic planning with campaigns emphasising factors that delay the onset of the disease, such as physical and mental exercise. Thus, predictive analytics seeks to contribute to preventive planning and optimal management of conditions.[496] In this way, predictive analytics can strengthen preventive actions and precision medicine therapeutic approaches. Additionally, predictive analytics can contribute to healthcare services management, primarily towards the fair allocation of resources to ensure logistical adequacy, the right of access to health, cost containment, and system resilience, especially when it comes under in-

[495] Ran Balicer, "The Doctor Will See Your Future Now," *Forbes*, 16 April 2018, https://www.forbes.com/sites/startupnationcentral/2018/04/16/for-predictive-medicine-its-back-to-the-future/

[496] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31 January 2025), 2, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

tense pressure (pandemics, natural or human-induced disasters, etc.).[497] Predictive medicine can forecast a pandemic, an infectious disease, environmental disasters and contribute to the resilience of the health system. Such prediction is not, however self-evident, as Google failed to predict the recent coronavirus pandemic.

Third, knowledge of a condition and prediction of death allows an individual to manage their affairs and resolve outstanding matters, such as preparing their will and settling their financial and family obligations.

Fourth, predictive medicine tools can develop personalised treatment regimens by leveraging electronic medical records to identify types of patients who are most likely to respond to a particular type of therapy. They can identify treatments that maintain health with greater accuracy than ever before, as well as determine which individuals are likely to cease benefiting from a specific treatment regimen at a given point in time.[498] In this respect, accurate predictions can reduce hospital readmissions. A notable example is the Carolinas HealthCare System (CHS), a hospital network with more than 900 health centres in North and South Carolina, which recently reduced readmission rates by one-third using Predixion software. In this particular application, CHS provided nurses with patient information at the point of care so that when patients were about to be discharged, nurses could tailor clinical interventions based on each patient's predicted risk of readmission.[499] Another example is when a patient visits their doctor with chest pain, for instance. If the doctor can input the patient's responses into a reliable predictive algorithm, a clearer picture of the patient's needs may emerge. This algorithm will include work history, chest pain history, other symptoms, and the results of any other predictive indicators within the patient's data set, including the likelihood of heart disease. In this case, predictive medicine could con-

[497] Ibid, 3-4.

[498] Jeff Elton and Arda Ural, "Predictive Medicine Depends on Analytics," *Harvard Business Review*, 23 October 2014, https://hbr.org/2014/10/predictive-medicine-depends-on-analytics

[499] Ibid.

firm or refute the doctor's suspicions and assist them in making informed decisions regarding the patient's care.[500]

Fifth, the use of polygenic risk scores in combination with traditional risk assessments may assist physicians in identifying patients who are at greater risk of developing diseases. Polygenic risk scores can also improve diagnostic effectiveness.[501]

Sixth, predictive medicine can lead to resource savings. Algorithms will enable doctors and hospitals to provide insurance companies with predictions regarding the number and type of cases they will handle in a given year. As time passes, these predictions will achieve greater accuracy and may potentially save significant amounts of money for insurance companies and policyholders.

2. Disadvantages: Knowledge as a liability

At times, prediction can become tormenting. Processing large amounts of data does not necessarily result in individual or societal benefit – and this is for the following reasons:

First, the potential knowledge of an illness can become nightmarish for the individual, who may passively endure their fate, await the progression of the illness, and have no motivation to improve. After all, what is the point of pursuing studies, for example, when one knows they stand at death's doorstep?

Second, the possibility of a misdiagnosis could have devastating consequences for the individual concerned. They may be devastated by the idea of a death or disease that may never come and passively resign themselves to what is often a mistaken fate. This raises the issue of information management on the part of patients: if someone finds out that they will suffer from dementia in the very near future, they may even be driven to suicide.

---

[500] "Everything You Need to Know about Predictive Healthcare," *educations.com*, https://www.educations.com/articles-and-advice/healthcare-studies/everything-you-need-to-know-about-predictive-healthcare

[501] Matthew Warren, "The Approach to Predictive Medicine That Is Taking Genomics Research by Storm: Polygenic Risk Scores Represent a Giant Leap for Gene-Based Diagnostic Tests. Here's Why They're Still So Controversial," *Nature* 562 (2018): 181–83, https://doi.org/10.1038/d41586-018-06956-3

Third, including too many variables could undermine the reliability of this type of analysis. For instance, genetic tests, which constitute the cornerstone of preventive medicine, are not always accurate: at the very least, genetic tests do not always provide a complete picture of the patient, whereas genes are not the only factors responsible for diseases. Other factors, such as environment, lifestyle, and work history, may also play a significant role when it comes to patients' health and the development of various diseases. For example, there exist life-affirming motivations for an elderly patient to see their grandchild graduate from school or university. There are variables for these models that we do not yet know, and it is very likely that once these are discovered and the systems are trained on them, the model's prediction for each patient will change accordingly.

Thus, the validity and reliability of the data being used come into question. The data employed for the parameterisation of the algorithm may lead to bias.[502] The sample must be representative for the mean and standard deviation to have meaning.[503] Biases may also arise in the implicit criteria of an algorithm, stemming from the learning phase in machine learning techniques. For example, if the trainer of the algorithm defines a dog as having two ears, the system will not be able to recognise as a dog one with only one ear.[504] Likewise, if the training sample of images does not include any Peruvian hairless dogs, the algorithm will not identify such a dog as belonging to the category.[505] Validity checks of such applications should be conducted in advance.[506] Using health history for future predictions would likely encounter limitations posed by the lack of representativeness of population groups, as well as the unsystematic recording of social, psychological, and behavioural determinants in addition to biomedical data.[507] It should not escape our at-

[502] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 103.

[503] Ibid.

[504] Ibid., 105.

[505] Ibid., 107.

[506] Paraskevi Panagopoulou, "The Use of Artificial Intelligence in Medicine," *dia-LOGOS* 14 (2014): 253 ff. (267).

[507] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31

tention that predictive algorithms are always based on an analysis of the past.[508] The fragmentation of data casts doubt on data quality.[509] Potential biases contained in algorithm training data are also added to these weaknesses, as predictions rely on data that may not be representative or inclusive. Models can perpetuate prejudices embedded in their training data.[510] Moreover, ambiguities, lack of commonly accepted terminology, differing reference scales, inaccuracies in diagnosis during examinations and treatment administration, as well as acronyms in record-keeping can create unsuitable data sets.[511] The issue of the temporal validity of data must also not escape our attention: given that the data used by predictive analytics have been collected up to a given point in time and thus cover a specific time period, any failure to update them promptly may lead to underestimation or overestimation of factors that may have influenced the situation up to the moment the prediction concerns.[512] It should also be noted that if health policies are based only on current data, there is a risk that these data will already be outdated and thus unreliable. Therefore, the following question arises: can an algorithm, no matter how complex, replace human abilities and function like a human being?[513]

Fourth, information concerning an individual's condition and death is at risk of being leaked to unauthorised parties, such as employers, insurance companies, and banks. Hence, employers may add predictive medicine parameters to their hiring criteria, sidelining meritocracy. Likewise, insurance companies may hesitate to insure future patients or will

January 2025), 3, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

[508] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 119.

[509] Paraskevi Panagopoulou, "The Use of Artificial Intelligence in Medicine," *dia-LOGOS* 14 (2014): 253 ff. (266).

[510] Paraskevi Panagopoulou, "The Use of Artificial Intelligence in Medicine," *dia-LOGOS* 14 (2014): 253 ff. (267).

[511] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31 January 2025), 4, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

[512] Ibid.

[513] Eleni Kalokairinou, "Towards an Ethics of Artificial Intelligence," *dia-LOGOS* 14 (2024): 193 ff. (203).

do so under burdensome terms. An ethical issue arises as to whether we have the right to allow insurance companies to handle the results of predictions in a biased manner.[514] For years, banks have been using information about their customers to predict financial risks and recommend investment strategies. One major question persists: who has access to an individual's genetic profile, and who is responsible for it? Added to all the above is the fact that AI is trained on data that are not always properly anonymised, placing them at risk of misuse or malicious access.[515]

Fifth, there is a risk that individuals with negative genetic predictive factors for certain diseases may face discrimination.

Sixth, we must not overlook the risk of over-reliance on analytical predictions. Human medical judgement may be downgraded, fostering excessive reliance on the capabilities of machines. The dominance of the belief that technology can solve everything may undermine trust in humans and lead to detrimental consequences.[516] In the end, the indiscriminate use of predictive medicine could result in AI replacing doctors rather than assisting them.

E. Constitutional analysis

Predictive medicine affects individual dignity, the right to health, access to information, privacy, personal data protection, and the rights of minors. The critical constitutional question is whether an individual has a right to know their future health status.

Could such a right derive from the constitutionally enshrined right to health?

---

[514] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 114.

[515] Paraskevi Panagopoulou, "The Use of Artificial Intelligence in Medicine," *dia-LOGOS* 14 (2014): 253 ff. (268).

[516] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31 January 2025), 4, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

The right to health in the Greek Constitution has two aspects: on the one hand, it is established as an individual defensive right (Article 5(5)(a)),[517] and, on the other hand, as a social right (Article 21(3)).

The defensive right to health establishes a claim against state interference. Furthermore, Article 5(5)(b) of the Constitution, as revised in 2001, provides for the protection of the individual against biomedical interventions. It is emphasised, however, that this constitutional provision qualifies the protection offered by subjecting it to the general reservation of law.[518] In this way, the Constitution authorises the ordinary legislator to regulate such protection, allowing the law to impose conditions and limitations within this framework. In both cases, health is understood as both the state of physical and mental well-being and public health.[519] Beyond the state of physical and mental well-being, it is also deemed necessary to define the right to health in negative terms, that is, as the individual's physical condition that prevents any illness or disability capable of reducing their normal activity.[520] It is a fact that predictive medicine, after all, aims (also) at disease prevention and thus falls within the scope of the right to health.

Health as a social right, in the sense of positive actions taken by the state to organise a health care system, is enshrined in Article 21(3) of the Constitution, according to which the state must care for citizens' health.[521] According to the Council of State's case law, Article 21(3) imposes an "obligation on the state to take positive measures to protect citizens' health, giving them the right to demand fulfilment of this

[517] The defensive nature of the right is emphasised by Evangelos Venizelos in Evangelos Venizelos, *The Revisionary Acquis: The Constitutional Phenomenon in the 21st Century and the Contribution of the 2001 Revision* (Athens–Komotini: Ant. N. Sakkoulas, 2002), 143.

[518] Charalambos M. Tsiliotis, "Public Law Parameters of the Anti-Covid 19 Vaccination," in *Covid-19, Practical Issues of Legal Protection* (Athens: Nomiki Vivliothiki, 2021), 22.

[519] Evangelos Venizelos, *The Revisionary Acquis: The Constitutional Phenomenon in the 21st Century and the Contribution of the 2001 Revision* (Athens–Komotini: Ant. N. Sakkoulas, 2002), 143.

[520] Kostas Ch. Chrysogonos and Spyros V. Vlachopoulos, *Individual and Social Rights* (Athens: Nomiki Vivliothiki, 2017), 575.

[521] Council of State (Greece), Decision No. 400/1986, *The Constitution Journal* 1986: 433–439 (436); Council of State, Decision No. 549/1987; Konstantinos Kremalis, *The Right to Health Protection* (Athens, 1987), 175 n. 215.

obligation by the state"[522] For example, if many Alzheimer's cases are predicted, the state must adopt a national strategy to address it. In this sense, Article 21(3) recognises an actionable social right, granting citizens a claim against the state for health protection, whilst imposing an obligation on the state to provide necessary health services.[523] In practice, this constitutes the state's duty to provide services or take actions that promote, maintain, or restore citizens' health.[524] Therefore, constitutional protection of health is a right and not merely an expression of aspirations.[525] In view of this, taking measures to protect citizens' health becomes imperative. As predictive medicine aims at designing preventive health measures, its adoption falls within the scope of the social right to health, and it contributes to the advancement of medical knowledge and the optimisation of therapeutic methods.[526]

It is considered that the right to health, combined with the right to the free development of one's personality (Article 5(1) of the Constitution) and the right to information (Article 5A), also implies a right to know the state of one's health. It would be incongruous for the Constitution to enshrine a general right to information while excluding information so intrinsically linked to an individual's health. How can one take care of their health if they do not know its state? How can they seek the best possible treatment if they do not have all the relevant data? A question arises as to the extent to which such information should be provided. Is a limited right to have knowledge of only one's current health

[522] Council of State (Greece), Decision No. 400/1986, *The Constitution Journal* 1986: 433–439 (437).

[523] Konstantinos Kremalis, *The Right to Health Protection* (Athens, 1987), 175.

[524] Patrina Paparrigopoulou, "Article 21 paras. 2, 4, 5, 6 of the Constitution," in *Constitution: Article-by-Article Commentary*, ed. Filippos Spyropoulos, Xenophon I. Contiades, Charalambos Anthopoulos, and Giorgos Gerapetritis (Athens–Thessaloniki: Sakkoulas, 2017), 535 ff. (548).

[525] Ismini Kriari-Katrani, "Administrative Law in the Face of the Challenges of Biology and Medicine," in *Proceedings of the Hellenic Society of Administrative Studies 1992–2003* (Athens, 2004), 75 ff. (83); Theodoros Aravanis, "Articles 21 § 3 and 109 of the Constitution: Observations on CoS 400/86 (Plenary)," *The Constitution Journal* 1987: 480 ff. (483).

[526] Antonia Nikolopoulou, "Article 21, Health and Artificial Intelligence," in *Artificial Intelligence, Human Rights and the Rule of Law, ed. Evripidis Stylianidis* (Athens: Nomiki Vivliothiki, 2025), 426 ff. (442).

status sufficient, or should this knowledge also include the prediction of future events? – for example, knowing that certain insulin levels tend to cause diabetes in the future. It is deemed that comprehensive protection of health encompasses the prediction of future health status in order to enable effective management both at the individual and collective level. Therefore, the individual has the right to be thoroughly informed[527] about their state of health and the right of access to their medical file[528] and medical opinions.[529] In this respect, Article 11(1) of Law 3418/2005 (Code of Medical Ethics) stipulates that the physician has a duty of truthfulness towards the patient and must inform them fully and in a comprehensible manner about the actual state of their health.

A corresponding right to information is also provided under Article 10 of the Oviedo Convention. From the right to know medical data also derives the right not to know medical or genetic data.[530] The physician is obliged to inform the directly concerned person, but if that person declares that they do not wish to be informed and do not want to know distressing details about the course of their illness, then the patient is not obliged to be burdened with knowledge that will cause them distress.[531] Thus, Article 11(2) of Law 3418/2005 provides that the physician must respect the wishes of individuals who choose not to be informed. In such

[527] For a detailed discussion on the obligation to inform patients, see Ismini Androulidaki-Dimitriadis, *The Patient's Right to Information: Contribution to the Establishment of Civil Medical Liability* (Athens–Komotini: Ant. N. Sakkoulas, 1993), 83 ff.

[528] Udo Di Fabio, in T. Maunz, G. Dürig, R. Herzog, and R. Scholz, eds., *Kommentar zum Grundgesetz*, 48th update (Munich: C.H. Beck, 2006), Art. 2 para. I, marginal no. 204.

[529] Federal Constitutional Court of Germany (BVerfG), BVerfGE 32, 373 (378 ff.); BVerfGE 89, 69 (82 f.).

[530] Udo Di Fabio, "Article 2 para. I," in T. Maunz, G. Dürig, R. Herzog, and R. Scholz, eds., *Kommentar zum Grundgesetz*, 48th update (Munich: C.H. Beck, 2006), Art. 2 para. I, marginal no. 204; Spyros Vlachopoulos, "Prenatal Testing and Individual Rights: The Modern Developments of Genetics, Scientific Freedom, and the Right to Genetic Ignorance," *Dikaioma tou Anthropou* 2002: 363 ff. (364); Takis K. Vidalis, *Biolaw, vol. I: The Person* (Athens–Thessaloniki: Sakkoulas, 2007), 52 ff. Reservations regarding the right not to know are expressed by Ismini Kriari-Katrani, *Genetic Technology and Fundamental Rights* (Athens–Thessaloniki: Sakkoulas, 1999), 116 ff., in the case of genetic analyses.

[531] Martin Koppernock, *Das Grundrecht auf bioethische Selbstbestimmung: Zur Rekonstruktion des allgemeinen Persönlichkeitsrechts* (Baden-Baden: Nomos, 1997), 89.

cases, the patient has the right to request that the physician inform exclusively another person or persons designated by them.

Beyond the right not to know what one does not wish to know, the right to health in conjunction with the free development of one's personality also guarantees the right not to engage with matters one does not wish to deal with[532] – for example, the right not to draft a will if doing so entails an unpleasant and painful process for the individual concerned. In this vein, it is emphasised that the provision of knowledge deriving from predictive medicine must occur with the free consent of the individual. Mandatory disclosure infringes upon human dignity, as it deprives the individual of their autonomy and their right to an open future. An open future seems constrained when one knows they will soon become ill. As mentioned above, the right to knowledge is combined with the right not to know, whether this concerns the present or the future of a person.[533]

In addition to the above, due to the ability of predictive medicine to process vast volumes of data, significant challenges also arise in the area of patient privacy.[534] Predictive medicine affects the right to personal data protection, as enshrined in Article 9A of the Constitution. Under this Article, the individual has the right to informational self-determination, namely the right to determine who will have access to their personal data. Unrestricted access by unauthorised persons to an individual's health prediction data infringes upon their right to informational self-determination. Moreover, failure to implement the necessary security measures for their health prediction data violates their right to personal data protection.

---

[532] Federal Constitutional Court of Germany (BVerfG), BVerfGE 27, 1 (6); BVerfGE 44, 197 (203).

[533] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31 January 2025), 1, 4, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

[534] Antonia Nikolopoulou, "Article 21, Health and Artificial Intelligence," in *Artificial Intelligence, Human Rights and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 426 ff. (442).

Lastly, this technology must be protective of childhood[535]: this means that minors should not have access to this kind of information, as this would deprive them of their right to an open future. If a child becomes aware that they may become ill, they might abandon any aspirations they have.[536]

F. The European regulatory framework: Risk categorisation under the Artificial Intelligence Act

The AI Act classifies AI systems into four categories, depending on the level of risk that they pose. According to Article 5, the Regulation prohibits certain AI applications that threaten citizens' rights, reflecting a consensus to reject dangerous systems. The largest part of the Regulation concerns high-risk AI systems, pursuant to Article 6, which are subject to regulation. These systems, which include predictive medicine applications, require an impact assessment study. The Regulation sets out clear obligations for high-risk AI systems, due to the significant potential harm they may cause to health, safety, fundamental rights, the environment, democracy, and the rule of law. These systems must assess and mitigate risks, maintain usage logs, ensure transparency and accuracy, and guarantee human oversight. Citizens will have the right to file complaints regarding these systems and to receive explanations about decisions based on high-risk systems that affect their rights. The regulation of high-risk systems originates from safety standards related to the products concerned.

[535] National Commission for Bioethics and Technoethics, *Statement on the Protection of Children from the Adverse Effects of Algorithms on Social Media* (17 December 2024), https://bioethics.gr/announcements-26/nea-dhlwsh-gia-thn-prostasia-twn-paidiwn-apo-dysmeneis-epiptwseis-twn-algori8mwn-sta-mesa-koinwnikhs-diktywshs-17-dekembrioy-2024-3209

[536] See Andrie G. Panayiotou and Evangelos D. Protopapadakis, "Ethical Issues concerning the Use of Commercially Available Wearables in Children: Informed Consent, Living in the Spotlight, and the Right to an Open Future," *Jahr–European Journal of Bioethics* 13, no. 1 (2022): 9-22, especially 16ff, https://doi.org/10.21860/j.13.1.1

G. The matter of oversight

Can these prediction applications operate freely without oversight? Can any person simply install an application and predict their own death or future illness? Should we, as a society, be monitoring the use of such applications? It is true that overregulation may stifle innovation, but it protects fundamental rights. The operation of a predictive application poses a high risk to fundamental rights, as defined in Article 6 of the Regulation. It may devastate the individual, lead to misdiagnosis, violate their right to an open future, and limit their choices through unauthorised access to a range of highly useful data for the interests of insurance companies and recruitment firms. Devices lacking sufficient clinical validation pose risks to patients' rights.[537] It must be ensured that human agency and oversight are present at every stage, from design and development to operation.[538] Due to this reason, it is considered that such applications should be supervised by an independent authority to ensure their reliability. The most appropriate authority for this would be the reconstitution of the Data Protection Authority into an Authority for the Protection of Privacy, Information, and Artificial Intelligence.[539] Along the same lines, medical supervision is also necessary for patients receiving this information, to ensure they can cope with it appropriately.

H. Recommendations

The use of predictive medicine methods may lead to the enhancement of the right to health, but it also poses a high risk to individual rights. For this reason, strict planning of its use is required, along with an impact assessment study on the technology's effects on the fundamental rights of

[537] Sammy Chouffani El Fassi et al., "Not All AI Health Tools with Regulatory Authorization Are Clinically Validated," *Nature Medicine* 30 (2024): 2718–2720, https://doi.org/10.1038/s41591-024-03203-3

[538] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility," in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (274).

[539] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 89-90, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

those involved.[540] The predictive power of machines must be put to the service of human self-determination.[541] The risks are numerous and significant, and relate to the possibility of misdiagnosis, the violation of individual autonomy, and breaches of personal data through unauthorised access by groups wishing to gain this kind of knowledge, such as insurance companies and employers. Therefore, protocols must be designed, and all healthcare professionals should be trained in the proper management of patient information disclosure.[542] In this respect, patients should receive such information via a physician trained in how to inform them, who will also be responsible for overseeing how patients manage this information. Additionally, it is necessary to set technical requirements ensuring the transparency and explainability of decisions made by predictive analytics medical methods.[543] Furthermore, a detailed description of all the variables that a predictive method must take into account, depending on its subject matter.[544] Physicians must inform patients that this is merely a prediction, which may even be overturned by a random event. Continuous updating of predictive analytics models is also of utmost importance.[545] Ensuring that technical and organisational measures are taken to prevent unauthorised access and to protect patient privacy and their right to personal data protection is crucial. Finally, in order to protect childhood, access to predictive information should not be granted to minors.

---

[540] Article 27 of the AI Act provides for the obligation of deployers to conduct a fundamental rights impact assessment of high-risk systems.

[541] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility," in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (274).

[542] National Commission for Bioethics and Technoethics (Greece) and National Bioethics Committee (Cyprus), *Joint Opinion on the Ethics of Predictive Analytics in Health* (31 January 2025), 6-7, https://bioethics.gr/announcements-26/paroysiash-koinhs-gnwmhs-eebt-eebk-%22h8ikh-ths-probleptikhs-analytikhs-sthn-ygeia%22-31.01.2025-3215

[543] Ibid.

[544] Ibid.

[545] Ibid.

I. Concluding remarks

According to Hippocrates, the best physician is the one who can foresee.[546] Such foresight can be achieved by predictive medicine through AI applications. Indeed, predictive medicine can play a decisive role in improving citizens' health by contributing to timely diagnosis and treatment, as well as to more efficient management of medical resources,[547] provided that the values of AI predictive models align with human values.[548] Notwithstanding the above, its use carries many risks for people's rights, including their right to an open future, their autonomy, and the protection of privacy and personal data. For this reason, predictive medicine must be used with great caution and prudence. Human beings will always hope to overturn the prediction – and that is where their true greatness lies.

[546] Antonia Nikolopoulou, "Article 21, Health and Artificial Intelligence," in *Artificial Intelligence, Human Rights and the Rule of Law, ed. Evripidis Stylianidis* (Athens: Nomiki Vivliothiki, 2025), 426 ff. (426).

[547] Ibid, 449.

[548] Paraskevi Panagopoulou, "The Use of Artificial Intelligence in Medicine," *dia-LOGOS* 14 (2014): 253 ff. (269).

VI. Regulatory sandboxes

A. Introduction

The concern that over-regulation stifles innovation is addressed by the EU legislator through the introduction of regulatory sandboxes. Regulatory sandboxes are a mechanism for cooperation between product or service providers and regulators during the development phase. They were first used in the financial services sector, where they achieved significant success, and subsequently extended to other sectors.[549] The use of regulatory sandboxes is established in many countries, including Singapore, Canada, Australia, the U.S., and countries in Latin America and Africa, such as Brazil and Nigeria.[550]

B. Terminology

Under Article 3(55) of the Regulation, 'AI regulatory sandbox' means a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision. This definition broadly follows regulatory sandbox arrangements in other fields and legal orders. Time limitation, regulatory supervision, the existence of a sandbox plan, and the

[549] Financial Conduct Authority, *Regulatory Sandbox Lessons Learned* (2017), https://www.fca.org.uk/publications/research/regulatory-sandbox-lessons-learned-report; Dirk A. Zetzsche et al., "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation," *Fordham Journal of Corporate & Financial Law* 23 (2017): 64, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018534

[550] World Bank, "Four Years and Counting: What We've Learned from Regulatory Sandboxes," *World Bank Blogs* (2020), https://blogs.worldbank.org/en/psd/four-years-and-counting-what-weve-learned-regulatory-sandboxes

innovative nature of the products being developed are general features of sandboxes.

The term "regulatory sandbox" derives from virtual digital environments in which software can be executed without saving files or making permanent changes to the host computer's software. Such digital environments are typically used with software that may contain malicious code or software that may otherwise harm the operating system, and are therefore used for experimentation or testing. By analogy, regulatory sandboxes enable the development of products that may have negative consequences, but within a controlled environment.

Regulatory sandboxes are a way of reconciling the need for innovation with the objectives of regulation in the relevant economic sector, and mitigate potential disincentive effects of regulatory rules on economic activity. They usually focus on innovation and promote cooperation between participating private actors and regulators. This cooperation is often paired with favourable derogations from standard rules, such as granting temporary licences, exceptional waivers of licensing requirements, and limiting or eliminating participants' civil or administrative liability, provided they comply with the sandbox terms laid down directly in legislation, or left to the discretion of the regulatory authorities.

C. Their enshrinement in the Artificial Intelligence Act

The provision for regulatory sandbox in Article 57 of the Regulation came in response to the legitimate concern that over-regulation could become a barrier to innovation.[551] This provision fosters innovation by promoting a more favourable environment for developing new products, while mitigating companies' potential exposure to administrative

[551] Mario Draghi, *The Future of European Competitiveness*, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en. For a critical assessment see Anu Bradford, "The False Choice Between Digital Regulation and Innovation," *Northwestern University Law Review* 119, no. 2 (2024): 377, https://scholarlycommons.law.northwestern.edu/nulr/vol119/iss2/3/. See also Sofia Ranchordas, "Innovation Experimentalism in the Age of the Sharing Economy," *Lewis & Clark Law Review* 19 (2015): 871.

control. It is worth noting that limiting companies' potential exposure to legal risks relates not only to the exemption regime established by the Regulation, but also to close cooperation between regulators and participants. Such cooperation reduces the likelihood of authorities considering a product non-compliant with the law, provided that participants follow the relevant guidance.

Regulatory sandboxes pursue a number of purposes explicitly listed in the Regulation.[552] In particular, the Regulation provides that regulatory sandboxes aim to: (a) improve legal certainty in relation to compliance with its provisions; (b) enable the exchange of best practices between providers and cooperating authorities; (c) promote innovation and competitiveness; (d) contribute to regulatory learning; and (e) facilitate and accelerate the access of AI systems to the Union market, especially when provided by SMEs, including start-ups.

The competent authorities of the Member States must establish at least one regulatory sandbox and put in place a basic governance and oversight framework by 2 August 2026.[553] This obligation may also be fulfilled through participation in an existing regulatory sandbox, provided it offers an equivalent scope of application. Sandboxes may be established either by a single Member State, by several Member States, or by the European Data Protection Supervisor. In addition, regulatory sandboxes may also be established at regional or local level.

Regulatory sandboxes must be supervised by the national competent authorities in line with applicable EU and national rules; the supervisory and corrective powers of the competent authorities remain unaffected.[554] Where the development of the relevant products involves the processing of personal data, competent authorities must ensure the involvement of national data protection authorities in supervising the regulatory sandbox, within their respective competences. The same applies where the product development activities fall within the competence of another regulatory authority.

[552] Article 57(9) of Regulation 2024/1689.
[553] Article 57(1) of Regulation 2024/1689.
[554] Article 57(6), (7), and (11) of Regulation 2024/1689.

The eligibility conditions for providers to participate in regulatory sandboxes, as well as their operating conditions, are regulated by a Commission implementing act.[555] The Regulation provides that this implementing act must ensure fair access for all providers meeting the relevant criteria, keep pace with demand for participation, and support the flexibility of the competent national authorities.[556] Moreover, in order to enhance competitiveness, start-ups and SMEs may participate in regulatory sandboxes free of charge. The Regulation also obliges the Commission to ensure that participation procedures are simple and understandable, in particular for smaller companies with limited resources. Finally, the relevant conditions are uniform across the EU to ensure mutual recognition and avoid divergences between Member States.

The testing of a product within a regulatory sandbox requires the development of a sandbox plan, agreed between the provider and the competent authority.[557] The testing period lasts for a defined duration, depending on the characteristics of the product under development. During testing, the competent authorities support the participating provider, in particular regarding potential risks to fundamental rights, health, and safety. At the same time, the competent authorities must guide providers on measures to address these risks, including their effectiveness. Such guidance obligations do not affect the supervisory or corrective powers of the competent authorities. If the above risks arise during development and cannot be effectively mitigated, the competent authorities may temporarily or permanently suspend the testing process or participation in the sandbox.[558]

At the end of the development period, the competent authority issues written confirmation of the activities successfully carried out in the sandbox, together with an exit report describing the activities and their results.[559] Providers may use these documents to support their demonstration of compliance with the Regulation, and they are taken into account to expedite the conformity assessment process. It should be noted

[555] Article 58(1) of Regulation 2024/1689.
[556] Article 58(2) of Regulation 2024/1689.
[557] Article 57(5) of Regulation 2024/1689.
[558] Article 57(11) of Regulation 2024/1689.
[559] Article 57(7) of Regulation 2024/1689.

that these documents do not in themselves establish compliance, and providers remain fully responsible for documenting it.

As mentioned above, regulatory sandboxes are often accompanied by a favourable exemption regime involving derogations from general rules or procedures. Regulatory sandboxes for AI do not provide for procedural derogations. Nevertheless, they do introduce a favourable regime whereby, provided that providers comply with the authorities' instructions and the sandbox plan, they are not subject to administrative fines.[560] This exemption also extends to any third-party regulatory authorities involved in the sandbox. This provision raises interpretative issues, as the Regulation applies only once a product has been placed on the market, whereas participation in regulatory sandboxes occurs beforehand.[561] One view holds that the exemption from administrative fines should be interpreted as covering cases where the competent authorities have discretionary powers. Such discretion usually exists, however, at least when determining the amount of the fine. It therefore seems more appropriate to interpret the exemption as covering non-compliance arising from activities previously carried out within the sandbox, provided that there is no deviation from the sandbox plan and the authorities' instructions. Moreover, the interpretative issue of the prior operation of sandboxes is not linked to whether the competent authorities exercise binding or discretionary powers.

Otherwise, participation in the sandbox does not affect the liability of participants for damage caused to third parties. Maintaining participants' liability towards third parties is a widespread practice in regulatory sandboxes, though some commentators have criticised this provision as discouraging innovation.[562] Even so, any limitation of liability would raise questions of fairness at the level of legal policy, particularly in relation to Fletcher's well-established common law theory of the asym-

[560] Article 57(12) of Regulation 2024/1689.

[561] Nathan Genicot, "From Blueprint to Reality: Implementing AI Regulatory Sandboxes under the AI Act," *FARI & LSTS Research Group* (VUB, 2024), 28.

[562] John Truby et al., "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications," *European Journal of Risk Regulation* 13 (2022): 270, 286, https://ris.utwente.nl/ws/files/304762207/a_sandbox_approach_to_regulating_high_risk_artificial_intelligence_applications.pdf

metric distribution of potential risks and benefits in the context of tort liability.[563]

The Regulation also contains a provision departing from the general rules relating to the processing of data within regulatory sandboxes for purposes other than those for which they were originally collected.[564] Further processing of data for other purposes is solely for the trial development of AI systems within the sandbox and under specific conditions. First, the development of AI systems must serve the public interest in areas such as public security and public health, environmental protection, energy sustainability, the security and resilience of transport systems, or the efficiency of public administration. Second, the principle of data minimisation remains in force, and therefore the development of the AI system must not be feasible using anonymised or synthetic data. In addition, such processing must be accompanied by measures designed to mitigate the risks of the processing involved. The particularly strict conditions governing further processing make it doubtful that this provision will be widely applied, especially given the frequent circumvention of purpose-limitation requirements through vague and ambiguous descriptions of processing purposes.[565]

D. Rationale for the establishment of regulatory sandboxes

The reasons for creating regulatory sandboxes lie, as noted, in the friction that AI regulation can introduce for innovation.[566] This is because

[563] George Fletcher, "Fairness and Utility in Tort Theory," *Harvard Law Review* 85 (1972): 537, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?params=/context/faculty_scholarship/article/2036/&path_info=85_Harv._L._Rev._537.pdf

[564] Article 59 of Regulation 2024/1689.

[565] Katerina Yordanova and Natalie Bertels, "Regulating AI: Challenges and the Way Forward Through Regulatory Sandboxes," in *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, ed. Henrique Sousa Antunes et al. (Cham: Springer International Publishing, 2024), 452.

[566] Jonas Botta, "Art. 57," in *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, ed. Mario Martini and Christiane Wendehorst (Munich: C.H. Beck, 2024), para. 1; European Parliamentary Research Service (EPRS), *Artificial Intelligence Act and Regulatory Sandboxes* (Brussels: European Parliament, 2024), 3.

regulatory and legal barriers may limit the deployment of innovative solutions where the current regulatory framework does not support certain activities.[567] There is also a lack of openness to innovation, and an insufficient willingness to work with stakeholders to demonstrate the value and potential benefits of innovative solutions.[568] These issues are compounded by the immaturity of new technologies, and by limited capacity among suppliers to implement them at scale.[569] Lengthy and complex procedures for implementing innovative solutions further intensify these difficulties, potentially deterring developers from engaging in innovation activities.[570]

E. Regulatory sandboxes and EU innovation policy

In recent years, the regulatory sandbox approach has gained considerable momentum across the EU as a means of helping regulators address the development and use of emerging technologies in a wide range of sectors.[571] Sandboxes overseen by financial regulators are now widely used in financial technologies (fintech) to design new services, such as testing digital wallets and digital identity technologies.[572] Similarly, regulatory sandboxes have emerged as testing environments in transport, such as autonomous vehicles and drones; energy, such as smart meters; telecom-

[567] European Commission, Directorate-General for Energy, ETIP SNET, V. Efthymiou, N. Hartz, M. McGranaghan et al., *Regulatory Sandboxes – Policy Report Drafted by WG5's Regulatory Sandboxes Task Force* (Publications Office of the European Union, 2023), https://data.europa.eu/doi/10.2833/676429

[568] Ibid.

[569] Ibid.

[570] Ibid.

[571] European Parliamentary Research Service (EPRS), *Artificial Intelligence Act and Regulatory Sandboxes* (Brussels: European Parliament, 2024), 1.

[572] Deirdre Ahern, "Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon," *European Banking Institute (EBI) Working Paper Series* (September 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3928615; Wolf-Georg Ringe and Christopher Ruof, "Keeping Up with Innovation: Designing a European Sandbox for FinTech," *European Capital Markets Institute (ECMI) Commentary* no. 58 (January 2019), https://www.ecmi.eu/publications/commentaries/keeping-innovation-designing-european-sandbox-fintech

munications, such as 5G development; and health, such as services and innovations for early disease prevention.[573]

The inclusion of regulatory sandboxes in the AI Act forms part of the European Commission's broader action to foster innovation. As early as 2020, the Commission published its Communication "An SME Strategy for a Sustainable and Digital Europe", highlighting their importance.[574]

In recent years, the regulatory sandbox approach has gained significant momentum across the EU as a means of helping regulators address the development and use of emerging technologies across a wide range of sectors.[575] EU policymakers increasingly favour a more flexible approach to innovation and regulation in the high-tech sector. The EU promotes regulatory sandboxes to support start-ups in bringing innovative technologies to market, and to enable cross-border testing. The EU institutions have also formally committed to making EU legislative proposals more proactive and innovation-friendly, including through the use of regulatory sandboxes.[576] These trends are reflected in a series of Commission documents which, although not legally binding, are particularly useful for understanding the Commission's orientations and reasoning

[573] Organisation for Economic Co-operation and Development (OECD), *The Role of Sandboxes in Promoting Flexibility and Innovation in the Digital Age* (Paris: OECD, 2020), https://www.oecd.org/en/publications/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age_cdf5ed45-en.html; World Bank Group, *Global Experiences from Regulatory Sandboxes* (Washington, DC: World Bank, 2020).

[574] European Commission, *An SME Strategy for a Sustainable and Digital Europe*, COM(2020) 103 final (Brussels, 10 March 2020), 9; Anurag Atrey, Molly Lesher, and Chris Lomax, "The Role of Sandboxes in Promoting Flexibility and Innovation in the Digital Age," *Going Digital Toolkit Note* no. 2 (OECD, 2020), https://goingdigital.oecd.org/data/notes/No2_ToolkitNote_Sandboxes.pdf

[575] European Parliamentary Research Service (EPRS), *Artificial Intelligence Act and Regulatory Sandboxes* (Brussels: European Parliament, 2024), 1.

[576] Council of the European Union, *Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age* (2020). The 2023 *Better Regulation Toolbox* accordingly foresees the possibility to test innovations in real-world environments with safeguards and support.

when shaping these policies. Examples include the Commission's Better Regulation toolbox,.[577] and the New European Innovation Agenda.[578]

In addition to the AI Act, three EU regulations adopted in 2024 provide for regulatory sandboxes: the Interoperable Europe Regulation,[579] the Net-Zero Industry Act,[580] and the Cyber Resilience Act.[581] The proposed Regulation on the authorisation and supervision of medicinal products for human use is also under discussion.[582] Before these instruments, no other regulatory sandbox had been expressly introduced into EU legislation. Consequently, despite successful use in other jurisdictions, meaningful evaluation within the EU can only occur after a sufficient period has elapsed. This is especially true for the EU: given its complex institutional architecture and supranational character, the smooth operation of regulatory sandboxes is likely to encounter additional difficulties compared with national legal orders, whether of Member States or third countries.

---

[577] European Commission, "*Better Regulation* Toolbox — July 2023 Edition," https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en

[578] European Commission, *A New European Innovation Agenda*, COM(2022) 332 final (Brussels, 5 July 2022), 8.

[579] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 establishing measures for a high level of interoperability of the public sector across the Union (*Interoperable Europe Regulation*), Article 11.

[580] Regulation (EU) 2024/1735 of the European Parliament and of the Council of 13 June 2024 establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem and amending Regulation (EU) 2018/1724, Article 33.

[581] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (*Cyber Resilience Act*), Article 33(2).

[582] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Union Procedures for the Authorisation and Supervision of Medicinal Products for Human Use and Establishing Rules Governing the European Medicines Agency*, COM(2023) 193 final (Brussels, 26 April 2023), chap. IX.

F. Critical assessment

The effective implementation of the Regulation depends largely on the ability of competent authorities to exercise adequate supervision. The same applies to regulatory sandboxes. The existence of multiple authorities with concurrent competences over the activities taking place within the sandbox may create additional difficulties in coordinating the competent authorities and in exercising effective supervision, especially in view of their often limited resources. These difficulties become even more acute in the context of AI, where effective supervision requires a high level of technical expertise, which is often difficult to secure, especially given the very high demand for staff in the relevant technical fields. Therefore, the creation of a structure to coordinate the various authorities and, where appropriate, provide the necessary expertise is very likely to constitute a crucial factor for the effective supervision of sandboxes.[583]

Furthermore, although the Regulation provides for the operation of sandboxes across the EU under a uniform regulatory framework, it must be demonstrated in practice whether their operation in national legal orders will avoid regulatory fragmentation.[584] This risk in this respect is reinforced by the fact that, despite the provisions for a uniform regulatory framework, the competent national authorities enjoy a significant degree of flexibility, which may, over time, lead to notable variations in the operation of regulatory sandboxes.[585] The crucial role of the sandbox plan, which is drawn up ad hoc, may also leave room for differentiated practices. These may provide the necessary flexibility in relation to the specific circumstances of each legal order, but may also undermine the intended harmonisation of regulation in this field. At the same time,

[583] Nathan Genicot, "From Blueprint to Reality: Implementing AI Regulatory Sandboxes under the AI Act," *FARI & LSTS Research Group* (VUB, 2024), 35.

[584] Sofia Ranchordas and Valeria Vinci, "Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture," *Italian Journal of Public Law* 16 (2024): 107, 132, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4696442

[585] AI Act, art. 58(2)(c); Thomas Buocz et al., "Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?," *Law, Innovation and Technology* 15 (2023): 357, 379, https://ucrisportal.univie.ac.at/en/publications/regulatory-sandboxes-in-the-ai-act-reconciling-innovation-and-saf

the inclusiveness of regulatory sandboxes remains doubtful.[586] Despite the existence of some favourable provisions for the participation of start-ups and SMEs, the lack of sufficient resources may prevent these companies from complying effectively or from engaging with the competent authorities on an equal footing. As a result, these companies may have less scope for experimentation compared with larger companies, which may restrict their participation. At the same time, the lack of civil society participation may create mistrust towards regulatory sandboxes.

In addition, the close interaction between the competent authorities and the participants in the sandbox raises concerns about the possibility that participants may acquire excessive influence over the competent authorities (regulatory capture).[587] Although such a possibility is less likely in the case of start-ups and SMEs, the participation of larger companies with significant expertise, infrastructure, and human resources renders such a risk considerable. Avoiding this risk can only be achieved by ensuring adequate transparency, together with the possibility for third parties to exercise effective oversight.[588]

In short, regulatory sandboxes are associated with both advantages and disadvantages.[589]

Their advantages may be categorised as follows:

First, they help regulators to acquire a better understanding of innovative products, which enables them to develop appropriate policies for rule-making, supervision, and enforcement.

---

[586] Sofia Ranchordas and Valeria Vinci, "Regulatory Sandboxes and Innovation-Friendly Regulation," *Italian Journal of Public Law* 16 (2024): 134; Harry Armstrong, Chris Gorst, and Jen Rae, *Renewing Regulation: "Anticipatory Regulation" in an Age of Disruption* (London: NESTA, 2019), https://media.nesta.org.uk/documents/Renewing_regulation_v3.pdf

[587] Sofia Ranchordas and Valeria Vinci, "Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture," *Italian Journal of Public Law* 16 (2024): 107, 132, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4696442

[588] Ibid, 137.

[589] *Regulatory Sandboxes and Innovation Hubs for FinTech*. Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, September 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf

Second, innovation businesses can develop their products and services in a way that complies with the law, thereby avoiding potential legal risks. Regulatory sandboxes also help them to better understand the expectations of supervisory authorities. Moreover, testing in a controlled environment also mitigates risks and unintended consequences (such as hidden security gaps) during the introduction of a new technology to the market, which may potentially shorten the market cycle of new products. Supervisory authorities can provide guidance to technology developers on how specific rules should be applied to new products. From the innovators' perspective, one of the main benefits is the ability to test new technologies without having to meet all the regulatory requirements normally applicable in a given sector, which is particularly useful for addressing innovations that do not fit easily into an existing framework.

Third, consumers benefit from the introduction of new and potentially safer products, since regulatory sandboxes promote innovation and consumer choice in the long term.

Even so, it should not be overlooked that regulatory sandboxes also entail the risk of abuse or misuse.

The drawbacks are not negligible.[590]

First, regulatory sandboxes may be misused, with regulators reducing protective measures and requirements in order to attract innovators.

Second, there may be negative effects on consumer protection arising from this "race to the bottom" in the financial technology sector.[591]

Third, regulators may prioritise innovation over the adoption of adequate public and consumer protection measures, especially if the participation of innovators grants them excessive influence in shaping regulatory practices.

Fourth, private entities processing personal data are permitted to derogate from the applicable data protection rules when testing their AI systems.[592]

---

[590] Ibid.

[591] Hillary J. Allen, "Sandbox Boundaries," *Vanderbilt Journal of Entertainment & Technology Law* 22, no. 2 (October 2020), https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1017&context=jetlaw

[592] Sofia Ranchordas, "Experimental Lawmaking in the EU: Regulatory Sandboxes," *EU Law Live*, Weekend Edition, 22 October 2021, University of Groningen Faculty of Law

Fifth, there is concern that the choices of regulators may hinder, or even slow down, genuine innovation on the part of private actors.

Sixth, there is a risk of fragmentation of the EU single market if the testing parameters in a regulatory sandbox differ significantly between Member States.

Seventh, the establishment of regulatory sandboxes may create a false sense of security and compliance in the market. An AI system that meets regulatory requirements during testing may still pose liability risks or evolve into a high-risk AI through unforeseen applications. Approval by the regulatory sandbox must not be regarded as a guarantee of safety or absence of liability risks.[593]

G. Concluding remarks

The GDPR is guided by the need to protect research. In this direction, the AI Act seeks to respond to the pressing need for innovation by providing controlled environments for experimentation and innovation. Practice so far has shown that regulatory sandboxes are the answer to the difficulty of over-regulation. It is up to the supervisory authorities to rise to the occasion and promote a framework of supervised research that will foster innovation.

Research Paper No. 12/2021 (October 22, 2021). Available at SSRN: https://ssrn.com/abstract=3963810

[593] Sena Lezgioglu Ozer, "Regulatory Sandboxes in the AI Act: Between Innovation and Safety," *DigiCon* (2024), https://digi-con.org/regulatory-sandboxes-in-the-ai-act-between-innovation-and-safety

VII. Is it necessary for the Greek revising constitutional legislator to regulate artificial intelligence?

The question arises as to whether the Greek revising constitutional legislator is required to protect citizens from the consequences of AI. Should the provisions of the AI Act also be enshrined at the domestic constitutional level? The two principal positions are the following:

First, the wording in the Greek Constitution should be simple and timeless. Therefore, in a constitutional revision, the task of the revisionist legislator is to refrain from case-by-case references and to give the Constitution a simple, concise, precise, and clear character. Moreover, the regulatory scope of AI exceeds the capacity of the national constitutional legislator.[594] This position gives the Constitution a timeless quality. Yet it could be argued that the existing Constitution is already case-specific, as it refers to outdated instruments, such as phonography, in Article 15(1).[595] Therefore, either the Constitution must be modernised by replacing outdated provisions with more contemporary ones, or it must be redrafted in a general and timeless manner.

Second, the explicit inclusion of new rights in the constitutional text is very important for the "regulatory effectiveness of the Constitution".[596] Consequently, constitutionalisation is both symbolic and practical, as it strengthens their defensive force against legislative or ju-

[594] Xenophon Contiades, *What Should Change in the Constitution: Forty Questions and Answers for the New Constitutional Revision* (Athens: e-Politeia, 2024), 240, https://www.epoliteia.gr/e-books/2025/01/23/ti-prepei-na-allaksei-sto-syntagma

[595] Spyros Vlachopoulos, "Constitutional Revision in the Age of Artificial Intelligence," *Syntagma Watch*, 1 October 2024, https://www.syntagmawatch.gr/trending-issues/h-syntagmatikh-anatheorhsh-sthn-epoxh-ths-texniths-nohmosynhs/

[596] Xenophon Contiades, *What Should Change in the Constitution: Forty Questions and Answers for the New Constitutional Revision* (Athens: e-Politeia, 2024), 239, https://www.epoliteia.gr/e-books/2025/01/23/ti-prepei-na-allaksei-sto-syntagma

risprudential regressions.[597] Following this view, it is proposed that the Constitution explicitly provide for protection against the applications of AI, in order to clarify the reception of the relevant legislative initiative and strengthen the role of the judiciary within the framework of digital constitutionalism.[598] To this end, it would seem appropriate to safeguard at constitutional level the ethical use of AI and its supervision by an independent authority. For this reason, it is proposed to add a supplementary Article 5B, which would enshrine that AI contributes to the protection of human rights, democracy, and the rule of law.[599] The same Article could also set out the fundamental principles that should govern the functioning of AI, such as those of transparency, accountability and accessibility, fairness and integrity, human responsibility, and protection of privacy.[600] This position carries the advantage of modernising the Constitution. Furthermore, it must not escape our attention that AI is not just an application but constitutes the fourth industrial revolution. This fourth industrial revolution, if it is to be of benefit to humanity, should be regulated at the constitutional level. Such regulation should encompass both the control of technology and the protection of humans from its impact. An objection to this position could be that these principles that should guide AI are already enshrined in the Constitution and repeating them would make it verbose.

In light of the above considerations, the proposed solutions are as follows:

(a) No provision for AI at the constitutional level, as it is placed under the umbrella of existing provisions.

(b) Revision of existing case-specific and outdated provisions in a general and timeless manner.

(c) A general provision for the protection of the individual from the effects of AI.(d) A general provision enshrining welfare at con-

[597] Ibid, 240.
[598] Ibid.
[599] Evripidis Stylianidis, "A Proposal on Artificial Intelligence in View of the Revision of the Greek Constitution," in *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, ed. Evripidis Stylianidis (Athens: Nomiki Vivliothiki, 2025), 633 ff. (634).
[600] Ibid.

> stitutional level. In this context, AI policymakers stress that AI should promote individual well-being and not human marginalisation, degradation, or decline. This means that AI should be recognised as a tool that supports and inspires people to improve their quality of life by making use of their unique human capabilities, in the workplace, in education, in personal relationships, in the aesthetic realm, and in interaction with the state.

All four options are equally valid. Under the present circumstances, a bold[601] revision of the Constitution is proposed by replacing outdated provisions and generally enshrining new provisions on the impact of technology, especially AI, on humans. The revisionist legislator would be well advised to refrain from a detailed statement of principles regarding AI, as these are dynamic and it suffices to enshrine them at national level. The fundamental principles of human protection are already constitutionally enshrined and also cover AI. Finally, it would be useful to enshrine the principle of well-being primarily as a goal of AI.[602]

[601] Spyros Vlachopoulos, "Constitutional Revision in the Age of Artificial Intelligence," *Syntagma Watch*, 1 October 2024, https://www.syntagmawatch.gr/trending-issues/h-syntagmatikh-anatheorhsh-sthn-epoxh-ths-texniths-nohmosynhs

[602] Fereniki Panagopoulou, "Constitution and Happiness: Can the Constitution Guarantee Happiness?," *HuffPost Greece*, 7 July 2025, https://www.huffingtonpost.gr/entry/sentayma-kai-eetechia_gr_684fe2dae4b07f75743a89df

CONCLUSIONS

The issues that arise from AI are numerous and difficult to resolve. The landscape appears for some as a nightmare, and for others as a blessing. Our position lies somewhere in the middle. The advantages of using AI are many, provided we can avert the risks: this can be achieved through careful regulation based on the constitutional principle of proportionality. Systematic regulation within the EU is a first step, yet it is not sufficient, since lax regulation persists in the US and China. Caution and deliberation are required regarding indiscriminate resort to AI tools, especially when such resort leads to critical decisions affecting individuals and humanity as a whole.[603]

Regulation through the AI Act is directly linked to constitutionally protected goods such as national security, democracy, labour, research, health, education, the environment, and so on.

The concluding thoughts of the present study can be summarised as follows:

1. It is promising that the EU, after intense consultations, concluded a final regulatory text on AI. It is also promising that the U.S. and China are not leaving the issue unregulated.

2. Before examining the AI Act, it must be verified that it applies – which means that we need to determine that we are, indeed, dealing with AI. There is confusion between an algorithm and AI: AI presupposes autonomy, imitation, learning, adaptability, and inference; an algorithm, on the other hand, consists of a sequence of actions. If the problem can be solved efficiently in a fully understood way using algorithms based on linear computation, AI is not necessary[604] and the Act does not apply. Using AI where it is not required may introduce unnecessary complexity, increase

[603] Prokopios Pavlopoulos, "Critical Reflections on the Relevance of Aristotle's Positions on Law and Justice in the Age of Artificial Intelligence," *Public Law Review* 1 (2025): 41 ff. (53).

[604] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 145, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

costs and energy consumption, and potentially lead to incomplete or inadequate outcomes.[605]

3. The attempt to broaden the territorial scope of the AI Act's application sometimes reflects a utopian view of exercising sovereignty over another state without negotiation and without war. It did not seem to succeed with the GDPR, and it is not expected to fare better with AI.

4. The quasi-Directive Regulation model, meaning a Regulation with many Directive-like features via flexibility clauses to Member States, as in the GDPR, opens the door to divergences within the EU regarding protection against the effects of AI on humans. A typical example is the discretion left to Member States concerning supervisory authorities. This raises concern about supervisory authorities operating at different speeds.

5. Biometric monitoring for reasons of national security must not be extended to reasons of public order, mere facilitation of police work, or other administrative authorities. Strict legislation is required so that the exception permitting biometric surveillance does not become a "back door" to rights violations. We should not give in to the slippery slope.[606]

6. The labour sector highlights the need to constitutionalise the principle of well-being. In this direction, AI should not be viewed as a means of replacing human labour solely to reduce costs. It should be treated as a means to enhance quality of life, such as, for example, by reducing working hours and increasing leisure time. Furthermore, AI should not be perceived as a means of permanently linking the individual to technology and work; the right to disconnect should be recognised.

[605] Ibid.

[606] Evan Selinger and Brenda Leong, "Facial Recognition Technology Primer: What Is It and How Is It Used?," in *The Oxford Handbook of Digital Ethics*, ed. Carissa Véliz (Oxford: Oxford University Press, 2021), 590 ff. (598).

7. Democracy is directly affected by AI both positively (democratic upgrading) and negatively (digital authoritarianism). Mechanisms are needed to prevent disinformation, manipulation, and the imposition of a "dictatorship of the average". Democratic upgrading must not alter the qualitative features of representative government. This implies that citizen assemblies via AI applications using randomised participation should aim at consultation, not the diffusion of political responsibility.

8. AI signals the recognition of a right to digital education, derived from Article 16(2) in conjunction with Article 5A of the Constitution. This is because digitising the state without corresponding education would lead to a digital divide. This education must include both education in AI and education about AI, the latter familiarising learners with the new ethical, social, and legal issues raised by AI.

9. From the right to health, together with the right to free development of personality and the right to information, there follows a right to know the prognosis of one's health status, and a right not to know if one does not wish to be informed. This means that information should not be compulsory, otherwise it would deprive us of our right to an open future. From the right to the protection of personal data there follows a right to informational self-determination, meaning we must control who has access to our data. Therefore, unauthorised access to predictive data by insurance companies conflicts with the right to informational self-determination.

10. The response to the legitimate fear that over-regulation would hinder innovation came via the provision for regulatory sandboxes in Article 55 of the AI Act. This provision fosters innovation by offsetting the risks posed by over-regulation. It seeks to balance responsibility for innovation and the openness or potential of AI with the risks it entails. The aim is to promote innovation in AI by creating a controlled environment for experimenting with and testing innovative AI technologies, products, and services during development.

11. The AI Act, modelled on the GDPR, is largely animated by the need to facilitate research. For this reason, it provides for AI research under the guise of innovation-promoting regulatory sandboxes. The English term "sandboxes", meaning boxes of sand in which we can trial-build whatever we wish, is apt.

12. AI relies on data. Acquiring high-quality and relevant data is of paramount importance[607], otherwise, the entire project fails. Beyond ensuring quality and relevance, it is essential to establish procedures for data access and to prevent unauthorised access.[608]

13. The distaste for AI is also largely rooted in algorithmic prejudices. Discomfort with AI is rooted to a large extent in algorithmic biases. Such biases stem from omissions[609] by designers and thinkers of technologies.[610] Our sometimes distorted images of people, cultures, and things may impart bias to outcomes.[611] We cannot be certain that what we observe is in fact reality.[612] We must conduct a calm public dialogue to envision our common future with the algorithm.[613] We should not overlook that algorithms may carry biases, as they are built on our knowledge of the world, which is inherently limited and may itself contain bias.[614] Understanding the origins of biases in social behaviours implies understanding part of the mechanisms of algorithmic bias.[615] We must understand that

[607] Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence* (Athens: Government Foresight Centre, 2024), 146, https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

[608] Ibid, 147.

[609] Iliana Kosti, "Can the Algorithm Be Fair?," in *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, ed. Lilian Mitrou (Heraklion: University of Crete University Press, 2023), 97 ff. (97).

[610] Aurélie Jean, *On the Other Side of the Machine: A Journey into the Land of Algorithms*, trans. Giorgos Bolierakis (Athens: Stereōma, 2023), 25.

[611] Ibid., 96.

[612] Ibid., 108.

[613] Ibid., 25.

[614] Ibid., 97.

[615] Ibid., 100.

the algorithm is not responsible for racism, sexism, or favouritism; it does what we have programmed it to do.[616]

14. The main goal of all those developing AI applications should be environmental sustainability. Since creating AI requires substantial energy, the problem can be addressed through AI itself, such as by designing applications that save energy.

15. AI must rest on a web of ethical principles from which a technoethic of responsibility is woven. In this sense, AI should be used to highlight human virtues; therefore, the human being is both the means and the guide to its good use.[617]

16. We should replace "AI" with "IA", namely Artificial Intelligence with Intelligence Augmentation, signifying a shift in which new technology is used to enhance human capabilities rather than replace them.[618]

Whenever something new is incorporated into social practice, it is not in itself beneficial or just;[619] we must clarify its governance framework in a way that serves human dignity and well-being. This is the framework that the AI Act seeks to provide. The flexibility clauses granted to the domestic legislator should serve to enhance the protection of the individual while enabling the realisation of AI's anticipated benefits. The AI highway does not appear to have a speed limit. To reach our destination safely,

[616] Ibid., 127.

[617] Konstantinos Kornarakis, "Artificial Intelligence and the Contemporary Human" *diaLOGOS* 14 (2024): 204 ff. (221). Also, Alkis Gounaris, George Kosteletos, and Maria-Artemis Kolliniati, "Virtue in the Machine: Beyond a One-size-fits-all Approach and Aristotelian Ethics for Artificial Intelligence," *Conatus – Journal of Philosophy* 10, no. 1 (2025): 127–152, https://doi.org/10.12681/cjp.40628

[618] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility," *Philosophies* 1, no. 2 (2021): 8, https://www.mdpi.com/2673-2688/1/2/8

[619] Stavroula Tsinorema, "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility," in *Liber Amicorum Ismini Kriari* (Athens: Sideris, 2025), 259 ff. (280).

we require reliable brakes, effective steering, and modern mechanisms for accident prevention. This is precisely the role of Technoethics.[620]

[620] Metropolitan of Mesogaia and Lavreotiki Nikolaos, "Bioethical Approaches to the Impact of Artificial Intelligence on Human Life," *Estia*, October 11, 2025.

BIBLIOGRAPHY

Ahern, Deirdre. "Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon." *EBI Working Paper Series*, September 2021.

Alexandropoulou-Aigyptiadou, Eugenia, Theoharis Dalakouras, and Christos Mastrokostas, eds. *Exploring Aspects of Artificial Intelligence: Cutting-Edge Technologies as a Legislative Challenge (2nd Interdisciplinary Conference on Law and Informatics)*. Athens: Nomiki Vivliothiki, 2025.

Alexandropoulou-Aigyptiadou, Eugenia. *Personal Data*. Athens: Nomiki Vivliothiki, 2016.

Alivizatos, Nikos. *The Constitutional Position of the Armed Forces*. Athens: Sakkoulas, 1987.

Aloisi, Antonio. "Algorithmic Management." In *Artificial Intelligence and Labour Law*, edited by Matina Giannakourou and Christina Deliyianni-Dimitrakou, 621 ff. 2023.

Alpaydin, Ethem. *Introduction to Machine Learning*. Cambridge, MA: MIT Press, 2020.

Amnesty International. *EU: Lawmakers Reluctant to Stop EU Companies Profiting from Surveillance and Abuse through the AI Act*. December 5, 2023. https://www.amnesty.org/en/latest/news/2023/12/eu-lawmakers-reluctant-to-stop-eu-companies-profiting-from-surveillance-and-abuse-through-the-ai-act/

Anderson, Michael, Susan Leigh Anderson, Alkis Gounaris, and George Kosteletos. "Towards Moral Machines: A Discussion with Michael Anderson and Susan Leigh Anderson." *Conatus – Journal of Philosophy* 6, no. 1 (2021): 177–202. https://doi.org/10.12681/cjp.26832.

Avgerinou, Andriani, Fotis Gogoulos, Achilleas Kleisouras, Evangelos D. Protopapadakis, Dimitris Tsamis, and Giota Charalampaki. "Philosophy, Education, and Augmented Reality through the Digital Platform 'Traces of Philosophy: Connect, Reflect, Experience.'" *Paidagogikos Logos* 30, no. 1 (2024): 11 ff. https://doi.org/10.12681/plogos.39663

Andriotakis, Manolis. *Artificial Intelligence for All*. Athens: Psychogios, 2022.

Androulidaki-Dimitriadis, Ismini. *The Patient's Right to Information: Contribution to the Establishment of Civil Medical Liability*. Athens–Komotini: Ant. N. Sakkoulas, 1993.

Aravanis, Theodoros. "Articles 21 §3 and 109 of the Constitution: Observations on Council of State Decision 400/86 (Plenary)." *ToS* (1987): 480 ff.

Armstrong, Harry, Chris Gorst, and Jen Rae. *Renewing Regulation: "Anticipatory Regulation" in an Age of Disruption*. London: NESTA, 2019.

Avrantinis, Anastasios. "Artificial Intelligence: Towards a 'Digital Pnyx'." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 607 ff. Athens: Nomiki Vivliothiki, 2025.

Balicer, Ran. "The Doctor Will See Your Future Now." *Forbes*, April 16, 2018. https://www.forbes.com/sites/startupnationcentral/2018/04/16/for-predictive-medicine-its-back-to-the-future/

Balkin, Jack M. "The Three Laws of Robotics in the Age of Big Data." *Ohio State Law Journal* 78 (2017): 1217–1247.

Barfield, Woodrow, and Ugo Pagallo, eds. *Research Handbook on the Law of Artificial Intelligence*. Cheltenham, UK: Edward Elgar, 2018.

Baros, Vasileios, and Louis Henri Seukwa. "Article 2, Protection of Human Dignity." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 27 ff. Athens: Nomiki Vivliothiki, 2025.

Bhattacharya, Ananya. "Political Campaigns Embrace AI to Reach Voters across Language Barriers." *Rest of World*, September 19, 2024. https://restofworld.org/2024/aapi-victory-alliance-ai-voter-outreach

Biggar, Nigel. "An Ethic of Military Uses of Artificial Intelligence: Sustaining Virtue, Granting Autonomy, and Calibrating Risk." *Conatus – Journal of Philosophy* 8, no. 2 (2023): 67–76. https://doi.org/10.12681/cjp.34666.

Bletsas, Michalis. "The big problem is not bots but the toxic impact of social media." Quoted at Hellenic Cybersecurity Authority. https://cyber.gov.gr/athens-voice-michalis-mpletsas-to-megalo-provlima-den-einai-ta-bots-alla-i-toxiki-epidrasi-ton-social-media/

Bostrom, Nick. *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press, 2014.

Botta, Jonas. "Art. 57." In *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, edited by Mario Martini and Christiane Wendehorst. Munich: C.H. Beck, 2024.

Bouveret, Sylvain, and Michel Lemaître. "Computing Leximin-Optimal Solutions in Constraint Networks." *Artificial Intelligence* 173 (2009): 343–364. https://doi.org/10.1016/j.artint.2008.10.010

Bradford, Anu. "The False Choice Between Digital Regulation and Innovation." *Northwestern University Law Review* 119, no. 2 (2024): 377. https://scholarlycommons.law.northwestern.edu/nulr/vol119/iss2/3/

Brynjolfsson, Erik, and Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. Translated by Giorgos Nathanael. Athens: Kritiki, 2016.

Buocz, Thomas, et al. "Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?" *Law, Innovation and Technology* 15 (2023): 357–379.

Christodoulou, Konstantinos N. "Legal Issues Arising from Artificial Intelligence." In *Law and Technology: 22nd Scientific Symposium of the University of Piraeus and the Hellenic Court of Audit, 28–29 March 2019*, edited by Kornilia Delouka-Igglesi, Anna Ligomenou, and Aristea Sinanioti-Maroudi, 117 ff. Athens–Thessaloniki: Sakkoulas, 2019.

Christodoulou, Konstantinos. "Presentation at the European Laboratory of Bioethics, Technoethics and Law Webinar on Artificial Intelligence." YouTube, May 16, 2022. https://www.youtube.com/watch?v=4W3npEt_WDA

Christou, Sofia. "Christos Papadimitriou in Kathimerini: 'Archimedes Is in Danger.'" *Kathimerini*, July 10, 2025. https://www.kathimerini.gr/opinion/interviews/563640649/christos-papadimitrioy-stin-k-o-archimidis-vriskete ai-se-kindyno/

Christou, Vasiliki. "Towards a Digital Municipality?" In *Rule of Law and Democracy in the Digital Age*, edited by Giorgos Karavokyris, 19 ff. Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024.

Chrysogonos, Kostas Ch., and Spyros V. Vlachopoulos. *Individual and Social Rights*. Athens: Nomiki Vivliothiki, 2017.

CNIL. "CNIL Creates Artificial Intelligence Department and Begins Work on Learning Databases." https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases

Contiades, Xenophon. "Experimental Lawmaking in the EU: Regulatory Sandboxes." *EU Law Live, Weekend Edition*, October 22, 2021. SSRN: https://ssrn.com/abstract=3963810

Contiades, Xenophon. *What Should Change in the Constitution: Forty Questions and Answers for the New Constitutional Revision*. Athens: e-Politeia, 2024. https://www.epoliteia.gr/e-books/2025/01/23/ti-prepei-na-allaksei-sto-syntagma

Council of Europe. *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications*. March 2018. https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

Council of the European Union. "Artificial Intelligence Act: Council Gives Final Green Light to the First Worldwide Rules on AI." Press release, May 21, 2024. https://www.consilium.europa.eu/el/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

Csernatoni, Raluca. "Can Democracy Survive the Disruptive Power of AI?" *Carnegie Endowment for International Peace*, December 18, 2024. https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en

Cuthbertson, Anthony. "Artificial Intelligence 'Boy' Shibuya Mirai Becomes World's First AI Bot to Be Granted Residency." *Newsweek*, November 6, 2017.

Dagtoglou, Prodromos D. *Constitutional Law, Individual Rights*. Athens–Thessaloniki: Sakkoulas, 2022.

Danaher, John. "The Threat of Algocracy: Reality, Resistance and Accommodation." *Philosophy & Technology* 29 (2016): 245–268. https://doi.org/10.1007/s13347-015-0211-1.

Dausy, Tom. "Data, the New Gold: How AI Is Unlocking Insights and Driving Business Growth." *Medium*, May 19, 2024. https://medium.com/@tomdausy/data-the-new-gold-how-ai-is-unlocking-insights-and-driving-business-growth-c458b5676f08

David Harris, Michael O'Boyle, Ed Bates, and Carla M. Buckley. *Law of the European Convention on Human Rights*. 4th ed. Oxford: Oxford University Press, 2018.

Delaney, Kevin J. "The Robot That Takes Your Job Should Pay Taxes, Says Bill Gates." *Quartz*, February 17, 2017.

Di Fabio, Udo. "Article 2 para. I." In T. Maunz, G. Dürig, R. Herzog, and R. Scholz, eds., *Kommentar zum Grundgesetz*, 48th update, Art. 2 para. I, marginal no. 204. Munich: C.H. Beck, 2006.

Digital Policy Alert. "Order on Data Protection Authority's Supervisory Role over AI Algorithms." https://digitalpolicyalert.org/change/4226-order-on-data-protection-authoritys-supervisory-role-over-ai-algorithms

Dilmegani, Cem. *Responsible AI: 4 Principles & Best Practices in 2024*. AI Multiple Research, 2024. https://research.aimultiple.com/responsible-ai/

Dosa, David. "A Day in the Life of Oscar the Cat." *New England Journal of Medicine* 357 (2007): 328–29. https://www.nejm.org/doi/abs/10.1056/NEJMp078108

Dosa, David. *Making Rounds with Oscar: The Extraordinary Gift of an Ordinary Cat*. New York: Hyperion, 2010.

Draghi, Mario. *The Future of European Competitiveness*. European Commission, 2024. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

EDPS (European Data Protection Supervisor). *Artificial Intelligence, Robotics, Privacy and Data Protection*. Room Document, 38th International Conference of Data Protection and Privacy Commissioners, October 2016. https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

Efstratiou, Efstratios. *National Security as an Exception Clause in the Greek Constitution and the Treaties of the European Union*. PhD diss., Aristotle University of Thessaloniki, Faculty of Law, 2024 (unpublished).

Eisenberger, Iris. "Art. 17." In *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, edited by Mario Martini and Christiane Wendehorst. Munich: C.H. Beck, 2024.

El Fassi, Sammy Chouffani, et al. "Not All AI Health Tools with Regulatory Authorization Are Clinically Validated." *Nature Medicine* 30 (2024): 2718–2720. https://doi.org/10.1038/s41591-024-03203-3

Elton, Jeff, and Arda Ural. "Predictive Medicine Depends on Analytics." *Harvard Business Review*, 23 October 2014. https://hbr.org/2014/10/predictive-medicine-depends-on-analytics

ENA Institute for Alternative Policies. *Citizen Assemblies and Democratic Renewal*. Athens: ENA, May 2022.

Erfort, Cornelius. "Targeting Voters Online: How Parties' Campaigns Differ." *Electoral Studies* 92 (December 2024). https://www.sciencedirect.com/science/article/pii/S0261379424001306

European Commission. "Artificial Intelligence Act: Council and Parliament Reach Agreement." Press release, February 2024. https://ec.europa.eu/commission/presscorner/detail/el/ip_24_383

European Commission. "Over a Hundred Companies Sign EU AI Pact with Pledges to Drive Trustworthy and Safe Ai Development." https://digital-strategy.ec.europa.eu/en/news/over-hundred-companies-sign-eu-ai-pact-pledges-drive-trustworthy-and-safe-ai-development

European Commission. *Artificial Intelligence for Europe*. Communication, COM(2018) 237 final. Brussels, April 25, 2018. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018DC0237

European Commission. *Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators*. Luxembourg: Publications Office of the European Union, 2022.

European Commission: Directorate-General for Energy (ETIP SNET WG5). *Regulatory Sandboxes – Policy Report*. Publications Office of the European Union, 2023. https://data.europa.eu/doi/10.2833/676429

European Commission. *Digital Omnibus – AI Regulation Proposal*. 19 November 2025. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

European Parliamentary Research Service (EPRS). *Artificial Intelligence Act and Regulatory Sandboxes*. Brussels: European Parliament, 2024.

Evripidis Stylianidis, ed. *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. Athens: Nomiki Vivliothiki, 2025.

Ferretti, Agata, Manuel Schneider, and Alessandro Blasimme. "Machine Learning in Medicine: Opening the New Data Protection Black Box." *European Data Protection Law Review* 3 (2018): 320 ff.

Financial Conduct Authority. *Regulatory Sandbox: Lessons Learned*. 2017. https://www.fca.org.uk/publications/research/regulatory-sandbox-lessons-learned-report

Fitria, Tira Nur. "Artificial Intelligence (AI) in Education: Using AI Tools for Teaching and Learning Process." ResearchGate, 20 December 2021, 134 ff. http

s://www.researchgate.net/profile/Tira-Nur-Fitria/publication/357447234_Artificial_Intelligence_AI_In_Education_Using_AI_Tools_for_Teaching_and_Learning_Process/links/61ce7029e669eeof5c76b2ba/Artificial-Intelligence-AI-In-Education-Using-AI-Tools-for-Teaching-and-Learning-Process.pdf

Fletcher, George. "Fairness and Utility in Tort Theory." *Harvard Law Review* 85 (1972): 537.

Floridi, Luciano. *The Ethics of AI*. Oxford: Oxford University Press, 2023.

Garvie, Clare. *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*. Washington, DC: Center on Privacy & Technology at Georgetown Law, 2022. https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf

Gatzoufas, Anastasios G. "Everyday Life in the Age of Artificial Intelligence." *dia-LOGOS* 14 (2024): 293 ff.

Genicot, Nathan. "From Blueprint to Reality: Implementing AI Regulatory Sandboxes under the AI Act." Brussels: FARI & LSTS (VUB), 2024.

Gershgorn, Dave. "Inside the Mechanical Brain of the World's First Robot Citizen." *Quartz*, November 12, 2017.

Giannakopoulos, Giorgos. *Artificial Intelligence: A Discreet Demystification*. Athens: Ropi, 2020.

Giannakourou, Matina. "The Regulation of Algorithmic Labour Administration in the Draft Legislative Initiatives of the EU: Quo vadis, Europa?" In *Artificial Intelligence and Labour Law*, edited by Matina Giannakourou and Christina Deliyianni-Dimitrakou, 645 ff. 2023.

Giannopoulos, Georgios. "Presentation at the European Laboratory of Bioethics, Technoethics and Law Webinar on Artificial Intelligence." May 16, 2022. https://bioethics.panteion.gr

Giannopoulos, Georgios. *Introduction to Legal Informatics*. Athens: Nomiki Vivliothiki, 2018.

Gillespie, Tarleton. "The Politics of Platforms." *New Media & Society* 12, no. 3 (2010): 347–364.

Goodman, Rachel. "Why Amazon's Automated Hiring Tool Discriminated Against Women." ACLU, October 12, 2018. https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-againstGoogle.

"Google Translate Adds New Languages." *Google Blog*, 2024. https://blog.google/products/translate/google-translate-new-languages-2024

Gounaris, Alkis, George Kosteletos, and Maria-Artemis Kolliniati. "Virtue in the Machine: Beyond a One-size-fits-all Approach and Aristotelian Ethics for Artificial Intelligence." *Conatus – Journal of Philosophy* 10, no. 1 (2025): 127–152, https://doi.org/10.12681/cjp.40628.

Government Foresight Centre, *Plan for Greece's Transition to the Age of Artificial Intelligence*. Athens: Government Foresight Centre, 2024. https://foresight.gov.gr/wp-content/uploads/2024/11/Sxedio_gia_tin_metavasi_TN_Gr.pdf

Habermas, Jürgen. *Faktizität und Geltung: Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Frankfurt: Suhrkamp, 1992.

Hall, Joshua M. "Just War contra Drone Warfare." *Conatus – Journal of Philosophy* 8, no. 2 (2023): 217–239. https://doi.org/10.12681/cjp.34306.

Harari, Yuval Noah. *21 Lessons for the 21st Century*. Athens: Alexandria, 2018.

Harris, David, Michael O'Boyle, Ed Bates, and Carla M. Buckley. *Law of the European Convention on Human Rights*. 4th ed. Oxford: Oxford University Press, 2018.

Holmes, Kat. *Mismatch: How Inclusion Shapes Design*. Cambridge, MA: MIT Press, 2018.

Howard, Jeffrey W. "Extreme Speech, Democratic Deliberation, and Social Media." In *The Oxford Handbook of Digital Ethics*, edited by Carissa Véliz, 181 ff. Oxford: Oxford University Press, 2021.

Hubbard, Sarah. *The Role of AI in the 2024 Elections*. Cambridge, MA: Ash Center, Harvard Kennedy School, December 5, 2024. https://ash.harvard.edu/resources/the-role-of-ai-in-the-2024-elections

ICO (Information Commissioner's Office). *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Wilmslow: ICO, 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Iliadou, Aikaterini N. "Contemporary Issues in the Interpretation of the Right to Participate in the Information Society (Article 5A(2) of the Constitution)." *e-politeia* 13 (2025): 81 ff. https://www.epoliteia.gr/wp-content/uploads/2025/01/MELETES-2.13.pdf

Iliadou, Aikaterini N., Fereniki Panagopoulou, and Konstantinos Stratilatis. "Interpretation of Article 5A of the Constitution." In *Article-by-Article Commentary on the Constitution*, edited by Evangelos Venizelos; Spyros Vlachopoulos, Xenophon Contiades, and Giannis Tasopoulos. Athens–Thessaloniki: Sakkoulas; Syntagma Watch, 2025.

Implement Consulting Group. "The Economic Opportunity of Generative AI in Greece." https://implementconsultinggroup.com/article/the-economic-opportunity-of-generative-ai-in-greece

Inglezakis, Ioannis. *Law of the Digital Economy*. 2nd ed. Athens–Thessaloniki: Sakkoulas, 2024.

Jean, Aurélie. *On the Other Side of the Machine: A Journey into the Land of Algorithms*. Translated by Giorgos Bolierakis. Athens: Stereōma, 2023.

Kalokairinou, Eleni. "Towards an Ethics of Artificial Intelligence." *dia-LOGOS* 14 (2024): 193 ff.

Kanellos, Leonidas. *Applications of Artificial Intelligence in Law and Judicial Practice*. Athens: Nomiki Vivliothiki, 2021.

Karavokyris, Giorgos. "The Face of Democracy." *Constitutionalism*, August 16, 2022.

Karnow, Curtis E. A. "Introduction to Law and Artificial." In *Research Handbook on the Law of Artificial Intelligence*, edited by Woodrow Barfield and Ugo Pagallo, xix–xxx. Cheltenham, UK: Edward Elgar, 2018.

Karpouzis, Konstantinos. "From Plato's Forms to AI Norms: A Guide to Contemporary Technology through Ancient Greek Philosophy." *dia-LOGOS* 14 (2014): 275 ff.

Khatri, Mousam. "Data Privacy in the Age of Artificial Intelligence (AI)." LinkedIn Pulse, 2023. https://www.linkedin.com/pulse/data-privacy-age-artificial-intelligence-ai-mousam-khatri/

Koppernock, Martin. *Das Grundrecht auf bioethische Selbstbestimmung: Zur Rekonstruktion des allgemeinen Persönlichkeitsrechts*. Baden-Baden: Nomos, 1997.

Korinek, Anton, and Jai Vipra. "AI Monopolies." *Economic Policy* (Panel Brief), 27 March 2024. https://www.economic-policy.org/79th-economic-policy-panel/ai-monopolies/

Kornarakes, Konstantinos. "Artificial Intelligence and the Modern Human." *dia-LOGOS* 14 (2024): 204 ff.

Kosti, Iliana. "Can the Algorithm Be Fair?" In *Can the Algorithm … Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, edited by Lilian Mitrou, 97 ff. Heraklion: University of Crete University Press, 2023.

Koukiadis, Dimitrios. "The Regulatory Challenges of Artificial Intelligence and the Issue of Recognition of Personality." *Journal of Law and Technology* (2020): 17 ff.

Koulouri, Christina. "Universities in the Age of Metrics." *To Vima*, July 3, 2025. https://www.tovima.gr/print/opinions/ta-panepistimia-stin-epoxi-lfton-metrikon/

Kremalis, Konstantinos. *The Right to Health Protection*. Athens, 1987.

Kriari-Katrani, Ismini. "Administrative Law in the Face of the Challenges of Biology and Medicine." In *Proceedings of the Hellenic Society of Administrative Studies 1992–2003*, 75 ff. Athens, 2004.

Kriari-Katrani, Ismini. *Genetic Technology and Fundamental Rights*. Athens–Thessaloniki: Sakkoulas, 1999.

Kriari-Katrani, Ismini. *Technology and Parliament: The Institutional Role and Work of Parliamentary Committees and Technology Assessment Offices*. Athens–Thessaloniki: Sakkoulas, 2001.

Ladeur, Karl-Heinz. *Public Governance and Risk Regulation: Towards a Constitutional Framework for Transnational Decision-Making*. Oxford: Hart Publishing, 2017.

Lefebvre, Hippolyte, Christine Legner, and Elizabeth A. Teracino. "5 Pillars for Democratizing Data at Your Organization." *Harvard Business Review*, November 24, 2024.

Lekea, Ioanna K., George K. Lekeas, and Pavlos Topalnakos. "Exploring Enhanced Military Ethics and Legal Compliance through Automated Insights: An Experiment on Military Decision-making in Extremis." *Conatus – Journal of Philosophy* 8, no. 2 (2023): 345–372. https://doi.org/10.12681/cjp.35213.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Lezgioglu Ozer, Sena. "Regulatory Sandboxes in the AI Act: Between Innovation and Safety." DigiCon (2024). https://digi-con.org/regulatory-sandboxes-in-the-ai-act-between-innovation-and-safety

Lichfield, Gideon. "Meet Your AI Politician of the Future." *Futurepolis Substack*, October 4, 2024. https://futurepolis.substack.com/p/meet-your-ai-politician-of-the-future

Lindner, Ines, Bernd Heidergott, Saeed Badri, and Merle Praum. "The Impact of Bots on Social Learning and Consensus Formation: Why Even an 'Infinitesimal' Number of Bots Matters." SSRN preprint, December 2024. https://ssrn.com/abstract=5249942

Loftus, Alex. "EU Investigates TikTok over Alleged Russian Meddling in Romanian Vote." *BBC News*, 17 December 2024. https://www.bbc.com/news/articles/cm2v13nz2020

Manesis, Aristovoulos. *Individual Liberties*. Vol. A. 3rd ed. Thessaloniki: Sakkoulas, 1981.

Margaritis, Michail. *The European Convention on Human Rights and Protocols Nos. 1, 6, 7 and 13: Interpretation per Article*. Athens: Nomiki Vivliothiki, 2018.

Marinos, Vasileios. "The Constitution in the Digital Age." *Epitheorisi Dimosiou Dikaiou* 2024: 133 ff.

Martini, Mario, and Christiane Wendehorst, eds. *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*. Munich: C.H. Beck, 2024.

McCarthy, John. *What Is Artificial Intelligence?* November 12, 2017. http://jmc.stanford.edu/articles/whatisai.pdf

McSweeney, Latanya. "Psychographics, Predictive Analytics, Artificial Intelligence & Bots: Is the FTC Keeping Pace?" *Data Privacy Lab* (2013): 514 ff. http://dataprivacylab.org/projects/onlineads/1071-1.pdf

Metropolitan of Mesogaia and Lavreotiki Nikolaos. "Bioethical Approaches to the Impact of Artificial Intelligence on Human Life." https://bioethics.panteion.gr/dimosieyseis/

Metropolitan of Mesogaia and Lavreotiki Nikolaos. "Bioethical Approaches to the Impact of Artificial Intelligence on Human Life." *Estia*, October 11, 2025.

Miller, Sean J. "AI Is Helping Candidates Decide on Runs for Higher Office." *Campaigns & Elections*, October 22, 2024. https://campaignsandelections.com/campaigntech/ai-is-helping-candidates-decide-on-runs-for-higher-office

Mitrou, Lilian, ed. *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?* Heraklion: University of Crete University Press, 2023.

Mitrou, Lilian. "Digital Democracy, Participation and Threats." In *Rule of Law and Democracy in the Digital Age*, edited by Giorgos Karavokyris, 53 ff. Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024.

Mitrou, Lilian. "The 'Regulation' of Artificial Intelligence or the Collingridge Dilemma." Paper, SciFY Academy / NCSR Demokritos, June 2020.

Moraiti, Athina, and Charalampos Stamelos. "The Impact of AI on Data Protection: Evolution of Court of Justice of the European Union Case Law Regarding the General Data Protection Regulation (GDPR) in the Artificial Intelligence Era." In *EU Digital Law in the AI Era*, edited by Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou, and Thalia Prastitou-Merdi. Cham: Springer, 2025 (forthcoming).

Moukiou, Chryssoula P. *Algorithms and Administrative Law*. Athens–Thessaloniki: Sakkoulas, 2025.

Negnevitsky, Michael. *Artificial Intelligence: A Guide to Intelligent Systems*. 3rd ed. Boston: Addison Wesley, 2011.

New York Times. "Imran Khan's 'Victory Speech' from Jail Shows A.I.'s Peril and Promise." February 11, 2024.

Nikolopoulou, Antonia. "Article 21, Health and Artificial Intelligence." In *Artificial Intelligence, Human Rights and the Rule of Law*, edited by Evripidis Stylianidis, 426 ff. Athens: Nomiki Vivliothiki, 2025.

OECD. *Eight Ways to Institutionalise Deliberative Democracy*. Paris: OECD, 2021.

OECD. *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave*. Paris: OECD, 2020.

Orphanidis, Dimitris. *Homo Sapiens or Cyborg Sapiens? Legal Order for the Human or the Posthuman?* Athens–Thessaloniki: Sakkoulas, 2024.

Panagopoulou, Fereniki, and Metropolitan of Mesogaia and Lavreotiki Nikolaos (Chatzinikolaou). "Ethical, Philosophical, and Theological Approaches to the Impact of Artificial Intelligence on Human Life." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 549 ff. Athens: Nomiki Vivliothiki, 2025.

Panagopoulou, Fereniki. "Algorithmic Decision-Making in Public Administration." In *Rule of Law and Democracy in the Digital Age*, edited by Giorgos Karavokyris, 137 ff. Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024.

Panagopoulou, Fereniki. "Artificial Intelligence and Independent Authorities." *Journal of Public Administration* 6, no. 1 (2024): 34 ff. https://sryahwapublications.com/journals/journal-of-public-administration/volume-6/issue-1.

Panagopoulou, Fereniki. "Constitution and Happiness: Can the Constitution Guarantee Happiness?" *Huffington Post Greece*, July 7, 2025. https://www.huffingtonpost.gr/entry/sentayma-kai-eetechia_gr_684fe2dae4b07f75743a89df.

Panagopoulou, Fereniki. "Language as a Cultural Good in Large Language Models." *Huffington Post Greece*, April 9, 2024. https://www.huffingtonpost.gr/entry/h-ylossa-os-politismiko-ayatho-sta-meyala-ylossika-montela_gr_6613982ce4b056f720588bfb.

Panagopoulou, Fereniki. *Electronic Voting: A Constitutional-Ethical Approach*. Athens–Thessaloniki: Sakkoulas, 2023.

Panagopoulou, Paraskevi. "The Use of Artificial Intelligence in Medicine." *diaLOGOS* 14 (2024): 215 ff.

Panagopoulou-Koutnatzi, Fereniki. "Constitutional Approach to the Data Protection Law (Law 4624/2019)." *DiMEE* (2019): 328 ff.

Panagopoulou-Koutnatzi, Fereniki. "Constitutional Dimensions of Extending Personal Data Protection Beyond the EU: Extraterritorial Application of the GDPR and Cross-Border Data Transfers." *Efimeris Dimosiou Dikaiou* 4 (2019): 504 ff.

Panagopoulou-Koutnatzi, Fereniki. "Issues of Constitutionality in Distance Schooling." *Efimeris Dimosiou Dikaiou* (2020): 292 ff.

Panagopoulou-Koutnatzi, Fereniki. "Legal and Ethical Concerns about the Use of ChatGPT in Education." *Journal of Law and Technology* (2023): 6 ff.

Panagopoulou-Koutnatzi, Fereniki. "Research in Historical Sources and Protection of Information." *DiMEE* (2014): 28 ff.

Panagopoulou-Koutnatzi, Fereniki. "The Issue of Cameras (Portable and Body-Worn) Used by Riot Police." *Syntagma Watch*, January 4, 2021. https://www.syntagmawatch.gr/trending-issues/to-zitima-twn-kamerwn-foritwn-kai-swm

atos-poy-feroun-oi-monades-apokatastaseos-tis-taxis-mat-tis-ellhnikhs-astynomias/.

Panagopoulou-Koutnatzi, Fereniki. *Artificial Intelligence: The Path to a Digital Constitutionalism – An Ethical-Constitutional Approach*. Athens: Papazisis, 2023.

Panagopoulou-Koutnatzi, Fereniki. *Freedom of Blogs: New Technologies as National, European and International Challenge for Freedom of Expression*. Athens–Thessaloniki: Sakkoulas, 2010.

Panayiotou, Andrie G., and Evangelos D. Protopapadakis. "Ethical Issues concerning the Use of Commercially Available Wearables in Children: Informed Consent, Living in the Spotlight, and the Right to an Open Future." *Jahr – European Journal of Bioethics* 13, no. 1 (2022): 9-22, especially 16ff. https://doi.org/10.21860/j.13.1.1.

Papadopoulou, Lina. "Fake News and Hate Speech." In *Rule of Law and Democracy in the Digital Age*, edited by Giorgos Karavokyris, 99 ff. Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024.

Papadopoulou, Lina. "Robots and Sheriffs." *To Vima Daily*, March 19, 2025. https://www.tovima.gr/print/opinions/rompot-kai-serifides/.

Papakonstantinou, Souzana. "HDPA Decision 35/2022: Facial Recognition Technology in Schools." *e-Politeia* 6 (2023): 268 ff.

Papakonstantinou, Vagelis, and Paul De Hert. "Refusing to Award Legal Personality to AI: Why the European Parliament Got It Wrong." *European Law Blog*, 20 November 2020. https://europeanlawblog.eu/2020/11/20/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/

Papakonstantinou, Vagelis, and Paul De Hert. "Structuring Modern Life Running on Software: Recognizing (Some) Computer Programs as New 'Digital Persons.'" *Computer Law & Security Review* 34, no. 4 (2018): 732–738.

Papakonstantinou, Vagelis, and Paul De Hert. *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis, and EU Law Brutality at Play*. London: Routledge, 2024.

Paparrigopoulou, Patrina. *Article 21 paras. 2, 4, 5, 6 of the Constitution*. Athens: Nomiki Vivliothiki, 2017.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.

Pavlopoulos, Prokopios. "Critical Reflections on the Relevance of Aristotle's Positions on Law and Justice in the Age of Artificial Intelligence." *Public Law Review* 1 (2025): 41 ff.

Pavlopoulos, Prokopios. "Dilemmas of Legal Science in the Age of Artificial Intelligence." *Constitutionalism.gr*, February 2025. https://www.constitutionalism.gr/dilimata-tis-nomikis-epistimis-stis-prokliseis-tis-ai/.

Pierrakakis, Kyriakos. Introduction to Manolis Andriotakis, *Artificial Intelligence for All*, 9–12. Athens: Psychogios, 2022.

Polanyi, Karl. *The Great Transformation*. Boston: Beacon Press, 2001 [1944].

Polymeris, Spyros. "Chaos Theory, Artificial Intelligence and Education: A Discussion." *Public Administration Review* (Greece): 81 ff. https://www.lawjournals.unic.ac.cy/index.php/pareview.

Ranchordas, Sofia, and Valeria Vinci. "Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture." *Italian Journal of Public Law* 16 (2024): 107, 132. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4696442

Ranchordas, Sofia. "Experimental Lawmaking in the EU: Regulatory Sandboxes." *EU Law Live, Weekend Edition*, October 22, 2021. University of Groningen Faculty of Law Research Paper No. 12/2021. SSRN: https://ssrn.com/abstract=3963810

Ranchordas, Sofia. "Innovation Experimentalism in the Age of the Sharing Economy." *Lewis & Clark Law Review* 19 (2015): 871.

Reed, Chris. "How Should We Regulate Artificial Intelligence?" *Philosophical Transactions of the Royal Society A* 376, no. 2128 (2018).

Ringe, Wolf-Georg, and Christopher Ruof. "Keeping Up with Innovation: Designing a European Sandbox for FinTech." *ECMI Commentary* no. 58 (2019). https://www.ecmi.eu/publications/commentaries/keeping-innovation-designing-european-sandbox-fintech

Rizos, Panagiotis. *Tartaros Ltd*. Athens: Papadopoulos, 2024.

Rohrlich, Michael. *KI und Recht*. Munich: Hanser, 2025.

Roden-Bow, Ashley. "Killer Robots and Inauthenticity: A Heideggerian Response to the Ethical Challenge Posed by Lethal Autonomous Weapons Systems." *Conatus – Journal of Philosophy* 8, no. 2 (2023): 477–486. https://doi.org/10.12681/cjp.34864.

Rudschies, Catharina, Ingrid Schneider, and Judith Simon. "Value Pluralism in the AI Ethics Debate: Different Actors, Different Priorities." *International Review of Information Ethics* 32 (2024). https://informationethics.ca/index.php/irie/article/view/419/396

Sarafianos, Dimitris. *Interpretation of Article 16 of the Constitution*. Athens: Nomiki Vivliothiki, 2017.

Sarmas, Dimitris. "Article 14." In *Article-by-Article Commentary on the Charter of Fundamental Rights of the EU*, edited by Eugenia R. Sahpekidou and Haris N. Tagaras, 164 ff. Athens: Nomiki Vivliothiki, 2020.

Savcisens, Germans, et al. "Using Sequences of Life-Events to Predict Human Lives." *Nature Computational Science* (2023). https://doi.org/10.1038/s43588-023-00573-5

Schneier, Bruce, and Nathan Sanders. "The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture." *Ash Center, Harvard Kennedy School*, December 4, 2024. https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/

Schwartmann, Rolf, Kristin Benedikt, Moritz Köhler, and Markus Wünschelbaum. *Erste Hilfe zur KI-Verordnung: KI-Kompetenz, Rechte, Pflichten*. Munich: C.H. Beck, 2025.

Selinger, Evan, and Brenda Leong. "Facial Recognition Technology Primer: What Is It and How Is It Used?" In *The Oxford Handbook of Digital Ethics*, edited by Carissa Véliz, 590 ff. Oxford: Oxford University Press, 2021.

Soilentakis, Panagiotis. *Artificial Intelligence at the Core of Constitutional and Administrative Law*. Athens: Nomiki Vivliothiki, 2025.

Spelliscy, Connor, Sarah Hubbard, Nathan Schneider, and Samuel Vance-Law. "Toward Equitable Ownership and Governance in the Digital Public Sphere." *Stanford Journal of Blockchain Law & Policy* (2024). https://stanford-jblp.pubpub.org/pub/equitable-ownership-and-governance/release/1

Stiglitz, Joseph E. *People, Power, and Profits: Progressive Capitalism for an Age of Discontent*. New York: W.W. Norton, 2019.

Stratilatis, Konstantinos. "Article 5A of the Constitution: The Right to Information." In *Article-by-Article Commentary on the Constitution*, edited by Spy-

ros Vlachopoulos, Xenophon Contiades, and Giannis Tasopoulos. Syntagma Watch. https://www.syntagmawatch.gr/my-constitution/arthro-5a/.

Stylianidis, Evripidis and Thaleia Chalkidzi. "Article 16." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 306 ff. Athens: Nomiki Vivliothiki, 2025.

Stylianidis, Evripidis. "Article 5A." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 145 ff. Athens: Nomiki Vivliothiki, 2025.

Stylianidis, Evripidis. "Proposal on Artificial Intelligence in View of the Revision of the Greek Constitution." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 633 ff. Athens: Nomiki Vivliothiki, 2025.

Suzor, Nicolas P. "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms." *Social Media + Society* 4, no. 3 (2018): 1–11.

Tamamidis, Anastasios. *Interpretation of Article 2 of Protocol No. 1 ECHR*. Athens: Nomiki Vivliothiki, 2021.

Tassis, Spyros. "Can the Algorithm Be Ethical?" In *Can the Algorithm ... Be Ethical, Be Fair, Be Transparent, Judge and Govern?*, edited by Lilian Mitrou, 35 ff. Heraklion: University of Crete Press, 2023.

Tegmark, Max, Rob Shapiro, et al. *Life 3.0: Being Human in the Age of Artificial Intelligence*. New York: Vintage Books, 2018.

Tesla Team. "A Tragic Loss." *Tesla Blog*, June 30, 2016.

Theodosis, Giorgos. "Article 21." In *Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, edited by Evripidis Stylianidis, 452 ff. Athens: Nomiki Vivliothiki, 2025.

Times of India. "BJP to Use AI to Translate PM's Speeches." March 8, 2024. https://timesofindia.indiatimes.com/india/bjp-to-use-ai-to-translate-pms-speeches/articleshow/108298093.cms

Travlos-Tzanetatos, Dimitris. *Labour Law in the Fourth Industrial Revolution: Digitalisation, Robotics and Artificial Intelligence*. Athens–Thessaloniki: Sakkoulas, 2019.

Truby, John, et al. "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications." *European Journal of Risk Regulation* 13 (2022):

270–286. https://ris.utwente.nl/ws/files/304762207/a_sandbox_approach_to_regulating_high_risk_artificial_intelligence_applications.pdf

Tsekeris, Charalambos, Vangelis Karkaletsis, et al. *Generative AI Greece 2030: Possible Futures of Generative AI in Greece*. Athens: Secretariat for Long-Term Planning, 2023. https://foresight.gov.gr/wp-content/uploads/2024/02/GenAI_Greece_2030.pdf.

Tsekeris, Charalambos. "Human Communication in the Vortex of the 'Strange Magic' of Social Networks." *Oikonomiki Epitheorisi*, April 22, 2024. https://www.economia.gr/texnologia-kenotomia/h-anthropini-epikoinonia-sti-dini-tis-paraxenis-mageias-ton-koinonikon-diktion/.

Tsiliotis, Charalambos. *Public Law Parameters of the Anti-Covid 19 Vaccination*. Athens: Nomiki Vivliothiki, 2021

Tsinorema, Stavroula. "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility." In *Liber Amicorum Ismini Kriari*, 259 ff. Athens: Sideris, 2025.

Tsinorema, Stavroula. "Artificial Intelligence with a Human Face: Towards a Technoethics of Responsibility." *Philosophies* 1, no. 2 (2021): 8. https://www.mdpi.com/2673-2688/1/2/8

Tsiris, Panagiotis. *The Constitutional Protection of the Right to Confidentiality of Communications*. Athens–Komotini: Ant. N. Sakkoulas, 2002.

Turing, Alan M. "Computing Machinery and Intelligence." *Mind* 59, no. 236 (1950): 433–460.

Tzemos, Vasilis. "The New AI Regulation and the Charter of Fundamental Rights of the EU." In *Exploring Aspects of Artificial Intelligence: Cutting-Edge Technologies as a Legislative Challenge (2nd Interdisciplinary Conference on Law and Informatics)*, edited by Eugenia Alexandropoulou-Aigyptiadou, Theoharis Dalakouras, and Christos Mastrokostas, 99 ff. Athens: Nomiki Vivliothiki, 2025.

Uneecops. "How Data Analytics Drive Growth for Wealth Management Firms." August 2, 2024. https://www.uneecops.com/blog/how-data-analytics-drive-growth-for-wealth-management-firms/

UNESCO. *Artificial Intelligence and Democracy*. Paris: UNESCO, 2024. https://unesdoc.unesco.org/ark:/48223/pf0000388129

Véliz, Carissa, ed. *The Oxford Handbook of Digital Ethics*. Oxford: Oxford University Press, 2021.

Véliz, Carissa. "The Surveillance Delusion." In *The Oxford Handbook of Digital Ethics*, edited by Carissa Véliz. Oxford: Oxford University Press, 2021; online ed., Oxford Academic, 10 November 2021. https://doi.org/10.1093/oxfordhb/9780198857815.013.30

Venizelos, Evangelos. "The Constitutional Limits on the Lifting of Telephone Confidentiality of Citizens and Politicians for National Security Reasons – The Androulakis Case." *Constitutionalism*, August 27, 2022.

Venizelos, Evangelos. *Article 25, General Clause for the Protection of Rights*. Athens: Nomiki Vivliothiki, 2017.

Venizelos, Evangelos. *The Constitution and its Enemies*. Athens: Sideris, 2021.

Venizelos, Evangelos. *The Democratic Constitution at Risk*. Athens: Papazisis, 2024.

Venizelos, Evangelos. *The Revisionary Acquis: The Constitutional Phenomenon in the 21st Century and the Contribution of the 2001 Revision*. Athens–Komotini: Ant. N. Sakkoulas, 2002.

Vidalis, Takis K. "The Impact of Technology on Democracy." In *Liber Amicorum Ismini Kriari*, 21 ff. Athens: Sideris, 2025.

Vidalis, Takis K. *Biolaw, Vol. 1: The Person*. Athens–Thessaloniki: Sakkoulas, 2007.

Vlachopoulos, Spyridon. "Prenatal Testing and Individual Rights: Developments in Genetics, Scientific Freedom, and the Right to Genetic Ignorance." *Dikaioma tou Anthropou* (2002): 363 ff.

Vlachopoulos, Spyros V. "The Rule of Law and the Constitution in the Digital Age." In *Rule of Law and Democracy in the Digital Age*, edited by Giorgos Karavokyris, 65 ff. Athens: Hellenic Parliament Foundation for Parliamentarism and Democracy, 2024.

Vlachopoulos, Spyros. *The Selfish Gene of Law and the Law of Artificial Intelligence*. Athens: Eurasia, 2023.

Warren, Matthew. "The Approach to Predictive Medicine That Is Taking Genomics Research by Storm: Polygenic Risk Scores Represent a Giant Leap for Gene-Based Diagnostic Tests. Here's Why They're Still So Controversial." *Nature* 562 (2018): 181–83. https://doi.org/10.1038/d41586-018-06956-3

Weizenbaum, Joseph. *Computer Power and Human Reason: From Judgment to Calculation*. San Francisco: W. H. Freeman, 1976.

Wendehorst, Christiane. "Art. 1–3." In *KI-VO, Kommentar, Verordnung über künstliche Intelligenz*, edited by Mario Martini and Christiane Wendehorst. Munich: C.H. Beck, 2024.

Wile, Rob. "A Venture Capital Firm Just Named an Algorithm to Its Board of Directors." *Business Insider*, May 13, 2014. https://www.businessinsider.com/algorithm-named-to-board-of-directors-2014-5

Williams, Ross. "Georgia Political Campaigns Start to Deploy AI but Humans Still Needed to Press the Flesh." *GPB News*, 25 April 2024. https://www.gpb.org/news/2024/04/25/georgia-political-campaigns-start-deploy-ai-humans-still-needed-press-the-flesh

Winfield, Alan F. T., and Marina Jirotka. "Ethical Governance Is Essential to Building Trust in Robotics and Artificial Intelligence Systems." *Philosophical Transactions of the Royal Society A* 376, no. 2133 (2018).

World Bank Group. *Global Experiences from Regulatory Sandboxes*. Washington, DC: World Bank, 2020.

Yampolskiy, Roman. *Artificial Intelligence: Inexplicable, Unpredictable, Uncontrollable*. Athens: Epikentro, 2024.

Zekos, Georgios I. *Internet and Artificial Intelligence in Greek Law*. Athens–Thessaloniki: Sakkoulas, n.d.

Zetzsche, Dirk A., et al. "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation." *Fordham Journal of Corporate & Financial Law* 23 (2017): 64. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018534

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

The study critically outlines the key aspects of Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act) and selectively highlights issues of constitutional interest that merit serious consideration. It comprises an Introduction, a General Section, a Special Section, and Conclusions.

The Introduction sets out the overall framework of the study and provides a brief clarification of terminology. The General Part describes the process of adopting the Regulation and related legislation, followed by a comparative overview of AI regulation. It then examines the necessity of legislative intervention, outlines the philosophy and objectives of the text, and analyses the guiding principles that should govern the regulatory framework. The section proceeds with an examination of the scope of application and its similarities with Regulation (EU) 2016/679 (General Data Protection Regulation). It continues with the issues of control and supervision at both national and supranational level, and concludes with a systematisation of the sanctions and liability regime and an analysis of the Regulation's entry into force.

The Special Section addresses key areas raising significant constitutional questions, including biometric identification, employment, democracy, education, health, and innovation. A separate part considers whether the revising legislator should incorporate AI into the forthcoming constitutional revision. The study concludes with final observations.

Logos Verlag Berlin

ISBN 978-3-8325-6016-4