



Hellenic Republic
Greek National Commission
for Human Rights

GNCHR Report

Human Rights and Artificial Intelligence



October 2026



NOMIKI BIBLIOTHIKI



Co-funded by
the European Union

Co-financed by the European Union. Views and opinions expressed are
however those of the author(s) only and do not necessarily reflect those
of the European Union or ENNHRI. Neither the European Union nor
ENNHRI can be held responsible for them.



AVAILABLE AT



www.quallex.gr

GNCHR Report

Human Rights and Artificial Intelligence

GNCHR

The Report was adopted by the Plenary of the GNCHR on 22 July 2026. The Rapporteurs were Professor Maria Gavouneli, President, and Dr Christos Tsevas, Human Rights Advisor.

Research and drafting: Dr Christos Tsevas, Human Rights Advisor

Translation: Kelly Diavati, Official Translator

ISBN 978-618-08-1106-3

COPYRIGHT

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission of NOMIKI BIBLIOTHIKI S.A., or as expressly permitted by law or under the terms agreed with the appropriate reprographic rights organization. Enquiries concerning reproduction which may not be covered by the above should be addressed to NOMIKI BIBLIOTHIKI S.A. at the address below.

DISCLAIMER

The content of this work is intended for information purposes only and should not be treated as legal advice. The publication is necessarily of a general nature; NOMIKI BIBLIOTHIKI, the author and the contributors make no claim as to the comprehensiveness or accuracy of the information provided; Information is not offered for the purpose of providing individualized legal advice. Professional advice should therefore be sought before any action is undertaken based on this publication. Use of this work does not create an attorney-client or any other relationship between the user and NOMIKI BIBLIOTHIKI, or the author, or the rest of contributors.



NOMIKI BIBLIOTHIKI



23 Mavromichali str. | 106 80 | Athens | Greece

T +30 210 3678 800 | F +30 210 3678 819

www.nb.org | info@nb.org



© 2026, NOMIKI BIBLIOTHIKI S.A.

The printing of this report was carried out in the framework of the project Advancing Human Rights in the Age of AI: NHRI Cooperation, Capacity Building and Policy Dialogue, co-funded by the European Union (Project SGA-CERV-2026-07) through the European Network of National Human Rights Institutions (ENNHRI).



Hellenic Republic
Greek National Commission
for Human Rights

GNCHR Report

Human Rights and Artificial Intelligence



October 2026



NOMIKI BIBLIOTHIKI

PREAMBLE

Technological progress has been one of the key factors in transforming societies over time. In modern times, Artificial Intelligence (AI) is emerging as the most decisive technological advance, with the potential to affect almost every aspect of human activity: from work, health and education to justice, public administration, security and democratic participation. The rapid development and growing integration of AI systems into people's daily lives create new prospects for social and economic progress, while at the same time raising important questions concerning the protection of human rights, equality, transparency, accountability and the rule of law.

To date, human rights protection has been ensured through an extensive framework of international, European and domestic rules, supported by dedicated mechanisms for monitoring their implementation, albeit with different levels of effectiveness. But rapid technological change poses fundamental new challenges: Conventional legislation is generally developed in response to identifiable societal needs: legal rules seek to address those needs by setting out a prescribed standard of conduct, the breach of which gives rise to a sanction. Today, however, developments in AI are advancing at an exponential pace, while the legal rules continue to adapt in a linear manner. The resulting gap between regulation and societal needs is therefore growing ever wider. This occurs even without taking into account the industry's tendency to favour self-regulatory solutions, often justified by an alleged tension between two competent and parallel imperatives: promoting innovation and ensuring effective regulation.

In any case, it is becoming increasingly clear that the debate is slowly but surely shifting from an exclusively technological or economic approach to a perspective with a focus on the pillar of human rights. The debate on AI is primarily about how technology affects people, particularly those who are already in a vulnerable position or at risk

of being excluded from the benefits of technological progress. The need for such an approach is now reflected in the international, European and national regulatory environment. The United Nations (UN), the Council of Europe (CoE), UNESCO, the Organisation for Economic Cooperation and Development (OECD) and the European Union (EU) through the Artificial Intelligence Act acknowledge that the development and use of AI must be based on respect for human rights, democratic accountability and human oversight. At the same time, Greece is already taking important steps in shaping its national governance framework on AI, which make it necessary to systematically involve institutions with expertise in human rights.

In an international environment, the National Human Rights institutions (NHRIs) have a crucial role to play, ensuring that technological progress remains compatible with human dignity, freedom and democracy. Sharing a common purpose with our counterparts, we at the Greek National Commission for Human Rights (GNCHR) are moving forward in the same spirit, contributing both to the international debate and through practical means to the shaping of the new framework, in full respect of the human rights acquired and with an open mind to the evolving requirements of technology. This position is fully rooted in the mandate entrusted to us by the UN General Assembly and the Greek State. As Greece's independent and pluralistic NHRI, the GNCHR, has the responsibility to monitor, assess and highlight the impact of public policies and technological advances on the enjoyment of human rights. This mission is not limited to addressing existing violations, but extends to the early identification of emerging risks and the formulation of proposals that allow the State to prevent adverse developments and integrate human rights principles into the design of its policies.

This Reference Report seeks to offer an initial, coherent framework for examining the relationship between artificial intelligence and human rights in Greece. It maps the principal international, European and domestic instruments forming the emerging regulatory landscape; identifies AI's key prospects and challenges across critical areas of public policy; and considers the fundamental principles that should govern the development and deployment of relevant AI systems.

Particular emphasis is placed on the impact of AI on areas such as work, health, gender equality, children's rights, disability, migration and asylum, public administration and the democratic functioning of institutions.

The connection between AI principles and human rights becomes crucially important in this context. Human dignity, non-discrimination, equality, privacy and personal data protection, transparency, accountability, security, proportionality and human oversight are not merely technical or regulatory requirements. They establish substantial safeguards for the protection of human rights in the new digital age. The Report highlights precisely that the principles of trustworthy AI and human rights constitute interrelated fields

and it further highlights the particular added value of the GNCHR within the national AI governance system. Through its pluralistic composition, which includes independent authorities, universities, research institutions, professional bodies, trade unions and civil society organisations, the GNCHR provides a unique forum for dialogue, for bringing diverse perspectives together and for developing common approaches that place human rights at the heart of the AI landscape.

The Report is not intended to conclude the debate. Rather, it marks the beginning of a long-term project involving monitoring, dialogue, advisory opinions, interventions and focused analysis in the specific areas in which AI is expected to play a decisive role in the years ahead. The GNCHR will continue to be actively contributing to the national, European and international debate, working with the State, independent authorities, international organisations, NHRI networks, academia, the technology and research sector and civil society.

At a time when the digital transition is reshaping the boundaries between humans and technology, the protection of human rights does not constitute an impediment to innovation. On the contrary, it is the necessary condition for its sustainable, fair and democratic development. Artificial intelligence can only serve as a tool for collective progress if it is designed, developed and used with a human-centric approach. This is the central message and the fundamental



aspiration of this Reference Report; at the same time, it is its guiding principle and the first step on the long path of adaptation that is only just beginning. Let's make a start.

Athens, 1 October 2026

Professor Maria Gavouneli

President

Greek National Commission for Human Rights

CONTENTS

PREAMBLE.....	V
ABBREVIATIONS.....	XV

CHAPTER 1

Introduction	2
--------------------	---

CHAPTER 2

International, European and National Legal Framework.....	10
---	----

CHAPTER 3

Perspectives and Challenges in the light of Human Rights	22
3.1 Introduction.....	22
3.2 Work and artificial intelligence	24
3.2.1 Introduction	24
3.2.2 Challenges associated with human rights.....	25
3.2.3 Perspectives and recommendations	30
3.3 Artificial intelligence in the health sector.....	31
3.3.1 Introduction	31
3.3.2 Challenges associated with human rights.....	32
3.3.3 Perspectives and recommendations	36

3.4 Artificial intelligence in the sector of justice	38
3.4.1 Introduction	38
3.4.2 Challenges associated with human rights	39
3.4.3 Perspectives and recommendations	41
3.5 Artificial intelligence in the field of asylum and migration	45
3.5.1 Introduction	45
3.5.2 Challenges associated with human rights	48
3.5.3 Perspectives and recommendations	50
3.6 Education, research and artificial intelligence	54
3.6.1 Introduction	54
3.6.2 Challenges associated with human rights	54
3.6.3 Perspectives and recommendations	57
3.7 Artificial intelligence and its use in law enforcement, policing and the prison system	64
3.7.1 Introduction	64
3.7.2 Challenges associated with human rights	65
3.7.3 Perspectives and recommendations	68
3.8 Artificial intelligence in public administration and governance	72
3.8.1 Introduction	72
3.8.2 Challenges associated with human rights	73
3.8.3 Perspectives and recommendations	75
3.9 Women's and girls' rights and artificial intelligence	80
3.9.1 Introduction	80
3.9.2 Challenges associated with human rights	80
3.9.3 Perspectives and recommendations	83

3.10 Rights of the child and artificial Intelligence.....	85
3.10.1 Introduction	85
3.10.2 Challenges associated with human rights.....	86
3.10.3 Perspectives and recommendations	88
3.11 Persons with disabilities' rights and artificial intelligence.....	92
3.11.1 Introduction	92
3.11.2 Challenges associated with human rights.....	93
3.11.3 Perspectives and recommendations	94
3.12 Mass media, freedom of expression and artificial intelligence.....	96
3.12.1 Introduction	96
3.12.2 Challenges associated with human rights.....	97
3.12.3 Perspectives and recommendations	98
3.13 Democracy, elections, disinformation and artificial intelligence.....	99
3.13.1 Introduction	99
3.13.2 Challenges associated with human rights.....	99
3.13.3 Perspectives and recommendations	100
3.14 Environment and artificial intelligence.....	101
3.14.1 Introduction	101
3.14.2 Challenges associated with human rights.....	102
3.14.3 Perspectives and recommendations	103
3.15 Discrimination, prejudice and artificial intelligence.....	105
3.15.1 Introduction	105
3.15.2 Challenges associated with human rights.....	105
3.15.3 Perspectives and recommendations	107

3.16 AI business and human rights	109
3.16.1 Introduction	109
3.16.2 Challenges associated with human rights.....	110
3.16.3 Perspectives and recommendations	111

CHAPTER 4

The Principles of Artificial Intelligence as Safeguards for the Protection of Human Rights.....	112
4.1 Introduction	112
4.2 Principle of respect for human dignity and individual autonomy	114
4.3 Principle of human-centric AI	118
4.4 Principle of respect for privacy and data governance	119
4.5 Principle of trustworthiness in artificial intelligence	121
4.6 Principle of transparency	123
4.7 Principle of equality and non-discrimination in access to information	126
4.8 Principle of proportionality	128
4.9 Principle of accountability and responsibility	128
4.10 Human oversight	130
4.11 Principle of societal and environmental wellbeing	132
4.12 Awareness and literacy	133
4.13 The principle of safe innovation	134

CHAPTER 5

The added value of the Greek National Commission for Human Rights in the context of artificial intelligence governance.....	136
5.1 Article 77 of EU Regulation 2024/1689 – Principles for the protection of fundamental rights and the role of the GNCHR.....	136
5.2 List of national authorities referred to in Article 77 of the Regulation	138
5.3 Competences and tasks of the GNCHR in the framework of the Regulation	140

CHAPTER 6

Conclusions – Recommendations.....	152
6.1 Summary of the Report's purpose and structure.....	152
6.2 Thematic conclusions and recommendations	152
6.3 The role of the GNCHR in the context of AI governance in Greece.....	157

ABBREVIATIONS

ADAE	Hellenic Authority for Communication Security and Privacy
AI	Artificial Intelligence
CAI	Committee on Artificial Intelligence
CDNET	Steering Committee for New and Emerging Digital Technologies the Charter Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENNHRI	European Network of National Human Rights Institutions
EU	European Union
EU AI Act	Regulation (EU) 2024/1689 (Artificial Intelligence Act)
FRA	European Union Agency for Fundamental Rights
FRIA	Fundamental Rights Impact Assessment
GANHRI	Global Alliance of National Human Rights Institutions
GDPR	General Data Protection Regulation
GNCHR	Greek National Commission for Human Rights
GPAI	General-Purpose Artificial Intelligence
HDPA	Hellenic Data Protection Authority
HRIA	Human Rights Impact Assessment
ICT	Information and Communication Technologies
ILO	International Labour Organization



LLM	Large Language Model
ML	Machine Learning
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization 1



ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΓΙΑ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΑΝΘΡΩΠΟΥ
GREEK NATIONAL COMMISSION FOR HUMAN RIGHTS

The Greek National Commission for Human Rights (GNCHR) is the independent advisory body of the Greek State and the National Institution for the Protection of Human Rights. It has been established by Law 2667/1998 under UN rules (Paris principles) as replaced by Law 4780/2021. It is composed of members designated by twenty bodies (independent authorities, trade unions, human rights organisations, higher education institutions and research institutions).

CHAPTER 1

Introduction

The GNCHR, as the National Institution for the protection and promotion of human rights and the advisory body to the State, in accordance with the [Paris Principles \(UN GA Res. 48/134, 1993\)](#) Paris Principles (UN General Assembly Resolution 48/134, 1993) and [Law 4780/2021](#) Law 4780/2021, has, inter alia, the institutional mandate of continuously monitoring matters relating to human rights.

Artificial Intelligence (AI) is one of the most radical technological changes of the modern era, with profound implications for social relations, the economy, democracy and the exercise of human rights. Technologies are evolving, social rules are changing and new challenges are emerging. The increasing use of AI systems in recent years is no longer limited to technical or auxiliary functions but extends to decision-making areas that directly affect human life, freedom and dignity. In this light, the debate on AI shifts from the question of technological innovation to the question of the normative and ethical delimitation.

This text¹ of the GNCHR aims to outline its main issues and positions, focusing on the principles that should govern the development and use of AI and the protection of human rights where applied, as the common ground of all bodies dealing with this subject. The purpose of the report is to approach artificial intelligence, in terms of human rights perspectives and challenges; however, not all the relevant issues can be covered in a text of limited length, especially as new developments arise every day. **For this reason, through this report**

1. This text was adopted by the Plenary Meeting of the GNCHR on 22.7.2026. Rapporteurs: Professor Maria Gavouneli, President of the GNCHR and Dr Christos Tsevas, Human Rights Advisor of the GNCHR.



the GNCHR, presents its positions and recommendations, making a thematic separation of issues, as detailed below, while aiming at the follow-up of specific thematic reports, statements and other texts of the National Commission, which will focus on individual issues and provide a more comprehensive picture of each separate topic (e.g. labour and AI, migration and AI, gender and AI). In the same context, the GNCHR recognises the possibility of prioritising reports and actions relating to rights (e.g. right to work and AI, freedom of assembly and AI, freedom of expression and AI, etc.). In its first report on human rights and artificial intelligence, the GNCHR maps the relevant ecosystem and clarifies its own institutional role within it. It highlights the importance of protecting human rights in view of all these developments while underlying the challenges, prospects and related issues. It is important to emphasise that, for the purposes of this report, account has been taken of the recommendations and views expressed orally and in writing by stakeholders and persons during the hearing of stakeholders and persons organised by the GNCHR in January 2026, entitled “Artificial Intelligence and Human Rights”.² The hearing was organised on the basis of four thematic pillars and corresponding questions: (1) the relationship between AI and human rights; (2) challenges and perspectives; (3) procedures, tools and good practices; and (4) AI governance in Greece, taking into

-
2. GNCHR, [Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026. Participants included the Special Secretariat for Artificial Intelligence and Data Governance of the Ministry of Digital Governance and Artificial Intelligence; the Hellenic Data Protection Authority; the Hellenic Authority for Communication Security and Privacy; the National Council for Radio and Television; the National Cybersecurity Authority; the National Infrastructures for Research and Technology (GRNET S.A.); the Special Secretary for Long-term Planning; the National Commission for Bioethics and Technoethics; the Foundation for Research and Technology, Homo Digitalis, a non-profit civil society organisation; civil society actors and organisations participating in the network; [Greek Artificial Intelligence Network](#), the Hellenic Informatics Union; the Hellenic Artificial Intelligence Society; the Hellenic Association for the Protection of Personal Data and Privacy; the Labour Institute of the Greek General Confederation of Labour (INE GSEE); representatives of academia and the private sector; and members of the GNCHR.

account AI principles and a broad range of thematic fields of policy, administration and social action, as analysed below.



GNCHR, Hearing of stakeholders on Artificial Intelligence and Human Rights

In this context, the GNCHR takes into account **the international, European and national legal framework**, as examined in the relevant section, with a view to incorporating it at national level and, more specifically, to placing a human rights-based approach at the centre of Greece's approach to AI.

Furthermore, this report seeks to present and analyse the **perspectives and challenges associated with artificial intelligence in the light of human rights**. AI presents significant potential for social progress but also entails serious risks. Data are often described as the “new gold” for AI. Its effects are not neutral; they frequently have a disproportionate impact on specific groups, including women, children, migrants and persons with disabilities. For instance, in the world of work AI may increase productivity and create new forms of employment, but at the same time threatens jobs and raises issues of discrimination, transparency and information. From a gender perspective, algorithms often reproduce gender stereotypes, while the digital divide restricts women's ability to benefit from

AI. In the field of asylum and migration, the use of AI in screening, surveillance and asylum procedures increases the risk of arbitrary decisions, a lack of transparency and violations of the principle of non-refoulement. As regards children, AI can support learning and creativity, but entails risks of manipulation, violations of privacy and exposure to harmful content. Therefore, the need for a clear, human-centric and rights-based approach becomes imperative. Emphasis needs to be placed on the perspectives and challenges facing the national governance system of the AI and the protection of human rights, as well as on the international and European environment in which the above positive outcomes and risks are identified.

Additionally, this report highlights **the AI principles as guarantees for the protection of human rights**: a set of basic principles stemming from the European, national and international regulatory and ethical framework (United Nations, Council of Europe, European Union, UN Educational, Scientific and Cultural Organization (UNESCO), the Organisation for Economic Co-operation and Development (OECD), and national legislation). These principles constitute the cornerstone for the development and use of trustworthy AI compatible with human rights. In particular, we could focus on certain main principles of AI including:

1. Respect for human dignity: AI must not degrade human beings or turn them into objects of automated assessment.
2. Human-centric approach and human oversight: AI must support, rather than replace, human judgement. Human oversight safeguards human dignity and prevents arbitrary automation.
3. Transparency and explainability: Decisions made or supported by AI must be understandable and controllable. Transparency and explainability protect the right to information and to fair treatment.
4. Accountability: It must be clear who is responsible for the operation and consequences of AI systems.
5. Non-discrimination and algorithmic fairness: AI systems must be designed so as to avoid reproducing biases. Non-discrimination and algorithmic fairness are directly linked to the principle of equality.

6. Personal data protection and privacy: Any processing of data must comply with the principles of necessity, proportionality and safety. Data protection is a prerequisite for respect for privacy.
7. Safety and reliability: AI systems must operate in a safe and predictable manner.
8. Principle of proportionality and risk-based approach: The intensity of the arrangements and guarantees must correspond to the degree of risk to the rights.

The report in this section links the main principles of AI to a broad range of human rights which are put at risk or enhanced by the use of AI. The analysis demonstrates that AI principles and human rights do not constitute parallel, but rather interrelated, fields. Each AI principle operates as a mechanism for protecting specific rights. The rights concerned include, in particular: the right to human dignity; the right to private life and the protection of personal data; the right to non-discrimination and equality before the law; equality between women and men; the right to work and to fair and equal working conditions; the right to information, transparency and justification of decisions; the right to education; the rights of the child (protection, development and participation); the rights of migrants and refugees (access to asylum and protection against non-refoulement); the rights of persons with disabilities; the right to sound administration; and the right of access to services and social protection.

The section on the **added value of the GNCHR in the context of AI governance**, presents (a) the **competences of the GNCHR** on the basis of its legislation, as well as additional responsibilities arising from the national AI governance system, which are directly linked to the implementation of the international, European and national framework; (b) **the work of the GNCHR** in issues related to AI and new technologies, **which unfolds through a broad range of competences** as will be analysed below. That analysis will highlight relevant examples, the **tool-kit available to the GNCHR** and the tools that have been used to date (e.g. hearings of stakeholders and persons on human rights and AI, training activities), or may be used in the future (e.g. representation before courts and any domestic or

foreign authority; on-site investigations; requests to public services and private parties for any information, document or other evidence relating to the protection of human rights; and access to documents, including classified documents). **It is clear that, under its founding legislation, the GNCHR has enhanced competences to protect human rights** against the challenges posed by new technologies and AI. **Its added value lies in the connection of AI and human rights**, as illustrated, at an introductory level, by the following elements, which will be further analysed in the relevant chapter of this report:

1. The GNCHR is the official National Human Rights Institution (NHRI) in Greece (Article 10(2) of Law 4780/2021).
2. It is noted that the GNCHR has a pluralistic composition of 20 members designated by human rights organisations from across all fields, independent authorities, trade union organisations, higher education institutions, research institutions and bar associations, which enables it to foster a unique dialogue between the various civil society actors and the State and facilitates the role of the National Commission as a bridge between the state, society and citizens. The fact that the composition of the GNCHR –namely the Greek Ombudsman, the Hellenic Data Protection Authority (HDPa) and the Hellenic Authority for Communication Security and Privacy– which have been identified by the Ministry of Digital Governance as authorities responsible for the protection of fundamental rights under the EU AI Act, is indicative of the significance of the GNCHR work as reflected in its composition.
3. The above composition is further substantially expanded by the Racist Violence Recording Network, the Recording Mechanism of Informal Forced Returns, and the network of civil society actors participating therein.
4. The dynamics described above are utilised through the institutional capacity of holding hearings of stakeholders and persons, which contributes to the rapid acquisition of knowledge and assessment of each field in which the GNCHR is active [Article 18(4) of Law 4780/2021 and the GNCHR Regulation].

5. These dynamics are reinforced at European and international level through the GNCHR European and international representation within the European Network of National Human Rights Institutions (ENNHRI) and the Global Alliance of National Human Rights Institutions (GANHRI).

Finally, through this report, the GNCHR seeks to lay the foundations for the approach of the National Human Rights Institution to artificial intelligence issues and to make recommendations to the State. This final section includes recommendations to the State highlighting the positions of the GNCHR, which have been analysed in the preceding sections, as well as conclusions concerning the mapping of the main challenges and emerging perspectives for effective protection of human rights, as these stem from the use of AI in a wide range of policy, administration and social fields such as childhood, gender, disability, work, migration and asylum, justice, health, education and research, policing, democracy and elections, public administration, the environment.

The GNCHR report seeks to highlight the need for a coherent, binding and human-centric framework, in which technological innovation goes hand in hand with democracy, accountability and respect for human dignity. The present report is intended to serve as a **reference document** on human rights and AI to be followed by texts, reports, hearings, statements and other tools, related to the GNCHR's competences, in specific **thematic areas** in line with the priorities outlined above. AI can be a tool for social progress as long as human rights principles are embedded into its design.

CHAPTER 2

International, European and National Legal Framework

This section provides an indicative overview of key legal and policy instruments governing artificial intelligence at international, European and national level, examining how they relate to and help safeguard human rights. The purpose of focusing on the international, European and national context in this introductory section is not to analyse at this stage all the texts referring to AI but to outline the framework of those key texts that link human rights and AI. Moreover, starting from these instruments and throughout the reference report, it becomes evident that developments in binding texts but also in soft-law texts, reports, studies, findings, etc. accelerate in a very short period of time. Therefore, the purpose of this section is not to exhaustively mention and analyse all these texts but to provide an overview of the legal ecosystem at international, European and national levels. Account shall be taken, *inter alia*, of the following texts:

- The [UN Framework on Artificial Intelligence](#)³ and [UN Human Rights Conventions](#),⁴ especially the Convention on the Rights of the Child and the Convention on the Rights of Persons with Disabilities;
- The [European Convention on Human Rights](#) and the [European Social Charter](#);

3. UN, [Artificial Intelligence](#).

4. UN OHCHR, [The Core International Human Rights Instruments and their monitoring bodies](#).



- The [Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law](#)⁵;
- [Regulation \(EU\) 2024/1689 on Artificial Intelligence](#), Regulation (EU) 2026/1744 on the Digital Omnibus on AI, which simplifies the rules on AI, and all EU directives and texts on AI⁶;
- The [UNESCO Recommendation on the Ethics of Artificial Intelligence](#)⁷;
- The [OECD Recommendation of the Council on Artificial Intelligence](#)⁸
- National legislation including, *inter alia*, Law 4961/2022 (Official Government Gazette, A 146, 27 July 2022), “Emerging information and communication technologies, strengthening digital governance and other provisions”, and Law 5321/2026 (Official Government Gazette, A 114, 20 July 2026), “Measures for the Implementation of

-
5. CoE, [The Framework Convention on Artificial Intelligence](#).
 6. [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 \(Artificial Intelligence Act\)](#) . As regards Digital Omnibus on AI see. [Regulation \(EU\) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations \(EU\) 2024/1689, \(EU\) 2018/1139 and \(EU\) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence \(Digital Omnibus on AI\)](#) also indicatively: European Commission, AI Omnibus enters into force, July 2026, available here: <https://digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force>. As regards the legal framework of the regulations and texts see also indicatively: White Paper on Artificial Intelligence, 2020·European Commission, Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office, 24 January 2024; Commission Guidelines on transparency obligations for providers and deployers of certain AI systems, 20 July 2026; Commission Guidelines on the definition of an artificial intelligence system, February 2025 and for the rest: European Commission, Supporting the implementation of the EU AI Act with clear guidelines, 2025.
 7. UNESCO, [Recommendation on the Ethics of Artificial Intelligence](#), adopted on 23 November 2021.
 8. OECD, [Recommendation of the Council on Artificial Intelligence](#), adopted on 22 May 2019, amended on 3 May 2024.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act) – Amendment of Law 4961/2022 (Official Government Gazette, A, 146) and Other Provisions”;

- [The Blueprint for Greece's AI Transformation](#) of the High-Level Advisory Committee on Artificial Intelligence⁹.

ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΓΙΑ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΑΝΘΡΩΠΟΥ
ΚΥΚΛΟΣ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΣΕΜΙΝΑΡΙΩΝ

Η επόμενη μέρα των Δικαιωμάτων
Τεχνητή Νοημοσύνη - Βιωσιμότητα - Ασφαλιεποίηση

1ο Σεμινάριο - Τεχνητή Νοημοσύνη: Τα επίπεδα προστασίας
Δευτέρα, 29 Σεπτεμβρίου 2025, 17.00 - 19.00

*Σοφία Καστραντά, Νομικός Σύμβουλος Α' Ειδική Νομική Υπηρεσία ΥΠΕΣ
 Ευφροσύνη Σιουγλέ, Ειδική Επιπλήρωμα Πληροφορικής ΑΠΔΠΧ
 Ελευθέριος Χελιουδάκης, Διαηγόρος-Εκτελεστικός Διευθυντής της Homo Digitalis
 Χρήστος Τσεβάς, ΔΝ, Ειδικός Επιπλήρωμα, ΕΕΔΑ*

*Συντονίζει ο Γιάννης Ιωαννίδης, Α' Αντιπρόεδρος ΕΕΔΑ, Διαηγόρος
 Την εκδήλωση θα χαιρετήσει ο Πρόεδρος του ΔΣΑ Δημήτρης Βερβεσός*

Αίθουσα Εκδηλώσεων ΔΣΑ, Ακαδημίας 60, Αθήνα
**Οι συμμετέχοντες/ουσες θα λάβουν βεβαιώσεις παρακολούθησης*

ΕΕΔΑ, 1st Seminar of the GNCHR Educational Seminar Series entitled:
 “Artificial Intelligence: Levels of Protection”

More specifically, the **Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law**¹⁰ is the first international, legally binding convention in this field. Opened for signature on 5 September 2024, the Convention seeks to ensure that activities throughout the lifecycle of AI systems are fully consistent with human rights, democracy and the rule of law, while remaining conducive to technological progress and innovation. The Framework Convention complements existing international standards on human rights, democracy and the rule

9. High-Level Advisory Committee on Artificial Intelligence Blueprint, November 2024.

10. Council of Europe [Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law](#), 5 September 2024.

of law and aims to fill any legal gaps that may arise from rapid technological developments. Designed to remain relevant over time, the Framework Convention does not regulate technology as such and is essentially technology neutral. Within the Council of Europe ecosystem, the European Court of Human Rights (ECtHR) will play a pivotal role in cases concerning AI-related human rights issues¹¹. The GNCHR takes into account for the purposes of this report and in its work on human rights in general, the Handbook on Human Rights and Artificial Intelligence¹², a key tool of the Council of Europe, as it highlights international human rights standards and criteria and serves as a guide for states and national AI ecosystems.

The **Regulation (EU) 2024/1689 (EU AI Act)** is the first legal framework for AI, which addresses the risks of AI and enables Europe to play a leading role globally. The EU AI Act is the world's first comprehensive legal framework for AI. The rules laid down are designed, among other things, to foster trustworthy AI across Europe. The EU AI Act lays down a clear set of risk-based rules concerning specific uses of AI and forms part of a broader package of policy measures to support the development of trustworthy AI, including measures to boost innovation in the field of AI,¹³ to set up AI factories¹⁴ and implement the Coordinated Plan on AI¹⁵. Taken together, these measures guarantee safety, fundamental rights and human-centric AI, and strengthen the uptake, investment and innovation in AI throughout the EU. On the basis of the amendments to the Digital Omnibus on AI, of course, it is also necessary to take into consideration issues having an impact on the application of the Regulation and its timetable in practice since then, in the light

11. *Arnfinn Bårdsen, AI and Human Rights at the European Court of Human Rights* in *VerfBlog* 2025/12/08, 8 December 2025.

12. Council of Europe, CDDH, *Handbook – Human Rights and Artificial Intelligence*, April 2026.

13. European Commission, *Commission launches AI innovation package to support Artificial Intelligence startups and SMEs*, 24 June 2024.

14. European Commission, *AI Factories*, 23 April 2026 (last update).

15. European Commission, *Coordinated Plan on Artificial Intelligence*, 19 June 2023 (last update).

of what has been highlighted by different actors and as discussed in this report, in particular the issues related to the protection of personal data and privacy, AI literacy, etc¹⁶. To facilitate the transition to the new regulatory framework, the Commission launched the AI Pact¹⁷ in 2024 to help stakeholders prepare for the implementation of the EU AI Act. The first pillar of the Pact focuses on gathering and exchanging information with the AI Pact network, while based on the second pillar, companies providing or developing AI systems can demonstrate and share their voluntary commitments towards transparency and high-risk requirements and prepare early on for their implementation. It is important at this point to stress the risk-based approach (acceptable, high, minimum, zero), in particular Article 6 of the Regulation on classification rules for high-risk AI systems and Annex III. According to the Regulation, in Recital 48, the extent of the adverse impact of the AI system on the fundamental rights protected by the Charter is of particular importance for the classification of an AI system as high-risk. These rights include the right to human dignity; respect for private and family life; the protection of personal data; freedom of expression and information; freedom of assembly and of association; the right to non-discrimination; the right to education; consumer protection; workers' rights; the rights of persons with disabilities; gender equality; intellectual property rights; the right to an effective remedy and to an impartial tribunal; the rights of the defence and the presumption of innocence; and the right to good administration. Beyond these rights, it is important to emphasise that children have specific rights, as enshrined in Article 24 of the Charter and in the United Nations Convention on the Rights of the Child (UNCRC), which are further developed in General Comment No 25 of the UNCRC on children's rights in relation to the digital environment.

16. EDPB-EDPS, [Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence \(Digital Omnibus on AI\)](#), 20 January 2026. The contribution of Homo Digitalis was considered during the hearing of stakeholders on Artificial Intelligence and Human Rights. See [GNCHR Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026.

17. European Commission, [AI Pact](#), 9 June 2026 (last update).

Both provisions require that the vulnerable characteristics of children be taken into account and that the protection and care necessary for their well-being be provided. The fundamental right to a high level of environmental protection, as enshrined in the Charter and implemented through Union policies, should also be taken into account when assessing the severity of the harm that an AI system may cause, including, *inter alia* risks to the impact on the health and safety of persons.

Furthermore, special reference should be made to the **UNESCO Recommendation on the Ethics of Artificial Intelligence**. The Recommendation addresses ethical issues related to the domain of Artificial Intelligence to the extent that they are within UNESCO's mandate. It approaches AI ethics as a systematic normative reflection, based on a holistic, comprehensive, multicultural and evolving framework of interdependent values, principles and actions that can guide societies in dealing responsibly with the known and unknown impacts of AI technologies on human beings, societies and the environment and ecosystems, and offers them a basis to accept or reject AI technologies. It considers ethics as a dynamic basis for the regulatory assessment and guidance of AI technologies, referring to human dignity, well-being and the prevention of harm as a guiding principle for the ethics of science and technology. The Recommendation is addressed to Member States, both as AI Actors and as authorities responsible for developing legal and regulatory frameworks throughout the entire AI system life cycle, and for promoting business responsibility. However, what makes the Recommendation extremely useful is its wide-ranging Areas of Policy Action, which enable policymakers to translate core values and principles into action in relation to data governance, the environment and ecosystems, gender, education and research, the economy and work, health and social well-being, amongst many other areas.



*GNCHR, The GNCHR at the UNESCO Expert Roundtable
on Capacity Building for AI supervisory Authorities*

Another area that needs to be explored is the framework of the Organisation for Economic Co-operation and Development (OECD) and the **OECD Recommendation of the Council on Artificial Intelligence**. The Recommendation, the first intergovernmental standard on AI, was adopted by the OECD Council meeting at Ministerial level on 22 May 2019 on the proposal of the Digital Policy Committee (DPC, formerly the Committee on Digital Economy Policy, CDEP). The Recommendation aims to foster innovation and trust in AI by promoting the responsible stewardship of trustworthy AI while ensuring respect for human rights and democratic values. In June 2019, at the Osaka Summit, G20 Leaders welcomed the G20 AI Principles, drawn from the Recommendation. The Recommendation was revised by the OECD Council on 8 November 2023 to update its definition of an “AI System”, to ensure the Recommendation continues to be technically accurate and reflect technological developments, including with respect to generative AI. Based on the 2024 Report to the Council on its implementation, dissemination and continued relevance, the Recommendation was revised by the OECD Council meeting at Ministerial level on 3 May 2024 to reflect technological and policy developments, including with respect to generative AI, and to further facilitate its implementation.

At United Nations (UN) level, the UN Global Digital Compact provides a comprehensive global framework for digital cooperation and AI governance. Twenty years after the World Summit on the Information Society, the Compact sets out a roadmap for global digital cooperation, with a view to harnessing the immense potential of digital technology and bridging digital divides. On 22 September 2024, the Summit of the Future was held in New York, where the Pact for the Future, which includes the Global Digital Compact, was adopted. The Pact for the Future and its annexes –the Global Digital Compact and the Declaration on Future Generations– constitute the broadest international agreement designed to make the international system more inclusive, effective and fit for the challenges of the twenty-first century. It covers a broad range of issues, including peace and security, sustainable development, climate change, digital cooperation, human rights, gender, youth and future generations, as well as the transformation of global governance.



*GNCHR, The GNCHR in Parliament on the Ministry of Digital Governance
draft bill on artificial intelligence*

On the other hand, **national legislation** has been developing at a rapid pace and covers a range of different areas. More precisely, this legislation and policy will be discussed below in the relevant sections.

Law 4961/2022¹⁸, entitled “Emerging information and communication technologies, strengthening digital governance and other provisions”, laid the foundations for artificial intelligence, without covering a wide range of issues, such as those set out in the text of the aforementioned Regulation on AI. The purpose of that Law was to establish the appropriate institutional framework for the legitimate and secure use of the capabilities of artificial intelligence technology by public and private sector bodies, and to strengthen the resilience of public administration cyber threats. The section on artificial intelligence was intended to lay down provisions for appropriate safeguards to protect the rights of natural and legal persons and to strengthen accountability and transparency in the use of artificial and to supplement the current institutional framework for cybersecurity.

A recent legislative initiative related to the framework for emerging technologies, personal data and AI is Law 5169/2025¹⁹, concerning the ratification of the Protocol of 10 October 2018 amending the Council of Europe Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (data protection). The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and particularly his right to privacy, with regard to automatic processing of personal data relating to him.

An even more recent legislative initiative is Law 5321/2026 (Official Government Gazette, A 114, 20 July 2026), entitled “Measures for the Implementation of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act) – Amendment of Law 4961/2022 (Official Government Gazette A 146) and other provisions”, which repeals specific provisions

18. [Law 4961/2022](#), Official Government Gazette A 146/27.7.2022, “Emerging information and communication technologies, strengthening digital governance and other provisions”.

19. [Law 5169/2025](#), Official Government Gazette A 4/17.1.2025, «Ratification of the Protocol of 10 October 2018 amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (data protection).

of Chapter B (“Arrangements for the Development of AI”) and amends Law 4961/2022. Consequently, where Law 4961/2022 is referred to in this report, it is taken into account in respect of the period and the provisions that were in force, and for the purposes of commenting thereon in relation to the corresponding issues – for example, the framework of principles in the respective chapter and the manner in which those principles had been incorporated into that Law. As regards matters relating to Law 5321/2026, the GNCHR has submitted comments and made a public statement before the Standing Committee on Public Administration, Public Order and Justice of the Hellenic Parliament²⁰.

20. GNCHR, [The GNCHR in Parliament on the Ministry of Digital Governance draft bill on artificial intelligence – Submission of Memorandum](#), 13 July 2026. See also the relevant analysis in the section referring to the role of the GNCHR.

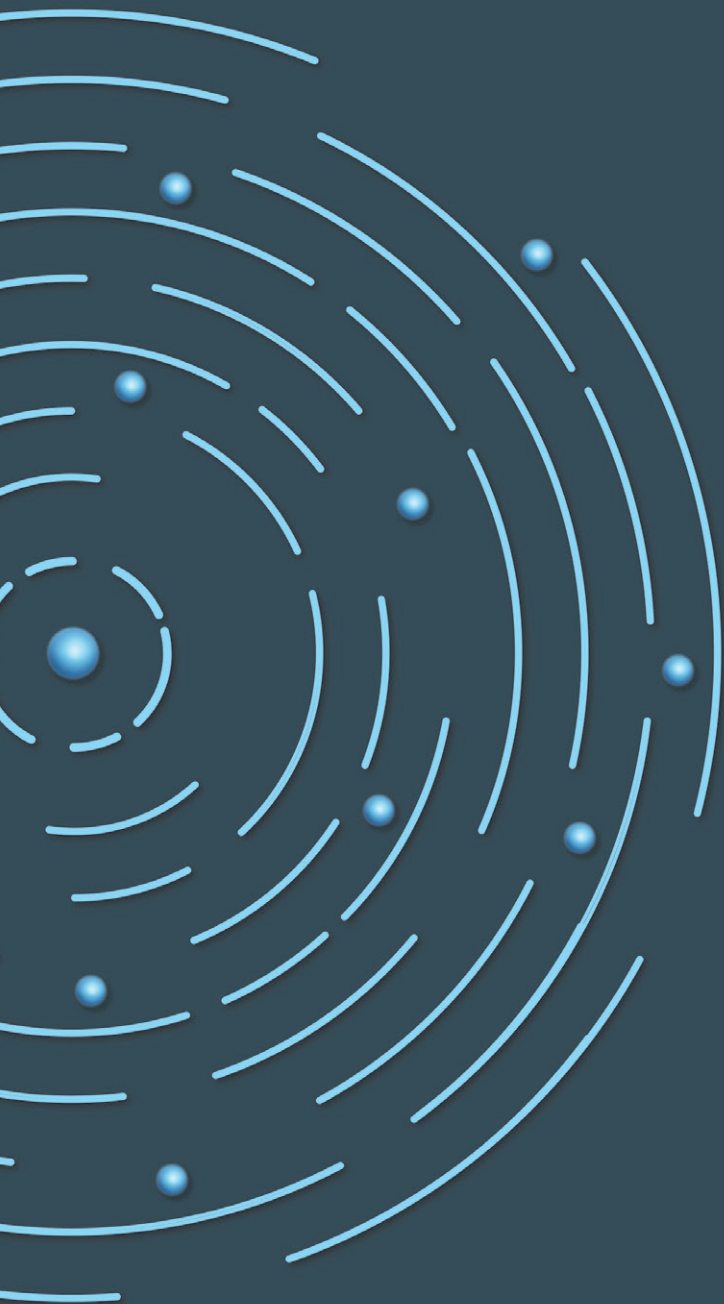
CHAPTER 3

Perspectives and Challenges in the light of Human Rights

3.1 Introduction

The rapid development and integration of artificial intelligence systems into critical areas of social, economic and political life creates new opportunities, but also poses complex challenges for the protection and promotion of human rights. The use of algorithmic systems in decision-making directly affects fundamental rights, such as the right to privacy, the right to work, access to justice and the right to a fair trial. As technology becomes increasingly autonomous and applies to a wider range of fields, the need arises to consider it not only as a tool for innovation and efficiency, but also as a factor that reshapes the framework for the protection of human rights, that is, as a technology which, depending on how it is used, may advance the protection of human rights, or it could lead to human rights violations.

Artificial intelligence offers the potential to improve the efficiency of services, reduce the administrative burden and facilitate faster decision-making, particularly in areas such as employment, justice, migration and public administration. At the same time, however, the use of algorithms carries the risk of reproducing or even exacerbating existing inequalities and discrimination, particularly to the detriment of vulnerable groups, such as children, women, refugees and migrants, persons with disabilities and socially excluded groups. The lack of transparency in algorithmic processes, data bias and



the limited scope for challenging automated decisions raise serious issues regarding accountability and the rule of law.

In that light, analysing the perspectives and challenges of AI requires a human rights-based approach that places the individual at the heart of technological transformation. The incorporation of principles such as non-discrimination, transparency, proportionality and meaningful human oversight is a crucial prerequisite for the legitimate use of AI in various areas. This chapter examines the key challenges and opportunities arising in the separate thematic areas, highlighting the importance of a coherent regulatory and ethical framework that will ensure that artificial intelligence serves as a means of empowering, rather than undermining, human rights. The following analysis does not aim to provide an exhaustive overview of the perspectives and challenges posed by artificial intelligence, but rather to focus on those relating to human rights.

3.2 Work and artificial intelligence

3.2.1 Introduction

Work is a fundamental social right and constitutes a source of income, an essential element for the development of the individual's personality, the fulfilment of individual aspirations, social inclusion and decent living conditions. The world of work is being reshaped by technological developments. While these developments offer considerable opportunities for innovation and productivity, they may also threaten the very existence of work in all of its forms, since these systems reinforce the employer's managerial authority using sophisticated technological means for the digital monitoring of the performance of work²¹.

Artificial intelligence has become part of the world of work and employment relationships and will shape a different framework of challenges and prospects, generally and specifically with regard

21. Theodosis, G., "Artificial Intelligence and the Constitutional Protection of Labour", in E. Stylianidis (ed.), *Artificial Intelligence: Human Rights, Democracy and the Rule of Law*, 2025, pp 452-462 (pp. 452-453).

to human rights. It is likely to change the design and content of jobs, interactions among workers, and the ways in which their performance is monitored; it may also support skills development, raise productivity and improve job quality.

According to the International Labour Organization (ILO)²², in the world of work, there are two distinct types of application of AI technology in the workplace. The first is directed at automating tasks that workers perform; the second is to use AI-based analytics and algorithms to automate managerial functions - or what is commonly referred to as “algorithmic management”. When AI is used to automate tasks, it does not necessarily lead to redundancies, as the technology can also complement human labour when certain tasks are automated. Whether technological adoption leads to automation (job loss) or augmentation (job complementarity) depends on the centrality of the automated task to the occupation, how the technology is integrated into work processes and management’s desire to retain humans to perform or oversee some of the tasks, despite automation’s potential. As AI transforms occupations, a workforce equipped with necessary skills in machine learning (ML), data science, and AI ethics is crucial for harnessing its potential.

3.2.2 Challenges associated with human rights

The following challenges may result in potential infringements of rights under the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the European Social Charter (ESC), among other texts. In particular infringements may involve: the right to work (Article 6 of the ICESCR, Article 1 of the ESC), just and favourable conditions of work (Article 7 of the ICESCR, Articles 2–4 of the ESC), freedom of association and collective bargaining (Article 8 of the ICESCR, Articles 5–6 of the ESC), social security and social protection (Article 9 of the ICESCR, Articles 12–14 of the ESC), protection of health (Article 12 of the ICESCR, Article 11 of the ESC), the right to education (Articles 13–14 of the ICESCR, Articles 9–10, 15 and 17 of the ESC), protection of the family, children and young persons (Article 10 of the ICESCR,

22. ILO, [Artificial Intelligence](#).

Articles 16–17 of the ESC), protection of elderly persons (Article 23 of the ESC), protection of persons with disabilities (Article 15 of the ESC), protection against discrimination and equal opportunities in employment (Articles 20 and 26 of the ESC), protection against poverty and social exclusion (Article 30 of the ESC), participation in cultural life (Article 15 of the ICESCR).

According to the ILO²³ the uneven adoption of Artificial Intelligence (AI) is a critical issue that goes beyond economic growth. It impacts global equity, fairness and the social contract that is at the heart of social justice. Disparities in access to robust infrastructure, advanced technology, quality education and training are deepening existing inequalities. As the global economy increasingly shifts towards AI-driven production and innovation, less developed countries risk being left further behind, exacerbating economic and social divides. The relevant Report on the Digital Divide emphasises the importance of targeted and concerted efforts to bridge this digital divide, so as to ensure that AI is able to promote sustainable development and alleviate poverty. It further highlights the role of the workplace in the adoption of AI, where productivity gains and improved working conditions can be realised there only if the necessary conditions are in place, including digital infrastructure, relevant skills and a culture of social dialogue that fosters a positive integration of technology. The GNCHR stresses that these developments will have tangible consequences for particular groups, including young workers, older persons²⁴ and women, as well as persons in vulnerable situations,

23. UN/Office of the Secretary-General's Envoy on Technology – ILO, *Mind the AI Divide – Shaping a Global Perspective on the Future of Work*, 2024, pp. 6, 13 et seq.

24. The term 'older persons' follows UN terminology: UN, UN Principles for Older Persons, 16 December 1991, available on: <https://www.ohchr.org/en/instruments-mechanisms/instruments/united-nations-principles-older-persons>, UN Economic and Social Council, General Comment No. 6. The Economic, Social and Cultural Rights of Older Persons, E/1996/22, UN Committee on Economic, Social and Cultural Rights (CESCR), 8 December 1995. Independent Expert on the enjoyment of all human rights by older persons, Ageism and age discrimination, UN Doc. A/HRC/48/53, 4 August 2021, paragraph. 21, available on: <https://>

such as refugees and migrants. This assessment should also take account of the issues the GNCHR has highlighted in relation to the protection of social rights in the context of digitalisation and artificial intelligence²⁵. The GNCHR has observed that the use of digital tools based on new technologies, including AI-based tools²⁶, needs to facilitate improved information-sharing with workers, employers, other competent or jointly competent public services and the public, by automating the generation of reports²⁷, while at the same time addressing significant challenges, such as transparency, access and accountability.

Therefore, AI is expected to have a significant impact on the world of work²⁸. AI is expected to affect almost half of global employment, bringing both opportunities and challenges. Unlike traditional automation, which has generally focused on well-defined tasks and reducing manual work, AI is expected to affect highly skilled jobs as well as a far broader range of sectors, including transport and the automotive industry, healthcare, agriculture, finance, defence, education and entertainment. More than half of all jobs in developed economies with the greatest exposure to AI are expected

digitallibrary.un.org/record/3938306?ln=en&v=pdf. Where the report refers to provisions containing the term 'elderly', this term is used (see for example ESC, the Charter).

25. Among others, [The GNCHR Observations on the bill of the Ministry of Labour and Social Insurance entitled "Fair Work for All: Simplification of Legislation – Support for Workers – Protection in Practice"](#), October 2025, pp. 32 et seq.⁴⁰ and GNCHR, [Comments by the GNCHR to the European Committee of Social Rights on the 7th National Report on the implementation of the European Social Charter Articles 2, 3, 4, 5, 6, and 20](#), June 2026, p. 31.
26. ILO, [AI provides innovative ways to improve compliance with labour laws](#), 3 February 2025 and ILO, [Strengthening labour inspection systems for increased compliance with labour law through development cooperation](#), p. 6.
27. ILO, [Transformative Technology for Decent Work \(TT4DW\)](#).
28. High-Level Advisory Committee on Artificial Intelligence Blueprint, November 2024 p. 66 et seq. with reference to the findings of a Goldman Sachs study: Goldman Sachs, Global Macro Research, [Generative AI: Hype, or Truly Transformative?](#), Top of Mind, Issue 120, 5 July 2023.

to experience its effects. Approximately half of these economies are expected to benefit from increased productivity, while the remainder may face reduced demand, lower wages and job losses.

According to the OECD²⁹ workers may need to re-skill or up-skill in order to adapt to the reorganisation of tasks and the emergence of new tasks, and to weather potential job loss and navigate transitions to new jobs. This does not simply mean acquiring AI-related skills but also acquiring skills in areas that AI cannot perform so well, such as creative and social intelligence, reasoning skills, and dealing with uncertainty. The smoothness of the transition to AI and the extent of its impact on workers will also depend on whether undertakings have incentives to retain and retrain staff, and on institutional factors, such as the general infrastructure for training and job search available in the country, direct government funding, tax incentives and social benefit systems³⁰. The framework and ecosystem in question are also directly linked to innovation and entrepreneurship objectives³¹, as well as to the manner in which rights arising from employment relationships –and, more broadly, social and economic rights– are respected, on the basis, *inter alia*, of the protection instruments of the UN and the Council of Europe, and the conventions of the ILO.

Moreover, according to the aforementioned Blueprint for Greece's Transition to the Age of Artificial Intelligence prepared by the High-Level Advisory Committee on Artificial Intelligence and coordinated by the Special Secretariat for Foresight of the Presidency of the

29. OECD, [The impact of Artificial Intelligence on the labour market](#), 25 January 2021.

30. In addition to the OECD study referred to above, see also Thanos, I. and Kapoutsis, I. (2024) [Future of Jobs, 2024 Greece](#), Future of Jobs, 2024 Greece, supported by the Special Secretariat of Foresight, concerning policy proposals on: education and skills training; investment in AI infrastructure –including the development of a national strategy for AI infrastructure, with particular emphasis on supporting small and medium-sized enterprises (SMEs)– and addressing demographic challenges.

31. High-Level Advisory Committee on Artificial Intelligence [Blueprint for Greece's AI Transformation](#), November 2024 p. 36 et seq.

Government³², AI in the world of work should not be seen as a tool for replacing people. Instead, it should be treated as a technology that enhances human capabilities and opens new avenues for human–AI collaboration. The proposal of the said Committee calls for the enhancement of labour legislation to protect work from the new reality introduced by AI and to ensure Greece’s timely alignment with the provisions of the EU AI Act relating to the use of AI in the world of work. The GNCHR endorses the Committee’s proposal according to which, where Greece has regulatory discretion, it is necessary to introduce legislation to protect workers’ rights and to set out a clear regulatory framework for the development and implementation of the AI.

According to the ILO³³, technological advancements can also lead to work intensification, job insecurity and “technostress”, as workers face increasing pressure to adapt to rapidly evolving tools and processes. Intrusive surveillance and constant monitoring may infringe on privacy and reduce job autonomy. As workers spend more time using digital tools, they may be increasingly exposed to cyberbullying. AI-driven decision-making risks task fragmentation, loss of job satisfaction and bias, potentially marginalizing certain groups and exacerbating inequalities in the workplace.

The GNCHR highlights the risk of bias and discrimination in the workplace, particularly during the recruitment process. According to the European Union Agency for Fundamental Rights (FRA)³⁴, in addition to the principle of non-discrimination, the use of AI systems may also affect other rights enshrined in the Charter of Fundamental Rights of the European Union, such as freedom of thought, conscience and religion (Article 10), freedom to choose an occupation and right to engage in work (Article 15), rights of the elderly (Article 25), workers’ right to information and consultation within the undertaking (Article 27), right to collective bargaining and

32. *Ibid.* pp 81-85.

33. ILO, [Global Report – Revolutionizing health and safety: The role of AI and digitalization at work](#), 2025, p. 5. See also United Nations, [Artificial Intelligence, Global Issues – AI and workers](#).

34. FRA, [Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks](#), 2025, pp. 41-42.

action (Article 28), right of access to placement services (Article 29). Of particular importance are also the right to privacy (Article 7), right to data protection (Article 8), non-discrimination (Article 21), equality between men and women (Article 23), integration of persons with disabilities (Article 26), right to an effective remedy (Article 47). These rights must be taken into account when carrying out a Fundamental Rights Impact Assessment (FRIA) for high-risk AI systems used in employment, such as systems for the AI-based search engine for recommending, ranking or shortlisting job applicants; the AI system for supporting hiring decisions by assessing the cognitive, social and emotional competencies of candidates; and the AI system for recommending jobs to jobseekers based on their background, preferences and other input.

3.2.3 Perspectives and recommendations

According to the ILO³⁵, AI and digital tools offer businesses significant opportunities to enhance occupational safety and health (OSH). When effectively designed and implemented, these technologies help mitigate occupational risks, reduce accidents at work and diseases and improve efficiency, productivity and overall performance. By removing workers from hazardous environments, automating repetitive or demanding tasks, and improving the organisation of work, digital technologies reduce both physical and mental strain, while AI-based systems can identify hazards, monitor working conditions and predict potential equipment failures. At the same time, they can support the continuous enhancement of workers' skills so that they can respond to the new requirements of work.

AI has the capacity to process large volumes of data in a short time, drawing conclusions and providing valuable insights that support evidence-based decision-making. One of its advantages is the automation of repetitive tasks, which increases operational efficiency and allows workers to focus on more complex activities. At the same time, it helps reduce operating costs by optimising operational

35. ILO, [Global Report – Revolutionizing health and safety: The role of AI and digitalization at work](#), 2025, p. 5.

procedures and limiting human error. Finally, tools such as chatbots and virtual assistants offer faster and more personalised customer service.

The GNCHR stresses that: (i) workers and job applicants must be informed whenever AI systems are used in decisions affecting their employment; (ii) they should have access to meaningful information on the role of AI in the decision-making process; (iii) a publicly accessible register of entities and organisations using AI systems in work environments should be established, including the purpose of use and key rights-protection measures³⁶; (iv) an effective right to appeal against decisions supported by or taken using AI should be enshrined; (v) workers should be able to request a review by a human being and a adequate reasoning of the decision; (vi) meaningful human oversight should apply to every use of an AI system in recruitment, evaluation of employees promotion, task allocation and disciplinary procedures; (vii) a fundamental rights impact assessment should be carried out before AI systems are developed or used; (viii) training programmes should be developed for workers, employers and public authorities on the capabilities, limitations and risks of AI; and (ix) international standards and relevant conventions on AI and labour must be ratified and implemented with a view to protecting workers' rights.

3.3 Artificial intelligence in the health sector

3.3.1 Introduction

Major technological breakthroughs in AI systems have the potential to advance biomedicine and benefit healthcare, yet uncertainty exists about their impact and direction of developments. AI systems are being developed for a variety of applications, encompassing ancillary applications, such as the automation of routine administrative tasks, but also applications of significant impact on the provision of quality

36. See for instance the reference in Republic of Croatia – Ombudswoman, [Discussion on Algorithmic Discrimination in the Labour Market](#), 20 May 2026 and [Discussion on the Impact of Digital Algorithms on Work and the Protection of Workers' Rights](#), 20 January 2026.

health services and a patient's treatment, that could be regulated as medical devices at national level, such as in radiology imaging. Key AI use cases include medical diagnostics; predictive analytics; personalised medicine: AI systems; virtual health assistants; remote monitoring and telemedicine; AI-powered wearable devices and telehealth platforms enabling patient monitoring; robotic surgery; process management; medical device development; mental health support³⁷. As AI systems are becoming an essential tool in modern medicine, the therapeutic relationship – particularly the patient-doctor relationship – remains a critical component of good patient care which such systems have the potential to improve or adversely affect³⁸. Accordingly, attention should focus both on the patient-doctor relationship in the context of AI and, more broadly, on healthcare and the use of AI systems within it.

3.3.2 Challenges associated with human rights

One of the most significant challenges concerns the use of health data by AI systems, including its potential links to infringements of the right to privacy and to a lack of transparency. The development and use of AI in health care may place a range of human rights at stake, notably the rights to privacy and data protection; the prohibition of discrimination; the right to health; the right to information; and the right to autonomy and physical integrity.

Data used for training, testing and the continuous improvement of AI systems should be representative, accurate and of high quality, in order to mitigate bias and ensure the reliable performance of algorithms. Moreover, because such datasets often contain sensitive personal data –including personal data concerning health– their processing must comply with the applicable legal and regulatory

37. Council of Europe, CDDH, [Handbook – Human Rights and Artificial Intelligence](#), 2026, p. 70 *et seq.*

38. Council of Europe, Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), [The application of Artificial Intelligence in Healthcare and its Impact on the 'Patient-Doctor' Relationship](#), September 2024. World Economic Forum, [How will generative AI impact healthcare?](#), 12 May 2023.

framework³⁹. Appropriate safeguards, including anonymisation and pseudonymisation, should be applied to protect privacy and prevent the identification or re-identification of patients.

A major challenge lies in ensuring that AI systems (their data and models) are empirically sound and robust, accurate, and their results consistent and reproducible (e.g., based on independent standards or expertise, such as independently tested algorithms). Standards for clinical trials involving AI systems are necessary to ensure the safety, quality and reliability of trial results. This will allow AI systems to be more easily appraised by investigators and others, such as regulators⁴⁵, forming part of a chain of responsibility for AI systems (especially as they self-improve). Care and standards should not waiver when AI systems are introduced. The challenge lies in understanding how these standards are applied and should adapt to safeguard the therapeutic relationship. This includes how to address the benefits and risks of AI systems considering their opacity (i.e. 'black box'⁴⁶ algorithms) and other shortcomings in transparency and reproducibility⁴⁰.

As AI systems train, share and infer new patterns and findings from these data, greater implications for privacy are likely to emerge. At its

39. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ([General Data Protection Regulation](#)), [Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data](#), Law 4624/2019 (Official Government Gazette A 137 29.8.2019 Law [5169/2025](#)(Official Government Gazette A 4 17.1.2025) Ratification of the Amending Protocol of 10 October 2018 to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. See also WHO, [Regulatory considerations on artificial intelligence for health](#), October 2023, p. 32 *et seq.* See National Commission for Bioethics and Technoethics , [Opinion on Artificial Intelligence Applications in Greece](#), 10.1.2024, 10.1.2024.

40. Council of Europe, Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), [The application of Artificial Intelligence in Healthcare and its Impact on the 'Patient-Doctor' Relationship](#), September 2024. p. 7.

root, the role played by health professionals and healthcare providers in collecting, generating and enriching, as well as safeguarding health data, becomes ever more important. For example, the protection and respect for privacy in and out of healthcare settings is a cause for concern. One arrangement between a company and healthcare institution provider may result in the company gaining access to a vast number of patient records. Without the patients' knowledge or consent, this agreement may result in a breach of data protection legislation⁴¹. The aggregation of data on platforms used to train AI systems presents a significant challenge that must be addressed in terms of transparency regarding the collection and use of data, whilst also taking into account issues of bias and discrimination against specific groups of people with particular characteristics (e.g. gender, ethnic origin, skin colour)⁴².

According to the Council of Europe⁴³ equitable access to AI-enabled care will be challenged where its deployment is geographically uneven across health settings in any given country leading to inequities in access to health care. Other inequities may result when such access is dependent on the financial means of individuals. A 'two-tier' access to care could occur; the wealthier having access to human doctors, the less wealthy having access to AI enabled chatbots or conversely, not having access to the latest AI developments such as robotic surgery. These differences in access could be further compounded should AI systems act as a gatekeeper in determining care needs and treatments.

These risks and requirements must also inform the deployment of healthcare systems such as the Digital Doctor Assistant⁴⁴ particularly

41. *Ibid* p. 22. See the case in Alex Hern, "[Royal Free breached UK data law in 1.6m patient deal with Google's DeepMind](#)", The Guardian, July 2017.

42. *Ibid*. pp. 26-27. See case of US health-care system at WHO, [Ethics and Governance of Artificial Intelligence for Health](#), 28 June 2021, p. 54, box 6: Discrimination and racial bias in AI technology.

43. *Ibid* 24 *et seq*.

44. Ministry of Digital Governance and Artificial Intelligence, [The Digital Doctor Assistant Is Operational in the National Electronic Health Record – Artificial Intelligence Is Being Used in the Health Sector](#), 30 October

where doctors may use the Digital Doctor Assistant through myHealthDoc to obtain immediate information from the patient's record, including a personalised view based on the rapid analysis of medical history, examinations and medication, and can request a summary medical overview of the patient. The same applies to the Citizen Personal Health Assistant⁴⁵; to the project "Review and Optimisation of Prescribing Rules through Artificial Intelligence" of IDIKA S.A. (Electronic Governance of Social Security Single-Member S.A.)⁴⁶; and to the cooperation of the Ministry of Health for the integration of AI into triage and coordination processes, where *"the aim is to increase service capacity, improve response times and provide consistent support nationwide, while at the same time strengthening the resilience of the service against sudden increases in demand"*⁴⁷. These systems, together with other systems in the health sector which may meet needs related to the protection of the right to health, facilitate and/or accelerate diagnosis, or even assist with the management of the bureaucratic needs of health structures and staff, are at the same time required to ensure safeguards for the

2025. See related references regarding the ERTRIAGE system: Medical Association of Trikala [Pioneering ERTRIAGE System with Artificial Intelligence at the General Hospital of Larissa](#), 23 September 2025.

45. Ministry of Digital Governance and Artificial Intelligence, The Citizen Personal Health Assistant – MyHealth Agent Presented by the Ministers of Health, Adonis Georgiadis, and Digital Governance and AI, Dimitris Papastergiou – Citizens Ask, the MyHealth Agent Responds with AI and Information from Their Health Record, 11 December 2025.
46. Ministry of Health, [Decision -No A3a/Γ.Π. οik. 17784 "Second Amendment to the Action 'Review and Optimisation of Prescribing Rules through Artificial Intelligence", Project Code 5225536, Health Sectoral Development Programme 2021–2025"](#) 21 April 2026. IDIKA S.A., Tender Notice for the project "Review and Optimisation of Prescribing Rules through Artificial Intelligence", 24 September 2025. IDIKA S.A. is jointly monitored and supervised by the Ministers of Digital Governance and Health, according to their respective competences. See also Law 5263/2025. Hellenic Informatics Union, Press ["Review and Optimisation of Prescribing Rules through Artificial Intelligence"](#), 7 April 2025.
47. Ministry of Health, [Key Points from the Ministry of Health Press Conference concerning the "Entry" of Artificial Intelligence Tools into the National Health System](#), 24 November 2025.

protection of fundamental rights, the protection of health data and its sharing in accordance with the criteria of international, European and national legislation, with due respect for safety mechanisms⁴⁸, as well as the principles of human oversight and explainability, amongst others.

The United Nations High Commissioner for Human Rights⁴⁹ has underlined that “digitality”, by contrast, describes a structural condition in which health systems become datafied and algorithmically mediated, health governance relies on digital infrastructures and platforms, health identities are increasingly constructed through data profiling and predictive analytics, system resilience depends on cybersecurity and technological integrity, and private technology actors exercise significant influence over public health governance. Under conditions of digitality, States’ obligations extend beyond regulating individual technologies. They must ensure that the broader socio-technical architecture governing health systems comply with international human rights law.

3.3.3 Perspectives and recommendations

According to World Health Organization (WHO)⁵⁰ AI offers immense opportunities to improve health outcomes (*via* early disease detection, prediction, etc.), as well as enhance health services (*via* optimized resource allocation, behaviour change interventions, etc.), in pursuit of global health equity. Moreover, AI can augment and complement the capacities of health workers as well as empower individuals and communities to take charge of their own health. The WHO envisages a future in which digital health will serve as a tool

48. See the decisions, opinions, guidelines and recommendations of the Hellenic Data Protection Authority (HDPa): HDPa, [Acts of the Authority – Thematic Category: Health](#).

49. OHCHR, [The right to health in conditions of digitality](#).

50. WHO, [Leading the Future of Global Health with Responsible Artificial Intelligence](#), 2024. See WHO, [Artificial Intelligence for Health](#), 2024. See WHO, [Global Initiative on AI for Health](#).

for innovation, equity and ethical integrity in healthcare. The overall objective is to enable improved, sustainable and smarter healthcare.

The integration of AI into evidence-informed policymaking presents substantial benefits, as it can enhance every stage of the policy cycle –by expanding and accelerating the generation of evidence, supporting the synthesis of diverse sources, and enabling more timely and adaptive responses to complex challenges in the field of health⁵¹. Consequently, on the basis of the above, the right to health, the provision of information to patients and access to necessary treatment may be more fully exercised, while the competent State mechanism may also respond more effectively in policymaking guided by the ethics of AI. AI systems may help mitigate existing biases identified in contemporary medicine and offer options for addressing discrimination in access to healthcare among groups such as older persons, persons from lower socioeconomic groups and minorities.

Notwithstanding the potential for AI systems to be effective supporting tools (a form of augmented intelligence for health professionals), the critical thinking and expertise of health professionals should not be underestimated. A responsible approach to AI should place humans (i.e. patients) at the centre and should align with stakeholder expectations, as well as applicable regulations and laws⁵². Furthermore, traditional medicine can make a significant contribution both in terms of its links with conventional medicine and with regard to sexual and reproductive health and rights⁵³. The GNCHR stresses that, in cases of predictive analytics in healthcare, the design of protocols, the training of all health professionals in the proper communication of

51. WHO, [Artificial Intelligence and Evidence-Informed Policy – Emerging Challenges and Opportunities](#), Discussion Paper, 2026.

52. Council of Europe, Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), [The application of Artificial Intelligence in Healthcare and its Impact on the 'Patient-Doctor' Relationship](#), September 2024, p. 18.

53. WHO, [Mapping the application of artificial intelligence in traditional medicine: technical brief](#), July 2025. WHO, [The role of artificial intelligence in sexual and reproductive health and rights](#), March 2024.

information to patients, and the definition of technical requirements for the transparency and explainability of decisions generated through predictive analytics methods in medicine constitute important criteria for the proper implementation of AI⁵⁴.

3.4 Artificial intelligence in the sector of justice

3.4.1 Introduction

The application of AI in justice system extends from support for legal research and judicial case management to the use of predictive tools and legal-data analytics. These developments highlight the potential of technology to contribute to a more efficient administration of justice, while at the same time raising significant issues related to lawfulness, transparency, the protection of fundamental rights and the role of the human factor in judicial decision-making. Consequently, the assessment of the prospects and challenges associated with the use of artificial intelligence in the administration of justice has become a matter of particular academic and institutional interest.

The integration of AI into the justice system affects the way in which judges, lawyers and other justice professionals perform their duties. Such tools may support the processing of legal information, case-law research and judicial case management; they must not, however, replace the human role in judicial decision-making. This development highlights the need to ensure that technology is used properly and responsibly, so that the functioning of the judicial system continues to be based on the fundamental principles of independence, impartiality and the protection of citizens' rights.

Bearing in mind that the process of reaching a judicial decision is divided into stages and that at each of these stages an AI system can intervene independently and provide its information, for the time being, the complete replacement of a human judge by a machine seems

54. National Commission for Bioethics and Technoethics of Greece – Cyprus National Bioethics Committee, [Joint Opinion of the National Commission for Bioethics and Technoethics of Greece and the Cyprus National Bioethics Committee, on the Ethics of Predictive Analytics in Healthcare](#), 2024.

rather dystopian, given the complexity of legal reasoning, the rules that the legal practitioner is called upon to interpret, and the uniqueness of the facts and circumstances in the course of proceedings⁵⁵.

3.4.2 Challenges associated with human rights

The use of AI in the field of justice is accompanied by a series of challenges relating to the operation and reliability of the relevant systems. According to the mapping carried out by the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ)⁵⁶, one of the most significant challenges concerns the potential production of false, inaccurate or misleading information, known as "hallucinations", whereby AI systems generate information that appears plausible without corresponding to reality. At the same time, the risk of unintentional biases being embedded during the training of models has been highlighted; this may lead to unintentional discrimination or reinforce existing cognitive biases. These issues may have serious implications, for example, at the level of judicial decisions and of the general functioning of the justice system.

Further concerns arise in relation to data protection and confidentiality, as the use of algorithms –particularly in cloud environments– may result in the disclosure of sensitive information. At the same time, the absence of references or supporting documentation for the answers generated gives rise to concerns regarding the verification of information, while potential risks of infringement of intellectual property rights have also been identified. Generative AI systems do not always ensure that they will provide the same answer to identical questions, while they may produce repetitive or similar outputs.

55. Sarmas, I. & Kourakis, N. Artificial Justice? Challenges and possibilities of Artificial Intelligence in the administration of (Criminal) Justice, Criminal Law, Issue 99, 2025. Sarmas, I notably invokes the words of the Chief Justice of the United States, on 31 December 2023: "I predict that human judges will be around for a while ", a fact which alarms judges about the replacement of their role by AI.

56. Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), [Note on the Use of Generative Artificial Intelligence \(AI\) by Judicial Professionals in a Work-related Context](#), 12 February 2024.

The stability and reliability of generative AI models may also vary, particularly in critical or time-sensitive processes. Over-reliance on technology without the application of critical human thinking can also result in improper usage. The rapid advancement of A.I. algorithms may lead to uncontrolled or excessive usage (hyper abuse) without adherence to all the in-house good-practice rules. Unfortunately, A.I. can provide new tools for sophisticated cyberattacks, enabling impersonation and data pollution that can be exploited by malicious actors⁵⁷.

When private sector technology is used, including in the public sphere, questions of accountability and transparency may arise due to the secretive nature of these algorithms. Members of the public often lack insight into the decision-making processes and therefore struggle to challenge outcomes. This hinders their right to be heard the right to an effective remedy⁵⁸ and their right to a fair trial and due process of law⁵⁹.

The right to legal protection is guaranteed by Article 20(1) of the Constitution of Greece, while Article 8 of the Constitution of Greece safeguards the principle of the natural judge—that is, the right of every person to have his or her case heard by a judge designated by law. The relevant protection is further reinforced by European instruments, and specifically by Article 6(1) of the ECHR.

The use of AI during judicial proceedings may place certain fundamental principles at risk. Automated data-processing methods may rapidly identify relevant case-law and legislation, but they may also encourage standardised approaches to cases whose circumstances are materially different.

Entrusting criminal, or even administrative, proceedings to generative AI would be incompatible with the guarantees of the Universal

57. CJEU, [Artificial Intelligence Strategy](#), 9 November 2023, p. 4.

58. ENNHRI, [Key human rights challenges of AI](#).

59. Council of Europe, [Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques and possible regulatory implications](#), 2018, pp. 10-12, 23-26 (on «effective remedy»).

Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), which require a public hearing before an independent and impartial tribunal, conducted in conditions of equality. AI software cannot be independent, as it depends on the data with which it has been trained and, on that basis, produces statistically and probabilistically plausible outputs. Those outputs may, however, reproduce or embed bias.

3.4.3 Perspectives and recommendations

Article 8 of the Constitution safeguards the right of every citizen to have his or her case heard by the natural judge designated by law. The principle of the natural judge is directly linked to judicial independence and the administration of justice, which constitute foundations of our constitutional order and so the possibility of creating computer systems that would exercise judicial functions must be rejected; however, in cases involving complex case files containing a large number of documents, AI could contribute to their classification according to their nature. AI could also help identify and classify documents as material or immaterial, thereby supporting legal professionals in a task that is often time-consuming⁶⁰. Generative AI has significant potential in tasks carried out within clearly defined parameters. It may, for example, be used to translate texts between languages; generate coherent text, images or audio; automatically summarise lengthy materials; analyse and identify views or opinions; undertake text mining; and facilitate access to content⁶¹.

In the field of justice⁶², AI can be leveraged to improve the efficiency and effectiveness of administrative and judicial processes, enhance the quality and consistency of judicial decisions, and increase access

60. Grivas G., “The Impact of Artificial Intelligence on the Principle of the Lawful Judge”, in E. Stylianidis (ed.), *Artificial Intelligence: Human Rights, Democracy and the Rule of Law*, 2025, pp. 204-210 (p. 206).

61. Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), [Note on the Use of Generative Artificial Intelligence \(AI\) by Judicial Professionals in a Work-related Context](#), 12 February 2024.

62. CJEU, [Artificial Intelligence Strategy](#), 9 November 2023, p. 3 and Sarmaş, I. & Kourakis, N. Artificial Justice? Challenges and possibilities of

to justice and transparency *vis-à-vis* EU citizens while strengthening transparency. As regards procedural efficiency, several examples include the detection of references in documents, suggesting metadata, proposing subject matters during case logging, and generating transcripts of hearings through speech-to-text algorithms. Besides automation, A.I. could soon be available for more advanced support: search engines that understand context, summaries of large documents proposed by a machine, or anonymisation algorithms. In the administrative realm, we could witness improved support for building operations, automation in financial processes (such as automatic invoice handling), and the integration of virtual assistants into our daily tools. These virtual assistants could assist in scheduling meetings, preparing presentations and documents, and composing response emails, among other tasks.

The quality and consistency of judicial decisions could also be enhanced through this technology by enabling automatic correlation and classification of cases, automating the processing of originating documents, and potentially employing advanced legal research tools as technology evolves. AI can contribute to judicial decision-making, for example through software that understands and processes the parties' claims; software that detects the rule of law applicable to the case and interprets it in relation to the facts; software that searches for the truth of the parties' factual claims, providing significant assistance in better assessing the factual circumstances without replacing the human judge in gathering and assessing evidence; software that subsumes factual circumstances under the applicable rule of law through the forward-chaining method, thereby achieving subsumption of facts under the legal rule; and software that carries out balancing exercises to find the point of fair balance⁶³.

Artificial Intelligence in the administration of (Criminal) Justice, *Poinika*, Issue 99, 2025, footnote 1, pp. 8–13.

63. Sarmas, I. & Kourakis, N. Artificial Justice? Challenges and possibilities of Artificial Intelligence in the administration of (Criminal) Justice, *Criminal Law*, Issue 99, 2025. It is difficult for AI to carry out so many and such significant balancing exercises taking into account multiple criteria, for example the best interests of the child. In this case too,

At the same time, AI can contribute to improving access to justice and transparency *vis-à-vis* citizens. In particular, for persons with disabilities, applications can be used, such as automatic subtitles in online-streamed court hearings and virtual assistants that provide information via audio or video in the user's language. Furthermore, systems such as chatbots, virtual assistants and digital avatars (AI avatars) can support both citizens and legal professionals in searching for information or in providing legal advice in standardised cases. At the same time, advances in translation and interpretation technologies are expected to help reduce language barriers. Predictive justice tools –including applications that estimate the likely judicial decisions, assess the prospects of success of a claim or appeal, support informed access to justice, or assist in the preparation of standardised judicial decisions– as well as other existing or future AI systems in the justice sector, require further clarification, assessment and rights-based safeguards. Their use must not compromise the specific rights and principles analysed in this report.

In practice, the Ministry of Justice and the Ministry of Digital Governance and Artificial Intelligence have introduced Artificial Intelligence in the justice system for the automatic translation of judicial documents, the interpretation and recording of testimonies of foreign witnesses, and the recording of oral speech in judicial proceedings. In particular, under the Memorandum of Understanding signed between the Ministry of Justice and the National Network of Infrastructure for Technology and Research (EDYTE S.A.), a body of the Ministry of Digital Governance, it is provided that systems for the automatic translation of judicial decisions in language pairs (e.g. Italian, English, Chinese, Arabic) will be developed, together with systems that will record the testimony of foreign witnesses and translate the text into the corresponding language, and systems that can be used by judicial bodies and entities for the recording of oral

where software is concerned, AI is not yet in a position to make such specific assessments; however, it can provide auxiliary support to the judicial decision making by proposing alternative solutions.

speech in judicial proceedings⁶⁴. Additionally, in 2024, the Ministry of Justice⁶⁵ had pre-announced the “application of AI in judicial systems”, in particular: the upgrading and extension of functionality of the integrated information systems of civil, criminal and administrative justice; the use of AI in the anonymisation of judicial decisions; the use of AI in small-claims cases (up to a certain amount), in summarising judicial decisions and creating keywords; in supporting the production, analysis and organisation of information in specific workflows; and in controls of automated payment processes. The safeguarding of human rights and guarantees is among the issues discussed by the Standing Scientific Committee of the Ministry of Justice on AI⁶⁶. The GNCHR stresses that, where issues pertaining to human rights are discussed, the National Commission should be included among the members of that Committee so as to contribute a relevant opinion.

64. Ministry of Digital Governance and Artificial Intelligence, [Justice is being digitally upgraded with Artificial Intelligence systems](#), 15 April 2025.

65. Toulas, M. (Head of the Directorate of e-Governance of the Ministry of Justice), [Application of Artificial Intelligence in Justice](#), March 2024, Mentioned, among others, are the upgrading and extension of functionality of the Integrated Case Management System of Civil and Criminal Justice Phase II – Recovery Fund, 2023–2026), the digital upgrading of the Integrated Case Management System of Administrative Justice (NSRF 2023–2026), and the development of an Integrated Information System (OPS) for the modernisation of the operation of the Court of Audit (2023–2025).

66. See Ministry of Justice, Standing Scientific Committee of the Ministry of Justice on AI, [Minutes](#) especially the most recent from the meeting on 19 February 2026.

3.5 Artificial intelligence in the field of asylum and migration

3.5.1 Introduction⁶⁷

AI is emerging as an increasingly important tool in asylum and migration management, with applications ranging from the processing of applications and risk assessment to border management and the analysis of large amounts of data. Although these technologies may improve efficiency, speed and consistency in administrative decision-making, they also raise serious human rights concerns⁶⁸. Issues such as the opacity of algorithms, the risk of discrimination and biased decisions, the protection of personal data, and the safeguarding of the right to an effective remedy and human oversight make it necessary to develop a robust regulatory and ethical framework. The GNCHR takes the view that, in the right conditions of transparency, accountability and compliance with international and European human rights law, AI can be a powerful tool assisting the competent authorities, without, however, replacing the individualised assessment required to protect asylum seekers, refugees and migrants.

67. The contribution of the Greek Forum of Migrants and of the non-profit organisation “I Have Rights” was considered during the hearing of stakeholders on Artificial Intelligence and Human Rights. See GNCHR [Greek National Commission for Human Rights, Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026.

68. European Parliament, [Artificial intelligence in asylum procedures in the EU](#), Briefing, July 2025. OSCE/ODIHR, [Border Management and Human Rights](#), 2021. PICUM – ECRE, [Beyond walls and fences: EU funding used for a complex and digitalised border surveillance system](#), June 2024. Amnesty International, [Primer: Defending the rights of refugees and migrants in the digital age](#), 5 February 2024. The interest and the tendency to address these issues can also be seen in the ongoing FRA study entitled: [«Use of artificial intelligence in asylum and immigration procedures – fundamental rights implications»](#), which is going to be published in 2027.



*GNCHR, The GNCHR at the OSCE seminar
on Human Rights and New Technologies at Borders*

Since its establishment, the GNCHR has consistently addressed asylum and migration issues. Moreover, in recent years, it has been monitoring developments, issued comments and made recommendations to the State on the intersection between AI and the rights of asylum applicants, refugees and migrants⁶⁹. The GNCHR takes into account that AI systems used in migration,

69. GNCHR “Refugees – Migrants” and “Artificial Intelligence” fields. See for instance: GNCHR Greek National Commission for Human Rights, [Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026. GNCHR, [The GNCHR at a parliamentary committee meeting on the draft bill of the Ministry of Migration and Asylum](#), 29 August 2025. GNCHR, [The GNCHR at an OSCE seminar on Human Rights and New Technologies at Borders](#), 28 March 2025. GNCHR, [The GNCHR is hosting a meeting of the ENNHRI Working Group on Asylum and Migration at its premises](#), 29 May 2023. GNCHR, [The GNCHR at the OSCE seminar on Human Rights and New Technologies at Borders](#), 28 March 2025. GNCHR, [GNCHR Online Conference on the application of the Charter of Fundamental Rights of the EU in cases involving applicants for international protection](#), 11 June 2024. GNCHR, [The GNCHR at the ENNHRI Co-Lab Event on Artificial Intelligence and Human Rights \(Ljubljana, Slovenia, 30 November–1 December 2023\)](#), 4 December 2023.

asylum and border control management affect persons who are often in particularly vulnerable positions and who are dependent on the outcome of the actions of the competent public authorities⁷⁰. Consequently, the accuracy, impartiality and transparency of AI systems used in these contexts are particularly important in ensuring respect for the fundamental rights of the persons concerned, especially their rights to freedom of movement, non-discriminatory treatment, protection of private life and personal data, international protection and sound administration. These considerations become even more pressing as the Pact on Migration and Asylum⁷¹ is implemented, particularly at the intersection of the relevant EU regulations and directives, national legislation, the EU AI Act, and applicable international, European and domestic legal frameworks.



*ENNHRI, The GNCHR at the ENNHRI Co-Lab Event
on Artificial Intelligence and Human Rights*

70. See EU AI Act recital 60.

71. See for instance: GNCHR, [GNCHR observations on the draft bill from the Ministry of Migration and Asylum](#), 5 June 2026. GNCHR, [The new EU Pact on Migration and Asylum: The role of the GNCHR](#), 5 May 2026. GNCHR, [The GNCHR at the meeting “Independent Monitoring of the New Pact on Migration and Asylum – Review and Planning for the Future”](#), 15 December 2025. GNCHR, [The President of the GNCHR on the new EU Pact on Migration and Asylum](#), 12 April 2024. Homo Digitalis, [Joint Statement on the draft bill ‘Implementation of the Pact on Migration and Asylum’ and the use of AI in asylum procedures](#), 8 June 2026.

3.5.2 Challenges associated with human rights

According to Annex III⁷² high-risk AI systems also include systems related to migration, asylum and border control management, in so far as their use is permitted under relevant Union or national law. The GNCHR stresses that the EU AI Act⁷³ itself emphasises that the use of AI systems in migration, asylum and border control management should not, under any circumstances, be used by Member States or Union institutions, bodies, offices or agencies as a means of circumventing their international obligations under the United Nations Convention relating to the Status of Refugees, done at Geneva on 28 July 1951, as amended by the Protocol of 31 January 1967. Nor should they be used to violate, in any manner, the principle of non-refoulement or to deprive persons of safe and effective legal pathways into the territory of the Union, including the right to international protection. Consequently, any such use constitutes a serious breach.

According to the International Organization for Migration (IOM)⁷⁴, the growing collection, storage and use of data for migration and asylum management—particularly biometric data, satellite data and large-scale data (big data)—enhances the efficiency of administrative procedures, but at the same time increases risks to the rights of migrants and asylum applicants. At the same time, weak data-protection and cybersecurity practices may expose

72. See paragraph 7 of Annex III (for example AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies 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; AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, 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.) and amendments on the basis of “Digital Omnibus on AI”.

73. See EU AI Act recital 60.

74. IOM, [World Migration Report 2022: Chapter 11 - Artificial intelligence, migration and mobility: implications for policy and practice](#), 2022, p. 17, 19.

migrants and asylum applicants to serious risks, including the disclosure of sensitive information and to serious infringements of privacy, particularly where private companies are involved without adequate safeguards. Moreover, limited transparency in the development and use of AI systems for migration management—often justified by security considerations or the need to guard against cyberattacks—hampers the effective monitoring of their operation and may undermine fundamental human rights, such as the right to the protection of personal data, non-discrimination and a fair administrative procedure.

It is therefore clear that AI may place at risk a number of rights protected under international and European instruments, notably the right to asylum, the principle of non-refoulement and protection in the event of removal, expulsion or extradition, as provided for in Articles 18 and 19 of the Charter. Furthermore, serious implications may also arise for the right to liberty enshrined in Article 6 of the Charter (e.g. if an AI system contributes to decisions to (continue to) detain asylum seekers);— the protection in the event of removal, expulsion or extradition enshrined in Article 19 of the Charter (e.g. if an AI system contributes to decisions to deny applications, relevant considerations for the applicants' protection would need to be taken into account) ;— equality before the law enshrined in Article 20 of the Charter (e.g. if an AI system contributes to comparable situations being treated differently, such as who is considered to be part of a family unit when determining who qualifies for international protection) ;— equality between men and women enshrined in Article 23 of the Charter(e.g. if an AI system contributes to gender inequality) ;— the rights of the elderly enshrined in Article 25 of the Charter (e.g. if an AI system directly or indirectly discriminates against the elderly) — the integration of persons with disabilities enshrined in Article 26 of the Charter (e.g. if the use of an AI system leads to direct or indirect discrimination against persons with disabilities) (55);— the right to good administration enshrined in Article 41 of the Charter and as a general principle of EU law (e.g. if the use of an AI system presents a barrier to accessing documents or giving reasons for

decisions)⁷⁵. Additionally, a key conclusion is that the growing impact of technologies on the human rights of migrants demonstrates the need for further engagement by human rights defenders, including NHRIs, in this emerging area⁷⁶.

3.5.3 Perspectives and recommendations

Considering the above, as well as the perspectives for the use of AI in this field, a human-rights-based approach is needed to ensure guarantees that reflect the protection needs of refugees, migrants and asylum-seekers, in line with the principles of artificial intelligence. For instance, human rights impact assessment tools could be used before the deployment of AI systems. This would increase algorithmic fairness and accountability and prevent situations in which AI technologies are tested on vulnerable populations, such as migrants and refugees, without prior assessment of the risks. Adherence to the “do no harm” imperative during the design, development and deployment of AI systems could help to mitigate some of the risks brought about by these technologies throughout the migration cycle⁷⁷.

Recognising the profound impact that AI can have on individual rights and liberties, the Assembly stresses that AI should support – not replace – human decision making in migration and asylum processes, even if in some cases AI may offer greater security and effectiveness than human decision making alone, by reducing the

75. FRA, [Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks](#), 2025, pp. 37-38.

76. ENNHRI, [ENNHRI scoping paper, Technologies, migration, and human rights: the role of European NHRIs](#), September 2024, p. 30, which was developed by ENNHRI’s Asylum and Migration Working Group under the chairmanship of the Head of the GNCHR Scientific Unit.

77. IOM, [World Migration Report 2022: Chapter 11 - Artificial intelligence, migration and mobility: implications for policy and practice](#), 2022, p. 9-10, 17. See also UNHCR, [Explainer: How UNHCR is using AI to support refugees and improve operations](#), 9 July 2026.

scope for human error⁷⁸. All mechanisms must be transparent, reliable, subject to oversight, and developed in accordance with key international instruments, including the ICCPR, the ECHR, the 1951 UN Convention relating to the Status of Refugees and the European Charter of Fundamental Rights.

According to the above, at the arrival stage, AI can contribute to individualised, fair and fundamental-rights-compliant asylum procedures, without, however, replacing the role of competent officials in interactions with applicants and in decision-making. Documents produced with the use of AI should be available in the language of the applicants and drafted in a clear and comprehensible manner.

At the same time, biometric systems and language recognition tools should be subject to regular audits to detect and address possible bias, to ensure equal treatment. Conversely, the use of technologies such as emotion recognition or lie detectors should not be permitted, and predictive tools assessing the likelihood of absconding should not be used as a basis for imposing detention, particularly in the case of minors. Therefore, it is important that AI systems in migration and asylum procedures undergo human rights, democracy and rule of law impact assessments before their deployment⁷⁹.

AI labour-matching tools should prioritise ethical criteria such as family unity and cultural fit. Gender-sensitive design is essential to avoid reinforcing labour market segregation that directs women into low-wage sectors⁸⁰. Continuous feedback loops should help address misplacements. Annual audits of AI systems used in welfare and housing are essential to detect and correct bias. Predictive analytics can support equitable urban planning, helping to prevent segregation and foster innovation and safety in diverse communities

Finally, AI chatbots used in return support programmes should comply with fairness standards, avoid nudging techniques and

78. Council of Europe, Parliamentary Assembly, [Resolution 2628 \(2025\) Artificial intelligence and migration](#), 36th sitting, 3 October 2025.

79. See above for the Council of Europe's HUDERIA methodology.

80. See Council of Europe, Parliamentary Assembly, [Resolution 2628 \(2025\) Artificial intelligence and migration](#), 36th sitting, 3 October 2025.

provide unbiased information. Moreover, migrants, refugees and asylum seekers should retain control over their data, with the ability to delete or transfer information upon exiting programmes and a guarantee against the sharing of biometric information with the country of origin.

Therefore, the opportunities offered in this field must be accompanied by specific safeguards for the protection of fundamental rights. The GNCHR welcomes the proposals of the Parliamentary Assembly of the Council of Europe to the Committee of Ministers to ensure that migration-policy tools incorporate robust and effective safeguards for the protection of fundamental rights, and to promote the drafting of a code of good practices for the use of AI in migration management and in procedures concerning those populations. It is also recommended that awareness-raising and training programmes on the impacts of AI be developed, with a view to strengthening the capacity of human rights institutions, competent authorities and civil society organisations to ensure effective respect for human rights⁸¹.

More specifically, the Ministry of Migration and Asylum has incorporated the REACTION project into its activities⁸²; REACTION is a European project aiming to improve surveillance of the EU's external borders through the use of AI technologies and the analysis of data from remotely piloted aircraft systems (RPAS), for the early detection of critical situations, so as to provide substantial assistance to border-management which is of vital importance and may also have an impact on human lives. According to the project information, it will utilise intelligent algorithms in order to make use of the large volume of data collected by law-enforcement agencies through heterogeneous sensors—including optical, thermal and multispectral cameras, LIDAR and others—and to transform these data into useful information for strengthening border surveillance and improving emergency response. REACTION will also be integrated with, and interconnected to, the

81. Council of Europe, Parliamentary Assembly, [Recommendation 2300 \(2025\) Artificial intelligence and migration](#), 36th sitting, 3 October 2025.

82. Ministry of Migration and Asylum, [Specific Action REACTION: Realtime Artificial Intelligence for Borders Surveillance via RPAS data analytics to support Law Enforcement Agencies](#), Specific Action BMVI 2021-2027.

information platforms already deployed at Reception and Identification Centres (RICs) and at the Evros Border Guard Post.

Furthermore, it is important to take into account the combination of projects involving new technologies⁸³, including the Ministry's projects entitled, "Centaur", which uses cameras and Artificial Intelligence Behavioural Analytics algorithms, and "Hyperion", which is an integrated entry–exit control system at the facilities of Closed Controlled Access Centres (CCACs) and Reception and Identification Centres (RICs), as well as any violations already identified by independent authorities⁸⁴, as lessons for the future. It should also be emphasised that guarantees for the protection of fundamental rights must be in place whether or not the actions are financed through

-
83. See among others ALKYONI II and Smart Policing projects in BVMN, [Surveillance Technologies at European Borders: Evros](#), 1 October 2024. See also the European project entitled, [Intelligent Portable Border Control System](#) (2016-2019) with the participation of Greek partners.
84. Hellenic Data Protection Authority, [Administrative fine and order to comply with the GDPR issued to the Ministry of Migration and Asylum in the context of the Authority's own-initiative inquiry](#), 3 April 2024. The HDPa imposed an administrative fine totalling EUR 175,000 on the Ministry of Migration and Asylum for the infringements identified in relation to its cooperation with the Authority and the Data Protection Impact Assessments. At the same time, it issued an order requiring the Ministry to comply, within three months, with its obligations under the GDPR. HDPa, [Own-Initiative inquiry into the development and deployment of the "Centaur" and "Hyperion" projects by the Ministry of Migration and Asylum for the control of reception and accommodation facilities for third-country nationals](#), 2 April 2024. See Ministry of Migration & Asylum, [Centaur & Hyperion Systems in the Reception and Identification Centres FRIA](#), updated version 11 January 2024. Homo Digitalis, [Homo Digitalis, Request to the Hellenic Data Protection Authority concerning the procurement and deployment of intrusive surveillance systems in reception and accommodation facilities for asylum applicants](#), 18 February 2022. I Have Rights - BVMN, [Controlled and Confined: Unveiling the Impact of Technology in the Samos Closed Controlled Access Centre](#), 2025. I Have Rights – Homo Digitalis, ["They never tell us anything" Ongoing Data Rights Violations in the Samos CCAC](#), 29 May 2025. Amnesty International, [Samos: Unlawful detention and sub-standard conditions must not become a blueprint for the EU Migration Pact](#), 25 February 2025.

specific European programmes, in accordance with the conditions for monitoring those actions and the Charter of Fundamental Rights of the European Union.

3.6 Education, research and artificial intelligence

3.6.1 Introduction

The rapid development of AI is transforming the educational landscape, creating new opportunities to improve learning processes, personalise teaching and enhance access to knowledge. AI applications can support learners, teachers and educational institutions, improving teaching effectiveness and broadening opportunities for lifelong learning. At the same time, the increasing integration of these systems in education raises significant challenges in terms of transparency, accountability, the reliability of algorithmic systems and the protection of personal data.

The development and use of AI in education should be grounded in respect for fundamental rights, with particular emphasis on the right to education, the principles of equality and non-discrimination, the protection of privacy and personal data, and children's rights, as set out in the UN Convention on the Rights of the Child. In this light, it is necessary to develop an appropriate regulatory and ethical framework that ensures AI is used in a way that complements the pedagogical role of teachers, promotes equal access to education and contributes to creating a safe, inclusive and trustworthy educational environment. The GNCHR emphasises that the key direction that needs to be taken is the promotion of education through a human rights-based digital transformation⁸⁵.

3.6.2 Challenges associated with human rights

According to the EU AI Act, AI systems⁸⁶ used in education or vocational training, in particular for determining access or admission, for assigning persons to educational and vocational

85. Council of Europe, [Education Strategy 2024-2030](#), March 2024.

86. See recital 56.

training institutions or programmes at all levels, for evaluating learning outcomes of persons, for assessing the appropriate level of education for an individual and materially influencing the level of education and training that individuals will receive or will be able to access or for monitoring and detecting prohibited behaviour of students during tests should be classified as high-risk AI systems, since they may determine the educational and professional course of a person's life and therefore may affect that person's ability to secure a livelihood. 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 and 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. They may also give rise to risks for the right to an effective remedy and to effective judicial protection, the right to good administration, and other fundamental rights⁸⁷.

Despite the significant opportunities that AI offers in education, its integration comes with challenges that require particular attention. The integration of AI in education comes with challenges related to privatisation and the increasing dependence of the educational process on digital platforms. Moreover, a particularly worrying tendency is the widening of the digital divide. Factors such as income, cultural background, gender, level of education, family circumstances, language, and residence in urban or rural areas affect equitable access to digital technologies. Inadequate connectivity, limited access to suitable equipment and insufficient digital literacy, all exacerbate the risk of falling further behind for learners without high-speed Internet or personal devices.

At the same time, AI changes the way that education is delivered and assessed, diverting traditional classroom methods towards personalized learning, automated assessments and data-driven learning analytics. However, the growing reliance on algorithmic

87. FRA, [Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks](#), 2025, p. 39, table 4.

systems may limit teachers' pedagogical role and lead to a weakening of their professional autonomy, particularly when educational and pedagogical decisions are heavily influenced by algorithms. However, over-reliance on technology can encourage students to rely on AI formulaic answers, limiting active participation in the learning process, inhibit critical thinking and reduce reasoning and synthesis skills. The widespread use of automated text-generation applications may also adversely affect the development of writing skills and creative expression. Concerns have also been raised about the possible effects of AI use on learners' well-being and mental health.

Moreover, the wider integration of AI applications in the educational process raises issues concerning the protection of privacy and personal data. The extensive collection and processing of data through educational platforms, school management systems, social networks and messaging applications increases the risk of unauthorised surveillance and of limiting users' anonymity. The continuous generation and use of educational data may broaden the access of public and private actors to personal information relating to learners and educators.

Algorithmic bias and the dissemination of inaccurate information pose further major challenges. Algorithms are not neutral, since they are influenced both by their training data and by the choices of the persons who design and evaluate them. As a result, social groups with a limited digital presence may be underrepresented in data sets, which may lead to biased outcomes. At the same time, general-purpose AI systems and generative AI models may amplify disinformation or generate inaccurate content, since they do not always provide accurate, reliable or appropriately adapted information to the cognitive level of learners, creating a risk of disseminating incorrect or misleading information and making it necessary to maintain human oversight and pedagogical guidance. Consequently, using generative AI or conversational tutors in education without critical oversight may impact the type of information and disinformation to which learners and educators are exposed.

The UN Special Rapporteur on the right to education and the Special Rapporteur on the rights of persons with disabilities and the

European Disability Forum, *inter alia*, are concerned that AI systems discriminate against individuals with asymmetrical or atypical facial features and different gestures, speech impairment and divergent communication patterns, as well as physical disabilities, cognitive and sensory impairments and autism spectrum disorders⁸⁸. Categorizing disability-specific issues and assessing potential risks, especially in education, is essential.

3.6.3 Perspectives and recommendations

Indeed, Artificial Intelligence Literacy and digital skills in general are among the most fundamental prerequisites for the exercise of the rights of all those within a country's territory, including citizens, refugees and migrants. Consequently, it is also a key element in the strategic planning that the state must take into account. The Council of Europe introduces a three-dimensional model of AI literacy encompassing the human, technological and practical dimensions of AI⁸⁹. Central to the model is the primacy of the human dimension, which addresses the ethical, socio-political, cognitive, cultural and environmental implications of AI, including its impact on fundamental rights and democratic participation.

With a view to preparing everyone for the use, potential and challenges of AI, it is important to introduce AI at all levels of education, so that pupils and students may develop critical thinking and computational skills, enhance their productivity and creativity, and improve their adaptability to technological change. Artificial intelligence in education may foster a better understanding of the ethical issues arising from its use and of ways to address them, both of which are critical to the responsible development and use of AI. It is becoming increasingly clear that teachers need to be fully trained in the concepts

88. Special Rapporteur on the right to education, [Artificial intelligence in education](#), A/79/520, 16 October 2024, paragraph 21. Homo Digitalis, [We submitted our report to the UN Special Rapporteur on the right to education regarding the use of AI in education](#), 3 June 2024.

89. Council of Europe, [The Steering Committee for Education \(CDEU\) approves a landmark framework on AI Literacy](#), 27 March 2026.

and fundamental principles of AI as well as in the use of AI tools, as the latter can be used to improve the effectiveness of education, personalise the learning experience and enhance students' active participation. The competent ministries and authorities must provide teachers with the necessary knowledge and skills. Finally, AI tutoring systems, or AI tutors, that support learners in learning at their own pace and receiving personalised feedback, while defining the areas in which only teachers can make an irreplaceable contribution to the learning experience. Furthermore, the use of AI systems in accordance with the above prospects must also be linked to addressing matters of data protection and ensuring their impartiality.

UNESCO adopts a human-centric approach to AI, seeking to harness it to reduce inequalities in access to knowledge and education, without widening the digital and technological divide between States and social groups⁹⁰. Within the framework of the Beijing Consensus on Artificial Intelligence and Education, UNESCO issued Artificial Intelligence and Education: Guidance for policy-makers⁹¹ calling on States to develop comprehensive and ethically grounded strategies for integrating AI into education, in line with United Nations Sustainable Development Goal 4 on quality education. It is recommended that AI be utilised to improve educational administration, teaching and the learning process, without replacing the role of teachers, whilst at the same time emphasis is put to the need for their continuous professional development. At the same time, UNESCO developed competency frameworks for students and teachers⁹², with a view to understanding both the potential and risks of AI. These frameworks focus on cultivating a human-centric perspective education on ethical issues and the responsible use of AI, the acquisition of basic knowledge of its applications, and the

90. UNESCO, [Artificial intelligence in education](#). UN, [Artificial Intelligence](#). UNESCO, [AI and the future of education. Disruptions, dilemmas and directions](#), 16 January 2026.

91. UNESCO, [Beijing Consensus on Artificial Intelligence and Education](#), 2019. UNESCO, [AI and education: guidance for policymakers](#), 2021.

92. UNESCO, [AI competency framework for students](#), 2024, p. 86.

development of skills, promoting the integration of relevant subjects across all fields of learning.

Therefore, the use of AI in education concerns the design of educational policies, the improvement of educational administration and service delivery, the support of teaching and learning, the development of skills for the AI era and the assurance of lifelong learning. At the same time, there is a need to promote equitable and inclusive access, gender equality, the ethical, transparent and secure use of data and algorithms, and systematic monitoring, assessment and international cooperation.

The GNCHR recommends the development of comprehensive policies for integrating AI into education, focused on supporting – rather than replacing– the work of educators, enhancing the skills of teachers and learners, and promoting lifelong learning. It is also proposed that AI be used to improve teaching, assessment and educational administration, while ensuring equitable access for all learners. Finally, stress is placed on the need to establish an appropriate regulatory framework that will guarantee transparency, the protection of personal data, the prevention of discrimination and the ongoing assessment of the impact of digital technology on education. The development of digital skills, digital literacy and the responsible use of technology must be given particular emphasis, along with ensuring transparency, accountability, the protection of privacy and respect for human rights.

The GNCHR underlines that the legal framework governing AI and digital education must be continuously updated so as to align with evolving human rights standards. This includes embedding core AI principles –such as transparency, accountability and fairness – in the development and deployment of artificial intelligence. In an increasingly digitalised environment, and as AI continues to develop in education, the right to education cannot be left solely to market forces or technological development; states must act to ensure inclusive and equitable digital education that is free from undue commercial influence, with preventive legal safeguards against algorithmic bias, data exploitation and threats to educational

autonomy⁹³. The policy framework for the use of generative AI should include, *inter alia*, the promotion of inclusion, equity, and linguistic and cultural diversity; the protection of human agency; the monitoring and validation of GenAI systems for education; the development of competencies, including GenAI-related skills for learners; and the promotion of plural opinions and plural expressions of ideas⁹⁴.

Technical and vocational education and training (TVET) institutions must prepare learners for r changing occupational tasks and skill requirements by applying key ethical principles that should govern any institutional AI strategy in the context of training, such as human agency, equity, fairness and non-discrimination, pedagogical purposefulness transparency and explainability, accountability, and protection of personal data⁹⁵.

A central recommendation of the GNCHR is to ensure that the development and use of AI in education are based on respect for human rights. States bear primary responsibility, but international organisations, civil society organisations, businesses—including technology companies— educational institutions and citizens themselves also have an important role in adopting a human rights-centric approach. Bridging the digital divide must also be a priority, so that all learners have equal access to the opportunities offered by artificial intelligence. The active participation of stakeholders, particularly educators, in the design and implementation of AI policies is equally important. The use of these applications should be aligned with educational objectives and should serve the learning process. It should also be guided by applicable ethical frameworks, including the 2021 UNESCO Recommendation on the Ethics of Artificial Intelligence and the relevant principles of the OECD Recommendation on Artificial Intelligence.

93. UNESCO, [AI and education: Protection the rights of learners](#), 25 September 2025.

94. UNESCO, [Guidance for generative AI in education and research](#), 2024.

95. UNESCO, [Integrating AI in TVET: A practical guide for institutions](#), 3 July 2026, p. 19.

The GNCHR also stresses the need for a robust legal and policy framework governing the use of AI in education, since the importance of effective regulation is internationally recognised. It is further proposed that AI literacy be promoted among all participants in the educational process and that the right to a fair procedure be recognised where decisions are made or supported through AI systems. Finally, the impact of AI on education should be systematically monitored and assessed to ensure its safe and effective implementation. At the same time, the importance of international cooperation and the exchange of best practices is highlighted, with a view to promoting common approaches and the responsible use of AI in the education sector.

The GNCHR welcomes the inclusion of digital skills and competences, as well as AI and its implications for education, among the national strategic priorities of the Digital Transformation Bible 2026–2030⁹⁶. According to the Bible⁹⁷, teacher training in digital technologies and the use of AI in teaching and learning is being strengthened through the Artificial Intelligence in Secondary Education programme, under which approximately 400 teachers from 20 Model, Experimental and Public Onassis upper-secondary schools (Lyceums) receive training in the pedagogical use of the capabilities of Artificial Intelligence. These initiatives need to apply to all schools and teachers, and they also reflect a state obligation to ensure appropriate supervision, oversight and evaluation by teaching staff, as required by Article 4 of the Joint Ministerial Decision laying down rules on the use of artificial intelligence systems in the educational process and the protection

96. Ministry of Digital Governance, [Digital Transformation Bible 2026–2030](#), December 2025. See, *inter alia*, the upgrading and further development of the Panhellenic School Network's digital-services ecosystem, as well as the expansion of the functionalities of the "myschool" platform. See also existing digital-reform initiatives, including the Ministry of Education, Religious Affairs and Sports, [Actions for the Operation of the Digital Tutoring Platform](#), 22 January 2025 and the [eParents](#) application on the [digitalschool.gov.gr](#) platform ("Digital School").

97. Cited above p. 253.

of personal data⁹⁸. Moreover, as noted above, education and participation are essential links in the chain of responsible integration of AI into education. The same applies to programmes focusing on teachers' skills and generative AI, such as GenAI Education Frontier⁹⁹.

Building on the analysis of children's rights set out above, the GNCHR stresses that these principles, together with the specific rights and risks identified in relation to children, must also be taken into account in initiatives such as the introduction of ChatGPT Edu in Greek public schools under the programme implemented by the Ministry of Education, Religious Affairs and Sports, the Onassis Foundation, OpenAI and The Tipping Point in Education¹⁰⁰. It is important that such initiatives be accompanied by an open and transparent consultation process involving the education community, including educators, students, parents' and guardians' associations, and civil society organisations representing relevant groups or possessing relevant expertise. Furthermore, the use of closed commercial models in high-risk contexts such as the education of minors raises

98. Joint Ministerial Decision No 55909/Δ6/7.5.2026 (Official Government Gazette B 2639/12.5.2026) [Determination of Matters Relating to the Use of Artificial Intelligence Systems in the Educational Process and the Protection of Personal Data](#). Furthermore, the specification of the legal framework, the training of the stakeholders concerned, and operational readiness must precede the deployment of AI applications.

99. Tipping Point/100mentors/data.org, [The GenAI Education Frontier: Generative Artificial Intelligence and Teacher Skills](#).

100. Ministry of Digital Governance, National Alliance for Digital Skills and Employment, C [ChatGPT Edu: Artificial Intelligence enters Greek public schools for the first time](#), 22 September 2025. See National Commission for Bioethics and Technoethics, [Opinion on Artificial Intelligence Applications in Greek Schools](#), 18.March2025. OpenAI, [OpenAI and Greek Government launch 'OpenAI for Greece'](#), 5 September 2025. Hellenic Ministry of Education, Religious Affairs and Sports, [Sofia Zacharaki on the Digital School: "We are placing technology at the service of education and knowledge – modern digital tools are entering the public school system and ensuring equality of opportunities, choices and possibilities."](#) 13 November 2025.

fundamental concerns regarding auditability, accountability and technological dependence¹⁰¹.

Finally, with regard to research, the “Archimedes” Research Unit is an Artificial Intelligence, Data Science and Algorithms Research Centre that has been operating since 2022 at the “Athena” Research Centre, with a view to organising systematic training and communication with leading international institutions, enabling young researchers to take part in high-quality research¹⁰². It is also encouraging that the Centre is collaborating with the Special Secretariat for Artificial Intelligence and Data Governance of the Ministry of Digital Governance and Artificial Intelligence, with the aim of enhancing the effectiveness, innovation and the digital transformation of public administration, through initiatives that include, amongst others: the development of intelligent document management and data analysis systems; the use of natural language processing (NLP) technologies; the automation of citizen support services; the development of tools to support the management of legal texts; the creation of infrastructure and testing frameworks for high-impact artificial intelligence applications, within the European regulatory framework for AI¹⁰³. The GNCHR welcomes such collaborations among institutions, as they enable the combination of the operational implementation of the Regulation on AI and the application of AI principles in the context of research, delivering practical results for various sectors, such as public administration and benefits for human rights. Additionally, the GNCHR emphasises that, within the framework of the National

101. Homo Digitalis, [222 Organisations and Experts Raise Questions over the Entry of OpenAI into Greek Schools](#), 30 Μαρτίου 2026. See [Open Letter concerning the Cooperation of the Ministry of Education, Religious Affairs and Sports with OpenAI](#) submitted by civil society organisations, including the Hellenic League for Human Rights, member of the GNCHR.

102. Athena Research Centre [ARCHIMEDES – Research Unit on Artificial Intelligence](#).

103. Athena Research Centre [Signing of a Memorandum of Cooperation between the Special Secretariat for Artificial Intelligence and Data Governance of the Ministry of Digital Governance and the Athena Research Centre](#), 19 May 2026.

Strategy for Research, Technological Development and Innovation, the principles of AI and respect for human rights must be taken into account, as set out in this report and in other documents of the National Commission, in all matters relating to AI, digital technologies, research and innovation.

3.7 Artificial intelligence and its use in law enforcement, policing and the prison system

3.7.1 Introduction

The rapid development of AI technologies is fundamentally transforming the way in which law enforcement agencies and the prison system operate, creating new opportunities but also complex challenges for the protection of human rights. According to the EU AI Act, “‘law enforcement authority’ means: (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;”¹⁰⁴. In the field of policing, the use of algorithmic systems for predictive policing, facial recognition, biometric data analysis and the surveillance of public spaces promise more effective prevention and investigation of crime. At the same time, however, the extensive use of such technologies raises serious concerns regarding the protection of private life, personal data, and freedom of expression and assembly, while increasing the risk of algorithmic discrimination against specific social groups. Opacity in the functioning of these systems, limited scope for judicial and administrative review, and difficulties in assigning responsibility in cases of error make it necessary to maintain meaningful human oversight and establish clear accountability rules, in accordance with the principles of the rule of law and international guarantees for the protection of fundamental rights.

Similar challenges arise in prison systems, where AI is increasingly used to assess the risk of reoffending, classify prisoners, allocate

104. See Article 3 (46) of the Regulation, as well as Annex III concerning high-risk AI systems referred to in Article 6(2).

resources, conduct electronic monitoring and manage security in detention facilities. Although these applications may contribute to the more efficient operation of detention establishments and better resource management, they may affect critical decisions concerning personal liberty, such as the granting of leave, conditional release or the transfer of prisoners. In the absence of adequate safeguards, algorithms may reproduce existing biases or rely on incomplete and biased data, leading to decisions that violate the principles of equality, proportionality and fair procedure. AI use in policing and prison systems must therefore be governed by a robust regulatory framework that ensures transparency, meaningful human oversight, the possibility of challenging automated decisions and full respect for fundamental rights so that technological innovation operates as a means of strengthening, rather than restricting, justice and the rule of law.

3.7.2 Challenges associated with human rights

The use of AI systems in law enforcement, policing and prison systems may affect a wide range of fundamental rights enshrined in the Charter¹⁰⁵ and other instruments, and the corresponding provisions thereof. In particular, human dignity (Article 1) may be affected where persons are treated as objects of processing or merely as data within the operation of an algorithmic system. At the same time, the right to the integrity of the person (Article 3) may be affected, especially where AI systems are used to assess the risk or dangerousness of prisoners and influence decisions with repercussions for their physical or mental integrity. Similarly, freedom of thought, conscience and religion (Article 10) may be infringed if algorithms produce direct or indirect discrimination on grounds of religious or ideological beliefs, while freedom of expression (Article 11) may be restricted where surveillance technologies create a chilling effect, leading persons to refrain from freely expressing their views or participating in peaceful protests.

105. FRA, [Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks](#), 2025, pp. 43 et seq.

Furthermore, the deployment of AI systems must ensure the principle of equality between women and men (Article 23), preventing the reproduction or reinforcement of existing gender inequalities through biased algorithms. Similar protection is required for the rights of the elderly (Article 25), in order to avoid direct or indirect discrimination on grounds of age in automated decision-making. Especially important is the protection of the right to good administration (Article 41), which presupposes that the use of AI systems will neither hinder the access of the persons concerned to administrative documents nor replace the obligation of authorities to give adequate reasons for their decisions. Safeguarding these rights is essential to the lawful, transparent and human-centric use of AI in law enforcement and the administration of justice.

Although AI is becoming an increasingly important tool for policing across the European Union, it also gives rise to significant ethical and societal challenges, including data bias, privacy violations through surveillance, and risks to accountability, transparency and human rights arising from discrimination. Fair and impartial policing constitutes a fundamental pillar of democratic societies. Bias in data can emerge from numerous sources. Historical data used to train AI systems can embed longstanding societal biases, reflecting past prejudices and discriminatory practices. For instance, if a certain neighbourhood was historically over-policed due to racial or socio-economic biases, an AI system trained on this data might suggest that the area is more prone to criminal activity¹⁰⁶. Moreover, where data do not adequately represent all segments of the population, AI systems may generate inaccurate predictions and disproportionately affect overrepresented groups¹⁰⁷.

While AI offers significant advantages for law enforcement, such as the ability to process vast amounts of data and utilise biometrics for rapid criminal identification and threat assessment, it also brings with it complex challenges. Advanced technologies like facial

106. EUROPOL, [AI and policing – The benefits and challenges of artificial intelligence for law enforcement](#), 2024., p. 32.

107. *Ibid* p. 32.

recognition systems can dramatically enhance efficiency. However, without sufficient safeguards, such as human oversight to evaluate their outputs, these technologies risk infringing on fundamental rights, such as the right to private life and the right to personal data protection (Art. 7 and 8 of the EU Charter of Fundamental Rights). This could manifest as disproportionate surveillance of innocent individuals or the potential for misuse targeting specific groups, raising concerns about privacy and the necessity of such monitoring¹⁰⁸.

The use of AI for surveillance purposes can lead to intrusive monitoring of individuals, potentially violating privacy rights. Policymakers should seek to promote public safety while also ensuring protection of individuals through privacy and data protection regulations to prevent misuse and overreach. In bringing together the risks of bias and privacy infringements, remote biometric identification (i.e. facial recognition) has proven particularly controversial because the systems involved may carry an inherent technological bias (e.g. discriminating by racial or ethnic origins). The use of AI in public spaces may also undermine the ability of individuals to freely exercise applicable rights related to privacy, data protection and freedom of expression and assembly¹⁰⁹.

With regard to prison systems, according to the Council of Europe's European Committee on Crime Problems (CDPC)¹¹⁰, although AI, algorithmic mechanisms and related digital technologies are already applied in certain prison and probation systems internationally, their use in Europe remains limited and, in most legal systems, is not accompanied by a specific legislative or regulatory framework.

108. *Ibid* p. 33.

109. OECD, [Governing with Artificial Intelligence – The State of Play and Way Forward in Core Government Functions](#), 2025, p. 261.

110. Council of Europe, European Committee on Crime Problems (CDPC), [Recommendation CM/Rec \(2024\)5 of the Committee of Ministers to member States regarding the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services – Explanatory Memorandum](#), CM (2024)105-add2final, 9 October 2024.

Their limited deployment also means that there is insufficient scientific evidence about their effectiveness, benefits and risks. However, as prison services form part of a broader digitalised public administration, they are called upon to harness the potential of AI in a manner fully compliant with national and international human rights protection standards, ensuring that technology operates in a supportive capacity and does not replace the decisive role of human judgement and oversight.

3.7.3 Perspectives and recommendations

In accordance with the Recommendation of the Committee of Ministers of the Council of Europe to member states on the ethical and organisational aspects of the use of artificial intelligence and related digital technologies the prison and probation services must be consulted in order to identify and evaluate their needs regarding safety, security and good order tasks and how to best assist them in executing these tasks by using AI and related digital technologies¹¹¹. The use of AI in electronic monitoring, including biometric recognition technologies, should be proportionate to the purpose and used only when strictly necessary. It should be carried out under regular human control and should be human centred. It should be oriented to favour the reintegration of offenders and should be respectful of all the principles and guarantees associated with the use of electronic monitoring. The rehabilitation and reintegration of offenders, as well as their social contacts, may be facilitated by the use of AI and related digital technologies. When such tools are used for the personalisation of treatment and reintegration plans, this should be done with care to avoid biases. The use of such tools should not replace regular face-to-face human contact between professionals and the offenders, including, where necessary, the work with their families and children.

111. Council of Europe, Committee of Ministers, [Recommendation CM/Rec \(2024\)5 of the Committee of Ministers to member States regarding the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services](#), 9 October 2024.

AI and related digital technologies in the selection, management, training and development of staff should be used to optimise human and managerial capacities and processes. This use should also be focused on supporting the staff's professional development. AI and related digital technologies should assist managers in predicting future organisational capacity, including detecting especially problematic areas in staff resourcing. Managerial decisions taken in this respect should not violate staff members' rights or lead to discrimination or unfairness. The use of AI and related technologies in prisons and by surveillance services should be governed by a clear legal framework, in order to ensure legal certainty and accountability.

The GNCHR underlines that the ethical, lawful and transparent use of AI in policing requires the recruitment of specialised experts or the establishment of a dedicated unit to develop and deploy the relevant technologies. It also requires an appropriate legal framework, grounded in ethics and privacy protection¹¹². New applications should be subject to assessment in a manner capable of withstanding judicial scrutiny and consistent with the values and standards of human rights law. INTERPOL and the United Nations Interregional Crime and Justice Research Institute (UNICRI) stress that, as law enforcement agencies increasingly deploy AI and robotics across society, with a growing impact on citizens' daily lives, it is becoming increasingly important for law enforcement agencies to ensure that the use of these technologies is ethical, following the principles of justice, accountability, transparency and explainability¹¹³. In any event, beyond AI ethics principles, States must comply with their obligations under international, European and national law.

In accordance with EUROPOL¹¹⁴ impact assessment is particularly important for AI systems used in the law enforcement domain, where the potential for harm is high. This assessment must be conducted throughout all phases of the AI lifecycle, taking into account the

112. INTERPOL – UNICRI, [Artificial Intelligence and Robotics for Law Enforcement](#), 2019, p. 26.

113. *Ibid*, p. 12-13.

114. EUROPOL, [AI bias in law enforcement – A practical guide](#), 2025 p. 48.

context in which the AI system is implemented. It should also include a thorough evaluation of data protection issues, such as the collection, storage, and use of personal data, ensuring compliance with relevant privacy laws and regulations. All potential risks, harms, and data protection concerns that the AI system might cause should be carefully evaluated and documented to ensure transparency, accountability, and the safeguarding of individual rights. More specifically, fundamental rights impact assessment for high-risk AI systems is mandated in Article 27 of the EU AI Act, and it includes describing how and when the system will be used, the categories of people likely to be affected by its use and the risks, and human oversight measures. The latter is a very important criterion for the examination of cases, for assessing the quality of the investigation and its findings, for ensuring consistency and, ultimately, for guaranteeing a fair process free from bias and discrimination. Furthermore, expertise in human rights is important for understanding when and how they are violated while using AI systems.

Addressing AI bias in law enforcement requires a multifaceted approach that integrates technical, human, and contextual factors. By fostering diversity, documenting biases, performing thorough impact assessments, and selecting appropriate fairness metrics, we can develop AI systems that are fairer, more transparent, and better suited to support just and equitable law enforcement practices¹¹⁵.

As discussed above, relevant decisions of independent authorities have highlighted risks to the exercise of fundamental rights. The use of AI may amplify these risks and, without appropriate safeguards, may result in serious rights violations. The Smart Policing case and the HDPa Decision 45/2025¹¹⁶ provide an illustrative example.

115. *Ibid* p. 50.

116. HDPa Decision 45/2025,, 31 December 2025. Homo Digitalis, [Another Important Victory! The HDPa rules the operation of the Hellenic Police's Smart Policing system unlawful](#), 15 January 2026. In Decision 45/2025, the HDPa warned the Hellenic Police not to activate the Smart Policing system, finding that any productive operation of the system under the applicable legal framework would amount to unlawful processing of personal data. The Authority found that there was no legal basis for the intended processing through that system and that the required data

The Authority found that there was no legal basis for the intended processing through that system and that the required data protection impact assessment had not been carried out in a timely manner during the pilot implementation phase of the system.

Law enforcement will become increasingly dependent on AI in the coming years, especially if it is considered to be superior to traditional policing methods, and cheaper than hiring more officers. Current models of regulating, organizing, and explaining policing are based on models of human decision-making¹¹⁷. Consideration must be given to how the design of the technologies, to the participation and information of users and persons affected by them, and to their broader social implications, given that the existing monitoring mechanisms are insufficient to address the individual, collective and social risks entailed by the use of AI¹¹⁸.

The use of any automated decision-making systems by police or criminal justice authorities must be made transparent, enabling affected individuals to exercise their rights and challenge automated predictions, profiles, or their resulting consequences¹¹⁹. By default, police and criminal justice authorities should publish relevant information on databased, algorithmic, or automated systems they use in a publicly accessible database. Such an Algorithm Transparency Register⁴⁰⁹ should include details about the system, how it works, the data it uses, the way it conducts analyses or generates outputs, its intended uses, and the potential consequences. If a system is

protection impact assessment had not been carried out in a timely manner during the pilot implementation phase of the system.

117. Rosamunde Van Brakel, [Legal, Ethical, and Social Issues of AI and Law Enforcement in Europe – The Case of Predictive Policing](#), In: Smuha NA, ed. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge Law Handbooks. Cambridge University Press; 2025:367-382. p. 381. On “predictive policing” see in particular EUCPN, [Artificial intelligence and predictive policing: risks and challenges](#), Recommendation paper, 2022.

118. *Ibid.*

119. Algorithm Watch, [Algorithm Injustice, ‘Predictive’ policing and criminal ‘prediction’ and profiling systems used by law enforcement and criminal justice authorities in Germany](#), March 2025. p. 62.

classified for national security purposes, the competent oversight bodies need to have full and unfettered access to compensate for the lack of public transparency. Automated systems used by public bodies, such as the police and criminal justice authorities, must not be subject to legal restrictions such as intellectual property or trade secrecy that hinder the publication of relevant details about their development, use, operation, and full analysis of their outputs¹²⁰. In addition, the GNCHR has highlighted the necessary safeguards concerning the framework for digitally enhancing road safety, including risks and recommendations related to the legislative framework¹²¹.

3.8 Artificial intelligence in public administration and governance

3.8.1 Introduction¹²²

AI is gradually transforming the functioning of public administration and governance, offering new possibilities for the automation of administrative procedures, the processing of large volumes of data and the improvement of the decision-making process. Making use of it can help public services to be delivered more effectively, reduce bureaucracy, save resources and enhance the transparency and efficiency of administrative activities, thereby forming a key pillar of the digital transformation of the public sector.

At the same time, integrating AI into public administration raises significant legal, ethical and institutional issues, particularly where it affects administrative decisions that concern the rights and legitimate interests of citizens and persons under State protection. The need to ensure transparency, accountability, the protection of personal data, equal treatment and meaningful human oversight requires the development of a robust regulatory framework, so

120. *Ibid.*

121. GNCHR, [The GNCHR participation in the Parliamentary Committees on the Draft Law of the Ministry of Digital Governance on the digital enhancement of road safety](#), 28 November 2025.

122. For further information on the framework for the governance of the AI in Greece and the role of the GNCHR, see the chapter below.

that the use of artificial intelligence enhances the quality of public governance while fully respecting fundamental rights and the principles of the rule of law.



*GNCHR, The GNCHR participation in the Parliamentary Committees
on the Draft Law of the Ministry of Digital Governance
on the digital enhancement of road safety*

3.8.2 Challenges associated with human rights

The use of AI systems in public administration may affect a range of enshrined fundamental rights. More specifically, human dignity may be affected where persons are treated as objects of algorithmic processing; freedom of thought, conscience and religion where the use of AI leads to direct or indirect discrimination on grounds of religious or other beliefs; freedom of expression where the assessment of applications for public benefits through AI systems deters persons from expressing themselves freely; and the principle of equality before the law where similar cases are treated differently as a result of the operation of algorithmic systems¹²³.

123. FRA, [Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks](#), 2025, p. 45-46.

National authorities have acknowledged¹²⁴ that AI poses challenges in various areas, including the functioning of democracy, while also driving change in many fields, such as the labour market, defence and value chains. Competitiveness and systemic resilience are also areas that should spur the government –and, above all, legislators– into action. The GNCHR underlines that significant challenges arise as regards transparency and accountability in public-sector decision-making where it relies on AI systems.

According to the OECD, the use of AI in public administration entails five main categories of risks¹²⁵: 1. Ethical risks: These include AI uses that undermine the free exercise of human rights and freedoms, including privacy, potentially infringing on human-centred values either deliberately or inadvertently. AI algorithms can introduce ethical risks from the digital realm to the physical world through biased algorithms and unethical behaviours like invasive surveillance; 2. Operational risks: These include technical and operational failures that might affect data privacy, the quality of AI outcomes and internal government operations due to cybers threats, unintended consequences, hallucinations, systematic errors and overreliance on AI systems; 3. Exclusion risks: These risks relate to gaps that arise when citizens without access to technology or digital literacy can be left behind and unable to benefit from AI advancements in public services; 4. Public resistance risks: These include public resistance to government use of AI. This can be driven by distrust in government AI systems or processes, or by the spread of false or misleading information about how AI is implemented in public administrations and its potential impacts and 5. Risks of inaction: Although often overlooked, this risk includes government delays in using AI to yield positive benefits. This can result in significant financial and non-financial costs –which could have otherwise been avoided with AI’s

124. Hellenic Republic, Prime Minister, [Briefing Note on the Meeting of the Advisory Committee on Artificial Intelligence, chaired by Prime Minister Kyriakos Mitsotakis](#), 25 October 2023.

125. OECD, [Governing with Artificial Intelligence – The State of Play and Way Forward in Core Government Functions](#), 2025, p. 35.

successful adoption— and a widening gap between public sector and private sector capabilities.

3.8.3 Perspectives and recommendations

AI can be leveraged as a public policy tool across a range of sectors, including health, the fight against tax evasion, civil protection¹²⁶, public financial management, and the National Cadastre. In addition to the measurable outcomes required in each sector to demonstrate the positive impact of AI use and the prevention of tax evasion or natural disasters, authorities must also take into account fundamental rights safeguards when implementing AI systems.

In order to address these challenges, the High-Level Advisory Committee on Artificial Intelligence was established as an interdisciplinary advisory body to the Prime Minister, with the aim of supporting his work with regard to preparing the country, *inter alia*, for the use of AI as a public policy tool in various policy areas¹²⁷. Coordinated by the Special Secretariat for Foresight, the Committee was tasked with formulating a national policy to harness the potential of AI. On the basis of the Blueprint for Greece's AI Transformation¹²⁸, the Committee stresses that the guiding principles are respect for human dignity, human well-being, pluralism, participation, transparency, oversight, adaptability and international multilateral cooperation. The use of AI in the performance of administrative tasks must be consistent with the core principles of administrative law, such as legality, the public interest, good administration and fairness.

126. Ministry for Climate Crisis and Civil Protection [The use of Artificial Intelligence for the benefit of citizens' security](#), 12 March 2025.

127. Hellenic Republic, Prime Minister's Office [Announcement – Press Office of the Prime Minister](#), 19 October 2023 and [Briefing Note on the Session of the Advisory Committee on Artificial Intelligence, chaired by Prime Minister Kyriakos Mitsotakis](#), 25 October 2023. Decision No Y4/16.1.2024, "Establishment, Composition and Operation of the Advisory Committee on Artificial Intelligence" Official Government Gazette, B 280, 17 January 2024.

128. High-Level Advisory Committee on Artificial Intelligence [Blueprint for Greece's AI Transformation](#), November 2024 pp. 14, 135.

The Blueprint also stresses the need to enhance the efficiency and transparency in public administration, the integration of AI in public procurements and data analytics from *Diavgeia* programme, and the development and implementation of AI-based chatbots for administrative navigation rigorously and cautiously. AI use in these areas must be accompanied by robust guarantees for the protection of fundamental rights, in particular through transparency of algorithmic processes, personal data protection, the prevention of discrimination, human oversight and safeguards for the right to a reasoned administrative decision and effective judicial protection.

AI's potential is recognised across all functions of public administration, but their maturity levels in terms of adoption and governance vary considerably. Some sectors are already implementing AI initiatives in a structured way, learning from their deployment and, in some cases, scaling successful solutions to other problem areas and broader contexts¹²⁹. Certainly, this recognition must be accompanied by guarantees and obligations on the part of the authorities and the public administration, based on human rights. In particular, as regards automated decision-making, public entities should engage with their own sector-regulators (insurance, credit reference agencies, banks, e-commerce and others) to develop specific standards and guidelines to ensure that they are able to respond to the challenges of the use of automated decision-making through algorithms and taking into account the interests of consumers and the general public¹³⁰.

According to the aforementioned AI Blueprint, data are regarded as the “new gold” and arguably constitute the most important raw material for AI applications, alongside human resources and computing resources. Making certified and secure datasets available

129. OECD, [Governing with Artificial Intelligence – The State of Play and Way Forward in Core Government Functions](#), 2025, p. 73. See also OECD, [Good Practice Principles for Public Service Design and Delivery in the Digital Age](#), 8 November 2022.

130. Council of Europe, Committee of Experts on Internet Intermediaries (MSI-NET), [Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques and possible regulatory implications](#), 2018, pp. 28-30, 46.

can enhance AI research and development, particularly by leveraging data in the areas of civil protection, border control and defence, and by upgrading digitisation in critical sectors, such as medical records in the National Health System, so that data are suitable for AI applications from the outset¹³¹. This assumption must also take into account the international, European and national frameworks for the protection of human rights, as well as the appropriate procedural safeguards when using these systems and data. Part of the drive to strengthen public digital infrastructure involves the launch of the new National Supercomputer 'DAEDALUS' and the *Lavrion* Data Centre¹³², the design of which must take environmental protection issues into account, as AI development leads to massive consumption of energy, water and land, raising environmental and equity challenges across all global infrastructures¹³³. In April 2025, the Ministry of Digital Governance launched the AI Factory "Pharos" project "Pharos" is one of thirteen "AI

-
131. High-Level Advisory Committee on Artificial Intelligence [Blueprint for Greece's AI Transformation](#), November 2024 p. 46.
 132. Ministry of Digital Governance and Artificial Intelligence "[The Implementation of the New European Supercomputer 'DAEDALUS' and the Data Centre at the Lavrion Technological and Cultural Park Begins – Greece Is Building One of the Most Powerful Computing Systems in Europe](#)" 26 March 2025. The project is being implemented by the National Infrastructures for Research and Technology (GRNET S.A.), under the auspices of the Ministry of Digital Governance and Artificial Intelligence. It is part of the National Recovery and Resilience Plan "Greece 2.0" and is funded by the European Union's NextGenerationEU programme, through the Recovery and Resilience Facility and the European High-Performance Computing Joint Undertaking (EuroHPC JU). The infrastructure has been designed with sustainability at its core, using renewable energy sources and advanced cooling systems to significantly reduce energy consumption.
 133. UNU-INWEH, [Report: Aczel, M., Chamanara, S., Matin, M., Farsi, A., Marwala, T., Madani, K. Environmental Cost of AI's Energy Use: Carbon, Water and Land Footprints](#). United Nations University Institute for Water, Environment and Health (UNU-INWEH), Richmond Hill, Ontario, Canada, 3 June 2026.

Factories” in Europe, dynamic ecosystems that promote innovation, collaboration and development in the field of AI¹³⁴.

The GNCHR welcomes the vision of the Ministry of Digital Governance, according to which the use of AI in public administration will require new, cross-sectoral models of governance and operation in which data and digital resources in general will transcend traditional boundaries between public bodies. Policy makers and public officials will need a proper understanding of the technology, its potential and its risks, so as to duly assess its integration into public policy areas. Moreover, it is essential to establish clear commitments regarding the type of data to be used, with a view to safeguarding fundamental rights by all parties involved, –including project contractors, data providers and the bodies operating the systems– and building of trust with individuals or communities affected by decision-making AI systems¹³⁵. It is important that cooperation in this direction with the NHRI and other authorities be clearly reflected within the national AI governance ecosystem.

In order to leverage AI applications, the Greek State has introduced the “Digital Assistant” mAigov¹³⁶, the mAIGreece application (developed

-
134. Ministry of Digital Governance and Artificial Intelligence, [“Implementation Begins for the Ministry of Digital Governance’s Flagship Project, AI Factory Pharos”](#), 15 April 2025. The new national supercomputer DAEDALUS will serve as the computing platform for AI Factory Pharos. See also Pharos, [The Greek AI Factory](#) and European Commission, [AI Factories](#), 23 April 2026 (last update). Law 5263/2025 (Official Government Gazette, A 238, 19 December 2025) established a public limited company under the corporate name “Hellenic Artificial Intelligence Factory S.A.” and the trading name “AI FACTORY PHAROS”. The company operates under the supervision of the Minister of Digital Governance.
135. Ministry of Digital Governance, [Digital Transformation Bible 2020–2025](#), June 2021, p. 160. See also [Digital Transformation Bible 2020–2025 – Artificial Intelligence, 10 Overall Projects](#).
136. Ministry of Digital Governance and Artificial Intelligence, [“mAigov – the gov.gr Digital Assistant at Citizens’ Service: Public Administration in the Age of Artificial Intelligence”](#), 12 December 2023. This is a bot that provides personalised answers to questions asked by members of the public on matters relating to public administration. Ministry of Digital

in cooperation with the Ministry of Tourism), the myCoast application (in cooperation with the Ministry of National Economy and Finance), and an AI application for the legal control of the National Cadastre¹³⁷. In particular, where AI applications relate to the setting of objectives and the evaluation of public administrative employees¹³⁸, there must be guarantees of transparency, human oversight, fair treatment, information¹³⁹, accountability and protection from algorithmic bias, and all requirements of international, European and national law must be observed –especially when such applications affect career evolution and the rights of employees. All the above must meet specific human rights safeguards, as analysed in this section and in this report in general.

Governance and Artificial Intelligence, [Terms of Use of the Ministry of Tourism's mAIgree Application](#). This is a personalised travel guide to Greece. Ministry of Digital Governance and Artificial Intelligence, [MyCoast: the New Digital Application for Citizens to Ensure Compliance on Seashores and Beaches](#)", 29 April 2024. Through the MyCoast app, citizens can obtain information on active concessions for the simple use of the seashore or beach and verify whether the applicable concession terms are being observed. Where concession limits or conditions are exceeded, or where there is unauthorised occupation, they may submit a report to the competent authority. At a later stage, the integration of an AI tool is expected to enable information systems to check compliance automatically.

137. Ministry of Digital Governance and Artificial Intelligence, [National Cadastre: The First Public Body to Introduce Artificial Intelligence](#), 4 September 2024.
138. See for instance: Ministry of the Interior, ["Procedure for the Specification and Allocation of Targets for 2025 – Technical Instructions for Data Entry in the 'Setting of objectives' Electronic Application of the Greek Public Administration Human Resources Registry \(Apografi\) – Artificial Intelligence Technologies: Digital Setting of objectives Assistant"](#), 9 May 2025. Law 4940/2022 and the Human Resource Management System (HRMS) [Institutional Framework – Circulars on Performance Assessment](#).
139. See, for instance, the example of Estonia concerning the use of AI in public administration: Estonia – Chancellor of Justice, [Chancellor's Year in Review 2024/2025, Surveillance society – Use of Artificial Intelligence in Public Service Delivery](#).

3.9 Women's and girls' rights and artificial intelligence

3.9.1 Introduction

On the basis of the points highlighted and emphasised by the GNCHR in its Report on the Status of Women in Greece and in its relevant documents, statements and initiatives¹⁴⁰, AI is increasingly affecting gender-related issues, given its use in fields such as employment, education, health, public administration and the administration of justice. Its use offers significant opportunities for advancing gender equality, through more effective data analysis, the identification of gender inequalities and the support of evidence-based public policies.

At the same time, the development and deployment of artificial intelligence systems are accompanied by significant challenges, since algorithms may reproduce or even reinforce existing gender bias and discrimination, particularly where they rely on biased data or lack transparency. AI must therefore be accompanied by appropriate safeguards, ensuring that technological innovation makes a meaningful contribution to gender equality and to respect for fundamental rights.

3.9.2 Challenges associated with human rights

It is important to consider the statistical data of the European Institute for Gender Equality on the overall situation in Greece¹⁴¹

140. GNCHR, [Report on the Status of Women in Greece](#), 2025. See pp. 11-12 on the contribution of the GNCHR to the monitoring of the country by regional and international protection bodies, as well as the [Gender Equality](#)" field in the GNCHR website. The contributions made by the civil society organisations DATAWO and WHEN during the GNCHR hearing of stakeholders and individuals were also taken into account.

141. EIGE, [Gender Equality Index – Greece in 2025 edition](#), July 2026. Greece scores 57.0 points out of 100 in the Gender Equality Index and ranks 22nd in the EU. This is due to low performance in the domains of time, in which Greece ranks 26th, and work, in which it ranks 21st. Greece's Index score has risen by 7.3 points since 2015 and by 5.7 points since 2020. Although Greece has made progress over time, its gender-equality performance remains below the EU average. The scores also point to widening disparities between Greece and the EU average.

alongside other data on new technologies and AI, and on their implications for the rights of women and girls. The European Commission underlines that, although women account for 51% of the EU population, only one in three STEM graduates and one in five information and communication technology (ICT) specialists are women¹⁴². Since 2015, the proportion of women employed in the ICT sector has changed very little. According to the ILO, although AI is expected to drive growth across technology-focused sectors, women account for only 30% of the AI workforce globally¹⁴³. According to UNESCO¹⁴⁴, women and girls are 25% less likely than men to know how to leverage digital technology for basic purposes, four times less likely to know how to programme computers, and thirteen times less likely to file for an Information and Communication Technologies (ICT) patent. Furthermore, only 20% of employees in technical roles in major machine-learning companies are women; women account for 12% of artificial intelligence researchers globally and 6% of professional software developers.

Available research evidence demonstrates that gender bias in AI systems is widespread since a significant number of applications display gender-based discrimination, while have repeatedly associated women with the home, family and childcare, while linking men to business, leadership and career success. In some cases, AI systems have generated responses portraying women as sexual objects or as subordinate to men¹⁴⁵. According to UN Women data, nearly one in four surveyed women human rights defenders, activists and journalists reported having experienced AI-assisted online violence; 12% stated that personal images had been shared without

142. European Commission, [Women in Digital](#), 25 April 2025 (last update). See also EUROSTAT, [Employed information and communications technology \(ICT\) specialists by sex](#), 18 April 2026 (last update).

143. ILO, [Gen AI, occupational segregation and gender equality in the world of work](#), 5 March 2026.

144. UNESCO, Gender Equality, [Women's access to and participation in technological developments](#) (last access: July 2026).

145. UN, [AI is getting women wrong as gender bias persists, data reveals](#), 22 June 2026.

their consent, while 6% reported having been targeted by deepfakes or manipulated images and videos¹⁴⁶. According to a 2023 study, pornographic deepfake content accounted for 98% of all deepfake videos online, 99% of which depicted women¹⁴⁷.

When linking the AI context and new technologies to the digital dimension of violence, we need to highlight the conclusions of General Recommendation No. 1 of the Group of Experts on Action against Violence against Women and Domestic Violence¹⁴⁸, according to which the digital dimension of violence against women encompasses a wide range of acts online or through technology that are part of the continuum of violence that women and girls experience for reasons related to their gender, including in the domestic sphere, in that it is a legitimate and equally harmful manifestation of the gender-based violence experienced by women and girls offline.

In its Contribution to the 2026 Thematic Report on Gender Equality, the Digital Space and the Age of Artificial Intelligence, prepared for the UN Working Group on discrimination against women and girls¹⁴⁹, the GNCHR highlighted challenges relating to women's leadership in political, economic, social and cultural rights; AI governance and moderation of AI-generated content; AI-enabled gender-based violence; work and the rights of women and girls; privacy and autonomy; non-discrimination; and the availability of disaggregated data.

146. UN Women, [Tipping point: The chilling escalation of online violence against women in the public sphere](#), 2025.

147. UN Women, [When justice fails: Why women can't get protection from AI deepfake abuse - What is deepfake abuse and why laws, platforms, and justice systems are failing women](#), 26 February 2026.

148. GREVIO, [General Recommendation No. 1 on the digital dimension of violence against women](#), 2021, p. 13.

149. GNCHR, [GNCHR contribution to the 2026 Thematic Report on Gender Equality, the Digital Space and the Age of Artificial Intelligence of the UN Working Group on discrimination against women and girls](#), October 2025.

According to a UNESCO¹⁵⁰ report, women continue to face significant barriers to internet connectivity and digital skills development. This inequality is linked to factors such as limited educational opportunities, social and cultural stereotypes, restrictions on their freedom of movement, a lack of financial independence, and difficulties in accessing digital infrastructure and technological equipment. The gender digital divide limits women's ability to search for and secure jobs, enter the labour market and pursue their career progression. At the same time, it reduces their opportunities to acquire the necessary knowledge and skills required in an increasingly digitalised working environment. Equal access to digital technologies involves more than the availability of devices and internet connectivity; it also requires the development of appropriate digital skills. Strengthening these skills is essential to supporting women's entry into the labour market, including retention and their career progression.

3.9.3 Perspectives and recommendations

The challenges outlined above underscore the need to apply and adapt existing human rights protection instruments to contemporary conditions. These include the United Nations Convention on the Elimination of All Forms of Discrimination against Women and the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence¹⁵¹.

AI systems may optimise job-search services in order to ensure that women receive equal opportunities when considering and applying for work. Better designed, gender-responsive tools and algorithms for matching vacancy requirements with jobseekers' skills could make AI-enabled job-matching services more inclusive for persons in vulnerable

150. UNESCO/OECD/IDB, [The Effects of AI on the Working Lives of Women](#), 2022, pp. 17, 19.

151. Law 4531/2018 (Official Government Gazette, A 62 5.4.2018). [Law 5172/2025](#) (Official Government Gazette, A 10 29.1.2025) concerning the tackling of new forms of violence against women and the transposition of Directive (EU) 2024/1385, constitutes an important legislative development.

situations in the labour market¹⁵². One opportunity lies in investing in initiatives, projects and companies that encourage women's access to digital devices and connectivity and develop women's digital skills. With support, women around the world have a better chance of preparing for and searching for and securing jobs. For example, the EQUALS Global Partnership aims at narrowing the digital gender divide and fostering the digital skills of women and girls¹⁵³.

These findings highlight the urgent need to embed gender equality in the design, deployment and governance of new technologies. Addressing these challenges requires deliberate action, including the development of debiasing techniques and more representative datasets to train learning models, alongside robust safeguards to prevent the reinforcement of gender stereotypes and biases in AI systems. Ensuring greater involvement of diverse stakeholders—particularly women and other underrepresented groups—in AI development is also essential to promote inclusive and equitable outcomes¹⁵⁴.

The role and responsibility of the ICT sector and social media platforms in preventing gender bias when designing products, in establishing internal monitoring mechanisms and raising awareness, particularly on issues of violence in the digital sphere¹⁵⁵, are crucial factors in enabling women and girls to exercise their rights in the age of AI. Addressing deepfakes, which result from human rather than autonomous AI Action, requires immediate and coordinated intervention including the adoption of a comprehensive legislative framework specifically covering forms of such abuse; the strengthening of law-enforcement and judicial authorities so that they can effectively investigate and prosecute the relevant offences; the imposition of meaningful accountability on digital platforms for

152. UNESCO/OECD/IDB, [The Effects of AI on the Working Lives of Women](#), 2022, pp. 19-20.

153. *Ibid.*

154. ILO, [Gen AI, occupational segregation and gender equality in the world of work](#), 5 March 2026 p. 11.

155. GREVIO, [General Recommendation No. 1 on the digital dimension of violence against women](#), 2021, p. 24.

the timely detection and removal of unlawful content; the provision of effective legal and psychosocial support to victims; and, finally, the promotion of education and awareness-raising as key means of preventing abuse¹⁵⁶.

3.10 Rights of the child and artificial Intelligence

3.10.1 Introduction

AI is increasingly shaping children's everyday lives, as it is integrated into educational platforms, social media, entertainment applications, health services and public services¹⁵⁷. Its use offers important opportunities to support education, personalised learning, healthcare and children's access to quality digital services, thereby contributing to their well-being and development.

At the same time, the use of AI raises serious challenges for the protection of the rights of the child, particularly as regards privacy, the protection of personal data, exposure to harmful content, algorithmic bias and safety in the digital environment. AI systems must therefore be designed, developed and deployed with the best interests of the child as a primary consideration and accompanied by appropriate safeguards ensuring full respect for children's fundamental rights, in accordance with the United Nations Convention on the Rights of the Child and other relevant instruments and recommendations.

The GNCHR takes into account the framework for the protection of the rights of the child in the digital environment, drawing on the Council of Europe's set of instruments, including the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention); the Convention on Cybercrime (Budapest Convention); the Council of Europe Strategy for the Rights of the Child (2022–2027); Recommendation CM/

156. UN Women, [When justice fails: Why women can't get protection from AI deepfake abuse - What is deepfake abuse and why laws, platforms, and justice systems are failing women](#), 26 February 2026.

157. See also the cross-cutting references to the other issues addressed in this Chapter.

Rec(2018)7 of the Committee of Ministers; the Handbook for policy makers on the rights of the child in the digital environment; the Internet Literacy Handbook; the Report on children with disabilities in the digital environment; and the Guidelines on children's data protection in an education environment¹⁵⁸.

3.10.2 Challenges associated with human rights

The use of AI in contexts concerning children raises significant challenges linked to the lack of a dedicated legal framework that effectively protects children's rights; the design of many AI systems without adequate consideration of minors' particular needs and rights; and limited scientific knowledge about AI's effects on children's development and well-being¹⁵⁹. These gaps heighten the risk of malicious uses of technology and unintended harm, with potentially far-reaching social consequences for children's well-being and future perspectives.

More specifically, according to UNICEF¹⁶⁰, AI may facilitate the mass dissemination of misinformation and harmful or illegal content. Children's growing interaction with conversational AI systems, or chatbots, may also affect their perceptions, cognitive development,

158. Council of Europe, [Digital environment](#). GNCHR, [Participation of the GNCHR in the Seminar "Raising awareness of the local community on human rights" under the auspices of the Ministry of Justice with a focus on the Rights of the Child](#), 30 October 2024. See National Commission for Bioethics and Technoethics, [Declaration on the protection of children from adverse effects of algorithms on social media](#), 17.12. 2024.

159. Council of Europe, Steering Committee for the Rights of the Child (CDENF), [Mapping Study on the Rights of the Child and Artificial Intelligence: Legal Frameworks that Address AI in the Context of Children's Rights](#), 2024, p. 12.

160. UNICEF, [Generative AI: Risks and opportunities for children](#). The GNCHR hearing of stakeholders and individuals also considered the contribution of the Foundation for Research and Technology – Hellas (FORTH) Research Ethics and Deontology Committee on the ethical issues and challenges associated with the psychosocial use of conversational AI by adolescents and young adults.

social behaviour and privacy. At the same time, with the increasing power and prevalence of AI, it is easy to see the many opportunities that generative AI can potentially offer children and young people directly or indirectly shaping their behaviour and perceptions, as well as causing disruptions in education due to the changes brought about by AI in the labour market. Existing digital inequalities may be further exacerbated, leaving some children more exposed to AI-related harms and less able to benefit from its potential.

The right to privacy is a fundamental right that can be violated; however, respecting this right enables children to enjoy other rights that are crucial to the development of their personality, such as freedom of expression and the right to health, amongst others. Children's privacy relates to their bodily and mental integrity, decisional autonomy, personal identity, informational privacy and physical/spatial privacy¹⁶¹. It also extends to children's digital identity and online participation with the opportunities and risks that these entail¹⁶².

AI and the digital environment are directly linked to the exercise of the child's fundamental rights, in particular the right to freedom of expression and information, since the internet constitutes a primary space for seeking information, communicating and expressing views¹⁶³. At the same time, children have the right to participate in online communities and associations, to take part in peaceful online activities, and to participate in public debate and policy-making processes concerning At the same time, children have the right to participate in online communities and associations, to take part in peaceful online activities, and to participate in public debate and policy-making processes concerning internet governance¹⁶⁴. The right to education also entails access to educational, scientific

161. UN/Special Rapporteur on the right to privacy, [Artificial intelligence and privacy, and children's privacy](#), Report, A/HRC/46/37, 25 January 2021, p. 10-11.

162. *Ibid* p. 13.

163. CoE, [Handbook for policy makers on the rights of the child in the digital environment](#), 2020, p 40.

164. *Ibid* p. 43.

and cultural content in digital form, together with the development of digital and information literacy, enabling children to use digital technologies safely and to assess critically the reliability of information and online services¹⁶⁵.

At the same time, children have the right to protection from all forms of violence, exploitation and abuse in, or through, the digital environment. States have an obligation to continuously assess, on the basis of reliable scientific evidence, the risks posed by new technologies to children's physical and mental well-being and to adopt, as a matter of priority, preventive protective measures. Such measures must serve the best interests of the child, take account of the child's age and maturity, and not unduly restrict the exercise of their other rights.

The main risks faced by children in the digital environment are divided into four categories¹⁶⁶. The main risks faced by children in the digital environment are divided into four categories: content risks, such as exposure to pornographic, violent or racist material; contact/communication risks, such as online grooming, harassment and exploitation by adults; conduct risks, including cyberbullying, attacks on reputation, incitement to self-harm, online fraud other harmful user-to-user interactions; and contractual risks, where children enter into online contracts which they do not understand or obtain access to goods and services inappropriate for their age.

3.10.3 Perspectives and recommendations

The increasingly widespread use of AI creates significant opportunities for children and young people, including personalised learning, tailored to their individual needs, the promotion of creativity and play through the creation of stories, works of art, music or software, improved accessibility for children with disabilities; and support for healthcare through the early detection of health problems and the more effective use of medical data.

165. *Ibid* p. 53.

166. *Ibid* See also *CNCDH, Avis sur la protection de l'intimité des jeunes en ligne*, 23 Janvier 2025.

In the National Strategy for the Protection of Minors from Internet Addiction¹⁶⁷, the Ministry of Digital Governance has highlighted AI as one of the powerful tools underpinning modern social networks and online applications. The rights of the child are referred to in recitals 9, 28 and 48 and in Annex II on sexual exploitation of children and child pornography of the EU AI Act, as well as in the Digital Services Act¹⁶⁸, specifically in Article 28 on the protection of minors online, and in the Guidelines on taking measures to ensure a high level of privacy, safety and protection of minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065¹⁶⁹.

According to the above Guidelines, there are specific benefits arising from the operation and use of online platforms. Online platforms are increasingly accessed by minors and can offer them a range of benefits. For instance, online platforms may provide access to numerous educational resources, helping minors to learn new skills and expand their knowledge. Online platforms may also offer minors opportunities to express their views and connect with others who share similar interests, helping minors to build social skills, confidence and a sense of community. By playing on and exploring the online environment, minors can also foster their natural curiosity, engaging in activities that encourage creativity, problem solving, critical thinking, agency and entertainment.

However, effective protection is also needed. According to the above Guidelines, there is, however, wide consensus among policy makers, regulatory authorities, civil society, researchers, educators and

167. Ministry of Digital Governance, National Strategy for the [Protection of Minors from Internet Addiction](#), 2025, pp. 5 and 26, on the EU AI Act and the protection of children.

168. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). See also Law 5099/2024.

169. European Commission, [Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28\(4\) of Regulation \(EU\) 2022/2065](#), 10 October 2025. See also the report: European Commission, [Special panel on child safety online](#), July 2026.

guardians that the current level of privacy, safety and security online of minors is often inadequate. The design and features of the wide variety of online platforms and the services offered by providers of online platforms accessible to minors may create risks to minors' privacy, safety and security and exacerbate existing risks. These risks include, for example, exposure to illegal content and harmful content, that undermines minors' privacy, safety and security or that may impair the physical or mental development of minors. They also include cyberbullying or contact from individuals seeking to harm minors, such as those seeking to sexually abuse or extort minors, human traffickers and those seeking to recruit minors into criminal gangs or promote violence, radicalisation, violent extremism and terrorism. Minors may also face risks as consumers as well as risks related to extensive use or overuse of online platforms and exposure to inappropriate or exploitative practices, including in relation to gambling and gaming. The increasing integration of artificial intelligence ('AI') chatbots and companions into online platforms as well as AI driven deep fakes may also affect how minors interact with online platforms, exacerbate existing risks, and pose new ones that can negatively affect a minor's privacy, safety and security. The increasing integration of artificial intelligence ('AI') chatbots and companions into online platforms as well as AI driven deep fakes may also affect how minors interact with online platforms, exacerbate existing risks, and pose new ones that can negatively affect a minor's privacy, safety and security.

Promoting children's privacy and autonomy also requires policies, laws and regulations that recognise children as independent holders of fundamental rights; ensure the protection of privacy beyond the protection of personal data; incorporate children's views and needs into public policymaking; and provide for independent and effective mechanisms of redress and sanctions in cases of violations of their rights.

The collection of children's biometric data should be permitted only exceptionally, where it is lawful, necessary, proportionate and fully compatible with the rights of the child. Their personal data must be processed fairly, accurately and securely, for a specific and

lawful purpose and in accordance with applicable data-protection standards¹⁷⁰.

The GNCHR highlights the United Nations recommendations on these issues, particularly those concerning the responsibilities of digital platforms. According to General Comment No. 25 (2021) of the United Nations Committee on the Rights of the Child¹⁷¹, States parties have an obligation to ensure that business enterprises respect and protect children's rights in the digital environment. To this end, States parties must adopt, monitor, enforce and evaluate legislation, regulations and policies to prevent digital networks and services from being used in ways that cause or facilitate violations of children's rights, particularly the right to protection from all forms of violence. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats. States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children. They should also establish effective mechanisms to prevent, monitor and investigate violations of children's rights by business enterprises, and to impose sanctions where such violations occur. In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. They should promote innovation in the best interests of the child and ensure that terms of service and other relevant information are provided to children, or to their parents and caregivers, in a form

170. UN/Special Rapporteur on the right to privacy, [Artificial intelligence and privacy, and children's privacy](#), Report, A/HRC/46/37, 25 January 2021, p. 22.

171. UN CRC, [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), 2 March 2021.

that is understandable and appropriate to their age and evolving capacities.

The GNCHR has emphasised the importance of children's digital rights, the obligations of the State and the private sector, and the links between the Charter of Children's Digital Rights and relevant international and European legal instruments and policies¹⁷². This threefold framework provides a basis for giving practical effect to children's digital rights.

Finally, with regard to cyberbullying, the Ministry of Digital Governance¹⁷³ recommends the establishment mechanism for the prevention and detection of cyberbullying, making use of artificial intelligence, big data and the combination of technology and human oversight. Drawing on its work and mandate as a National Human Rights Institution, the GNCHR underlines that hearings with children¹⁷⁴ must be a sine qua non tool for the implementation of relevant policies.

3.11 Persons with disabilities' rights and artificial intelligence

3.11.1 Introduction

AI offers significant opportunities to advance the rights of persons with disabilities, by enhancing accessibility, autonomy and equal participation in education, employment, health care and social life. Applications such as assistive communication systems, speech- and image-recognition technologies, smart digital assistants and

172. GNCHR, [The GNCHR at the hearing of the National Bioethics and Technoethics Commission on the "Charter of Children's Digital Rights"](#), 29 April 2025. For the analysis on social media, see GNCHR, [GNCHR observations on the Ministry of Justice draft bill on SLAPPs](#), 27 July 2026, p.14 et seq.

173. Ministry of Digital Governance, National Strategy for the [Protection of Minors from Internet Addiction](#), 2025, pp. 35.

174. GNCHR, [Online hearing of children held by the GNCHR on the situation of children's rights in Greece](#), 9 February 2026. GNCHR, [Hearing of children at the GNCHR premises on the situation of the rights of the child in Greece in Greece](#), 23 December 2025.

personalised support tools can reduce barriers faced by persons with disabilities and significantly improve their quality of life.

At the same time, the development and use of AI raise significant challenges for the protection of the rights of persons with disabilities, particularly where systems are not designed with accessibility in mind or where incomplete or biased data reproduce discrimination and exclusion. Therefore, the use of AI must be accompanied by appropriate safeguards to ensure transparency, equality, non-discrimination and the meaningful participation of persons with disabilities in the design and assessment of such technologies, so that innovation contributes to their empowerment rather than their exclusion.

3.11.2 Challenges associated with human rights

Uncritical acceptance of the results generated by flawed algorithms can have serious repercussions for human rights. For example, software used to inform decisions on health care and disability benefits has wrongfully excluded people entitled to those benefits, with serious consequences for the individuals concerned¹⁷⁵.

Eligibility for benefits, such as unemployment assistance, can be restricted by artificial intelligence using biased data sets and discriminatory algorithms¹⁷⁶. With a large number of persons with disabilities living in poverty across the world, many in extreme poverty, it is crucial that artificial intelligence systems do not improperly deny persons with disabilities their eligibility for services and support. The employment domain is increasingly dominated by artificial intelligence tools that can have a strong impact on persons with disabilities. Artificial intelligence tools can exclude candidates at each stage of the hiring process. For example, chatbots used

175. Council of Europe, [Safeguarding human rights in the era of artificial intelligence](#), 3 July 2018.

176. UN – Special Rapporteur on the rights of persons with disabilities, [Artificial intelligence and the rights of persons with disabilities](#), A/HRC/49/52, 28 December 2021, p. 9.

in interviewing that are enabled by artificial intelligence may be inaccessible to someone using a screen reader¹⁷⁷.

Faulty AI risk assessments based on certain disability types can also lead to improper increases in health insurance premiums¹⁷⁸. The lack of transparency as to the underlying logic used by ML and automated decision-making poses significant issues for the general population. Moreover, it is likely to impact persons with disabilities who are already marginalised in health and life insurance markets.

While the use of AI by individuals with disabilities, e.g. text-to-speech or real-time captioning, tends to be positive, institutional use of AI-powered human resources technology, e.g. filtering out persons with “non-standard” faces or speech patterns, tends to disadvantage and exclude job seekers and workers with disabilities¹⁷⁹. As a contribution to creating fair and efficient labour markets, AI developers and buyers of AI-powered employment tools need to address disability-based discrimination and its impacts on an organisation’s talent pool, workforce and customers. AI-related regulation needs to catch up on the existing disability equality gap and ensure AI tools are applied in a non-discriminatory way before they reach consumers, which includes both human resources departments of employers and consumers with disabilities.

3.11.3 Perspectives and recommendations

AI development and the digitalisation of the labour market offer significant opportunities to improve the employability and working conditions of persons with disabilities. At the same time however, they may deepen social and economic exclusion unless the digital divide is effectively addressed. The European Economic and Social

177. *Ibid* p. 10.

178. ENNHRI - Jerena Turin (guest blog), [Artificial intelligence and its impact on the human rights of persons with disabilities](#), 3 December 2023.

179. ILO, [AI's double-edged sword: A new frontier for employment of people with disabilities?](#), 6 October 2025.

Committee¹⁸⁰ notes that, since most jobs today require digital skills, the limited digital training and the more difficult access of persons with disabilities to technological tools and the internet make it necessary to strengthen investment in education, digital skills and their inclusion in education and training, also by making use of accessible AI applications, without replacing inclusive education.

At the same time, AI systems used for recruitment, employee evaluation and biometric identification may discriminate against persons with disabilities if they fail to take account of the particular features of their education and employment histories or of their reasonable accommodation needs. Automated systems used to screen CVs or recruit through inaccessible digital tools may unjustifiably exclude candidates with disabilities which makes human oversight and the provision of reasonable accommodation indispensable.

Finally, the disability dimension must be integrated at all stages of the design, development and assessment of AI systems. To this end, the participation of persons with disabilities themselves and of their organisations in the process of developing the relevant technologies is necessary, as is the enhancement of the education of programmers and engineers in matters of accessibility and inclusive design.

Recital 80 of the EU AI Act recognises that, as parties to the United Nations Convention on the Rights of Persons with Disabilities, the Union and the Member States are legally required to protect persons with disabilities from discrimination, promote their equality, ensure access on an equal basis with others to information and communication technologies and systems, and respect the privacy of persons with disabilities. Given the growing importance and deployment of AI systems, applying universal design principles to new technologies and services should ensure full and equal access for everyone who may be affected by, or use, AI technologies, including persons with disabilities, while fully taking account of their inherent

180. European Economic and Social Committee, [Inclusion of persons with disabilities in the context of the development of new technologies and AI – possibilities, challenges, risks and opportunities](#), 16 June 2025.

dignity and diversity. Providers must therefore ensure full compliance with applicable accessibility requirements, including those laid down in Directive (EU) 2016/2102 and Directive (EU) 2019/882. Providers should ensure compliance with those requirements by design. Accordingly, the necessary measures should be integrated, as far as possible, into the design of the high-risk AI system.

AI developers should actively involve persons with diverse disabilities, their representative organizations, and accessibility experts in the entire AI design, development, and testing lifecycle. This would help to ensure that tools are inherently unbiased, accessible and accurately assess candidates' potential¹⁸¹. AI must support, rather than replace, human judgement, with meaningful human oversight, clear accountability and effective scrutiny of decisions that affect persons with disabilities.

Furthermore, the ethical use of AI must be embedded into companies' broader disability inclusion strategies through appropriate training for managers and by enhancing the digital literacy for employees with disabilities, as well as strengthening the regulatory framework to ensure that artificial intelligence systems used in recruitment and employment processes are accessible, inclusive and free from discrimination on the grounds of disability.

3.12 Mass media, freedom of expression and artificial intelligence

3.12.1 Introduction

AI is rapidly transforming the way in which information is produced, disseminated and consumed, creating new possibilities for the mass media and for the exercise of freedom of expression. Its use may contribute to the automation of journalistic processes, the improvement of access to information, the faster processing of large volumes of data and the development of innovative forms of information and of civil participation in public debate.

181. ILO, *AI's double-edged sword: A new frontier for employment of people with disabilities?*, 6 October 2025.

At the same time, AI raises significant challenges for freedom of expression and media pluralism as it may facilitate the dissemination of disinformation and false content, reinforce the algorithmic manipulation of information and affect the transparency of online platforms and content-promotion mechanisms. AI use in the media sector must therefore be accompanied by appropriate safeguards for transparency, accountability and freedom of expression, ensuring that technological innovation strengthens rather than restricts democratic public debate.

3.12.2 Challenges associated with human rights

The decision to implement journalistic AI systems in the newsroom is a strategic choice with important consequences for internal processes and workflows. The decision to implement journalistic AI systems can also have broader implications for society and the journalistic profession, including public perceptions of journalism, the quality and fairness of working conditions in the broader media ecosystem (including freelancers, photographers and illustrators, content moderators, fact checkers, etc.), as well as the shape of digital communication infrastructure, and the formation of new relationships and dependencies¹⁸².

Freedom of expression and information also face challenges. AI-driven moderation on platforms can inadvertently suppress legitimate forms of expression beyond legal requirements on hate speech and other unlawful forms of expression. Indeed, AI systems struggle to understand context and nuance within speech, and the use of bots introduces new possibilities for abuse and manipulation. At the same time, algorithms that rely on addictive design or create “echo chambers”, as may occur on certain social media platforms, can interfere with the free formation of users’ will without coercion or manipulation, with consequences for democratic participation, the

182. Council of Europe, Steering Committee on Media and Information Society (CDMSI), [Guidelines on the responsible implementation of artificial intelligence systems in journalism](#), 2023, p. 10.

free flow of information and the exercise of freedom of assembly and association through online platforms¹⁸³.

3.12.3 Perspectives and recommendations

Journalistic AI systems¹⁸⁴ can be used for many different tasks. AI systems more broadly can be used for other generic tasks common to other businesses and organisations (as well as being seamlessly embedded into office software, search engines, smartphones, and a wide range of other software and hardware). Journalistic AI systems, as defined above, can be used for news production, for example in data analysis for investigative journalism and factchecking. They can be used for automated text, video and audio generation as well as routine support tasks like translation and transcription. For dissemination, AI systems can be used to match content with audiences through personalisation and the use of news recommender algorithms, or to organise or customise content. Journalistic AI systems can also be a means to engage with the audience, for example through virtual assistants and chatbots, or new pricing models.

Some journalistic tasks lend themselves to automation more than others. Highly repetitive tasks that can be executed by following explicit instructions are often amenable to automation, whereas tasks that are variable or require expert judgment, creativity and discretion

183. ENNHRI, [Key human rights challenges of AI](#). See Council of Europe, [Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques and possible regulatory implications](#), 2018, p. 16-23.

184. Council of Europe, Steering Committee on Media and Information Society (CDMSI), [Guidelines on the responsible implementation of artificial intelligence systems in journalism](#), 2023, p. 7. “*Journalistic artificial intelligence system*” means artificial intelligence system directly related to the business or practice of regularly producing information about contemporary affairs of public interest and importance, including the research and investigation tasks that underpin journalistic outputs. This can include, but is not limited to, large language models (LLM) and generative AI when used for journalistic purposes and/or news organisations. Journalistic AI systems are not a single technology but a range of different, often interlinked, tools for automating specific tasks.”.

are often less amenable to automation or at least require more human oversight and approval. In order to do much of the above, the news media often depends on external technology providers of AI systems, data, and computational infrastructures. The ability to innovate and use journalistic AI systems in accordance with professional ethics and human rights can contribute to the resilience of journalism in the digital age¹⁸⁵ and the role of journalists as defenders of human rights.

3.13 Democracy, elections, disinformation and artificial intelligence

3.13.1 Introduction

AI increasingly affects democratic processes, public debate and the conduct of elections, creating new possibilities but also significant challenges. Its use may support more effective data analysis, improve the information available to citizens, strengthen participation in democratic processes, and enable the earlier detection of disinformation and manipulation of public debate.

At the same time, AI entails serious risks for democracy as it may facilitate the mass production and dissemination of misleading content, the creation of false multimedia content (deepfakes), targeted political manipulation and opaque influence on electoral behaviour through algorithmic systems. Therefore, the use of AI requires effective safeguards for transparency, accountability and the protection of electoral integrity, so that technological innovation strengthens democratic participation and public trust in democratic institutions.

3.13.2 Challenges associated with human rights

The increase in the use of AI and automated decision making in the public sector raises several issues, among them accountability, transparency and the risk of discrimination. Without adequate safeguards in place, technology can adversely affect the enjoyment of individual rights and freedoms, for instance as regards privacy and

185. *Ibid* p. 9

data protection or the right not to be subjected to discrimination, on any ground, including digital literacy or access. There are two points of view regarding the impact of AI on turnout and voter choice: some promote AI in electoral processes through personalised advertising as a legitimate venue for conveying voter information and promoting voter education (including through micro-targeting campaigns)¹⁸⁶. Others argue that the use of AI should always be restricted in electoral processes as they could also be a way of increasing voter manipulation, including through micro-targeting, and could represent a potential danger of manipulating and narrowing the political offer. The objective is in fine to guarantee fair electoral processes by enabling voters to form and express their votes in an informed and free manner.

3.13.3 Perspectives and recommendations

AI may contribute to ensuring the integrity of electoral processes, promoting a more balanced presentation of information content, facilitating the detection of biased information and harmful content, as well as the detection of known forms of disinformation, including through automated tools. The focus should shift from simply labelling AI-generated content to certifying the provenance of the original source, as this is the most effective way of protecting against deepfakes¹⁸⁷.

186. Council of Europe, Steering Committee on Democracy (CCDEM), [Study on the impact of digital transformation on democracy and good governance](#), CDDG(2021)4 Final, 26 July 2021, pp. 4-5, Council of Europe, European Commission for Democracy through Law (Venice Commission), [Conclusions 2022 – 19th European Conference of Electoral Management Bodies \(EMBs\) “Artificial intelligence and electoral integrity”](#), 14-15 November 2022. See Algorithm Watch, [AI Chatbot produces misinformation about elections](#), 2023. The contribution made by the National Council for Radio and Television was taken into account during the public hearing of stakeholders and persons concerned on Artificial Intelligence and Human Rights. See GNCHRGNCHR, [Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026.

187. Having considered the contribution made by Giannis Assael, Special Adviser at the Ministry of Digital Governance and member of the National

At the same time, AI may help keep voters better informed, contribute to increasing voter participation and political inclusion, and support a better understanding of voting behaviour and the optimisation of the electoral process. However, its use must rely on anonymised personal data and ensure the protection of personal data and respect for the secrecy of the ballot. Accordingly, the right to free elections¹⁸⁸ is a fundamental right of particular importance in this context, as acknowledged, *inter alia*, in Article 3 of Protocol No. 1 to the European Convention on Human Rights.

3.14 Environment and artificial intelligence

3.14.1 Introduction

AI is emerging as a key tool for environmental protection and the promotion of sustainable development, given that it can support the monitoring of ecosystems, the tackling of climate change, the management of natural resources and the prevention of natural disasters by analysing large volumes of data and developing advanced predictive systems. Its use offers significant opportunities for more effective environmental policies and for evidence-based decision-making grounded in scientific data.

At the same time, the development and use of AI raise significant environmental and regulatory challenges, including the high consumption of energy and natural resources involved in developing and operating AI systems, and the need to ensure transparency, accountability and fair deployment of these technologies. Therefore, the integration of AI into environmental policy should be guided by the principles of sustainability, precaution and environmental protection, to ensure that technological innovation makes a meaningful

Council for Research, Technology and Innovation, observed during the hearing on Artificial Intelligence and Human Rights. See GNCHR [Greek National Commission for Human Rights, Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026.

188. See Council of Europe, [Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques and possible regulatory implications](#), 2018, pp. 30-32.

contribution to environmental governance. Consequently, the development of AI leads to enormous use of energy, water and land, raising environmental and equity challenges throughout its global infrastructure.

3.14.2 Challenges associated with human rights

The rapid growth of AI is driving an unprecedented expansion of data centres, significantly increasing electricity demand, carbon emissions and water use. This creates serious challenges for decision-makers seeking to balance technological competitiveness with environmental and societal sustainability. Projected global data centres' electricity consumption could exceed 945 Twh by 2030, accounting for almost 3% of projected global electricity use –with an associated water footprint of approximately 9.3 billion cubic metres annually¹⁸⁹. Nevertheless, it is necessary to focus on the environmental footprint of AI also as a challenge of governance and justice, and not solely as a technical problem¹⁹⁰.

The potential problems for human rights and the environment extend beyond resource intensity. Water, a recognised human right, is already scarce and becoming more so. While AI will hopefully democratize information, it may also have the reverse effect: aiding in disseminating vast amounts of misinformation¹⁹¹. The effects of social media on political polarization are already well documented. With AI, anyone can quickly produce an article on any subject, which could flood the internet with misinformation. As Michael Khoo, Climate Disinformation Program Director at Friends of the Earth, says: We can see AI fracturing the information ecosystem just as we

189. UNU-INWEH, [Report: Aczel, M., Chamanara, S., Matin, M., Farsi, A., Marwala, T., Madani, K. Environmental Cost of AI's Energy Use: Carbon, Water and Land Footprints](#). United Nations University Institute for Water, Environment and Health (UNU-INWEH), Richmond Hill, Ontario, Canada, 3 June 2026.

190. *Ibid.*

191. GNHRE, [Issues and Opportunities for AI, The Environment, and Human Rights](#), 17 May 2024. The Guardian, [AI likely to increase energy use and accelerate climate misinformation – report](#), 7 March 2024.

need it to pull it back together.” This is a particular threat in the context of climate change, which is already engulfed by misinformation.

3.14.3 Perspectives and recommendations

In addition to other issues, the GNCHR has addressed environmental protection, the right to a healthy environment and the right to water¹⁹². The following three key recommendations arising from the GNCHR position on the right to water, which could also be applied within the specific context described above, are: ensuring that private individuals contribute to remedying the consequences of pollution when they are responsible for it, thereby applying the ‘polluter pays’ principle, as well as ensuring that water remains affordable, to ensure access to water of sufficient quantity and safe quality for all, without discrimination and on an equal basis, with particular care for vulnerable groups within the population.

Energy and resource efficiency are key measures. They are important not only for reducing emissions, but also for lowering costs for communities located near power-generation facilities and easing pressure on electricity grids¹⁹³. Technology for the common good would mean a society where digital tools are built first to meet actual

192. See for instance: GNCHR, [The right to a healthy environment: The GNCHR’s third seminar was held in the events hall of the Athens Bar Association](#)”, 12 November 2025. GNCHR, [Written contribution of the GNCHR to the Special Rapporteur on the right to a healthy environment](#), 30 April 2025. GNCHR, [Right to Water – GNCHR Recommendations for its effective protection](#), 2014. According to the Recommendations, there is not a single right to water but rather a range of rights relating to water. These rights include, among others: the right to water for life and survival; the right to clean drinking water; the rights to water and sanitation; the right to water as part of the right to an adequate standard of living; the right to water in connection with food and nutrition; the rights to water and sanitation in the context of the right to adequate housing; the right to water for preparing food and for food production; the right to water in connection with the right to development and the right to natural resources; and the right to water as a component of the right to a healthy environment.

193. UNEP, [How to make AI data centres more sustainable](#), 26 January 2026.

social and ecological needs, not to deepen billionaire control or chase speculative profit, and where AI is not treated as an automatic solution but used only when it is appropriate, justified and not more resource-intensive than simpler alternatives¹⁹⁴. “Green artificial intelligence” is a solution with significant benefits, can accelerate the “green transformation” and refers to making AI itself sustainable and resource-efficient, which is critical, since some applications of AI significantly increase the consumption of energy, minerals and water¹⁹⁵. WWF also uses AI applications, in collaboration with technology companies, local stakeholders, Indigenous Peoples and academic institutions, to protect and restore important ecosystems, including forests, and to monitor endangered species¹⁹⁶. At the same time, it develops automated detection systems to combat the illegal trafficking of wildlife at airports and ports, using scanning technologies similar to those used to identify other security threats.

The United Nations Environment Programme (UNEP) sets out five key recommendations¹⁹⁷. Firstly, countries can establish standardized procedures for measuring the environmental impact of AI; right now, there’s a dearth of reliable information on the subject. Secondly, with support from UNEP, governments can develop regulations that require companies to disclose the direct environmental consequences of AI-based products and services. Thirdly, tech companies can make AI algorithms more efficient, reducing their demand for energy, while recycling water and reusing components where feasible. Fourthly, countries can encourage companies to green their data centres, including by using renewable energy and offsetting their carbon emissions. Finally, countries can weave their AI-related policies into their broader environmental regulations.

194. Greenpeace, [The energy and environmental impact of AI and how it undermines democracy](#), 2 April 2026.

195. WWF, [Artificial Intelligence has great potential to accelerate the Green Transformation](#), 11 February 2025.

196. WWF, [Artificial intelligence and conservation - Harnessing the power of technology to protect nature](#).

197. UNEP, [AI has an environmental problem. Here’s what the world can do about that](#), 13 November 2025.

3.15 Discrimination, prejudice and artificial intelligence

3.15.1 Introduction

AI is having an ever-greater influence on decision-making in areas such as employment, education, health, public administration and the administration of justice, offering significant perspectives in terms of greater efficiency and objectivity. However, when AI systems are trained on biased or unrepresentative data, or developed without adequate safeguards, they may reproduce or even amplify existing stereotypes and discrimination on grounds of gender, race or ethnic origin, age, disability, religion, sexual orientation, gender identity or other protected characteristics. At this point particular emphasis should be placed on the rights of Roma and LGBTQI+ people as vulnerable groups within the context of the AI.

Consequently, significant challenges arise regarding the protection of the right to equality and non-discrimination, as well as related fundamental rights, such as human dignity, the protection of personal data, equal access to goods and services, and the right to effective judicial protection. At the same time, AI can serve as a tool for identifying and mitigating discrimination, provided it is developed and used with transparency, accountability, human oversight and systematic monitoring of algorithmic bias, thereby reinforcing equal treatment and respect for fundamental rights.

3.15.2 Challenges associated with human rights

However, because algorithms simply present the results of calculations defined by humans using big data collected from humans, machines, or a combination of the two (at some point during the process), they reflect and process the human biases that are incorporated when the algorithm is programmed, when it processes data and when humans interact with it. In a nutshell, algorithmic bias happens when seemingly innocuous programming takes on the prejudices either of its creators or the data it is fed¹⁹⁸.

198. Council of Europe, Gender Equality Commission / CDADI, [Study on the impact of artificial intelligence systems, their potential for promoting](#)

AI systems can reinforce gender stereotypes, presenting major challenges for the working lives of women. This includes AI systems used in the workplace, government and rental spaces, etc, or at home. In domestic settings, AI systems might rely on certain gendered stereotypes around care and assistance and create an unequal and unconstructive model of flexible working, which reinforces the narrative of women primarily doing care and domestic work¹⁹⁹.

So how do these AI systems/algorithms become ‘biased’? The general answer is simple enough: the bias itself and the resulting discrimination is pervasive in society, rooted in psychological, social and cultural dynamics, and hence reflected in the data and texts that are used for developing AI models. The use of algorithms to support decision-making processes is often portrayed as rational and neutral. But machines and technology are not neutral, because they are developed and used by humans. Where bias is present in human decision-making, it may be transferred to machines. AI can not only reproduce but also reinforce existing biases, leading to discrimination and the exclusion of a person or group based on protected characteristics, such as ethnic origin, gender, religion, colour or sexual orientation²⁰⁰. Therefore, AI systems need to be developed in a way that deliberately and systematically seeks to remove or reduce bias throughout the process, from data collection and analysis to the reporting and assessment stages²⁰¹.

The right not to be discriminated against is at increased risk because AI systems tend to exacerbate existing social inequalities by targeting already vulnerable groups. Technologies such as facial recognition and language modelling have shown prejudice against racial and ethnic minorities, leading to injustices such as false

equality, including gender equality, and the risks they may cause in relation to non-discrimination, 2023, p. 15.

199. UNESCO – OECD – IDB, *The effects of AI on the Working lives of Women*, 2022, p. 26.

200. FRA, *Bias in Algorithms- Artificial Intelligence and Discrimination*, Report, 2022, p. 17.

201. IOM, *World Migration Report*, Chapter 11 - Artificial intelligence, migration and mobility: implications for policy and practice, 2022 p. 19.

arrests and accusations. Additionally, the opacity of and interests served by AI systems can perpetuate manipulative practices. Finally, AI systems further marginalise certain groups, such as people who are not digitally literate or people with disabilities²⁰². Issues relating to hate speech spread on the internet and on social media can also have serious implications, a phenomenon which can even lead to racist crime²⁰³.

3.15.3 Perspectives and recommendations

AI systems should recognise the existence of gender stereotypes and seek to challenge and transform them. AI Actors are enabled to change the way in which AI systems imitate or interact with gender stereotypes. For example, such systems should not reproduce biased associations between women and occupations related to care or assistance. However, if companies and societies frame and enforce these systems as allowing flexibility not just to women, but also to men, this could help change the narrative surrounding norms of parental and domestic responsibilities²⁰⁴.

Addressing AI-related discrimination requires the development and use of systems that incorporate the principles of equality, non-discrimination and inclusion from the design stage. The use of representative and high-quality datasets, the systematic assessment and checking for algorithmic bias, the transparency of models, the ability to explain their results, and the maintenance of meaningful

202. ENNHRI, [Key human rights challenges of AI](#). Council of Europe, [Algorithms and Human Rights – Study on the human rights dimensions of automated data processing techniques and possible regulatory implications](#), 2018, pp. 26-28.

203. See the work of the Racist Violence Recording Network (RVRN) coordinated by the GNCHR, as well as the GNCHR's broader work in the context of the Stand-Up, EXODUS and ECOSYSTEM projects, available on the GNCHR website. See also GNCHR, [GNCHR meeting with the Hellenic Telecommunications and Post Commission \(EETT\) on issues concerning misinformation, hate speech and platforms](#), 22 May 2026.

204. UNESCO – OECD – IDB, [The effects of AI on the Working lives of Women](#), 2022, p. 27.

human oversight over decisions that affect fundamental rights constitute key challenges that must be addressed. At the same time, the regulatory framework and accountability mechanisms must be strengthened, fundamental rights impact assessments must be carried out, effective judicial and administrative protection for affected persons must be ensured, and social actors and groups representing vulnerable categories must participate in the design and assessment of AI systems. Promoting diversity within development teams, training users and continuously monitoring system impacts can help reduce algorithmic bias and enhance trust in AI.

These considerations are especially important in light of intersectional discrimination and discrimination based on sexual orientation or gender identity, which can have serious consequences for the rights of LGBTQI+ persons²⁰⁵. AI may affect the rights of LGBTQI+ persons, as systems trained on biased or non-representative data may reproduce social prejudices, leading to discrimination in areas such as employment, health, insurance or access to services. Conversely, the responsible development and oversight of AI systems can help safeguard equality and non-discrimination through transparency mechanisms, risk assessment and the integration of human rights in the design stage.

205. See UNIA, [Artificial Intelligence and discrimination](#). GNCHR, [Participation of the GNCHR in an educational event of the Greek AI Network \(GAIN\) and Homo Digitalis on Artificial Intelligence](#), 23 December 2025 with a presentation on discrimination and artificial intelligence. GLAAD, [Build for Everyone: A Framework for LGBTQ Representation and Safety in AI](#), 2026.



Homo Digitalis, Participation of the GNCHR in an educational event of the Greek AI Network (GAIN) and Homo Digitalis on Artificial Intelligence

3.16 AI business and human rights

3.16.1 Introduction

AI is transforming the way in which businesses operate, creating significant potential for the enhancement of productivity, innovation, the automation of processes and informed business decision-making. Its use is expanding across a wide range of activities, such as human resources management, customer service, data analysis, supply chain and the development of new products and services. At the same time, the use of AI in business raises considerable challenges for the protection of human rights, including the risk of discrimination in employment relationships, the protection of privacy and personal data, the transparency and accountability of automated decision-making, and respect for human dignity and the rights of workers and consumers. The responsible development and use of AI, in accordance

with the principles of human rights due diligence²⁰⁶, is a fundamental prerequisite for ensuring that technological innovation is aligned with sustainable and socially responsible business conduct.

3.16.2 Challenges associated with human rights

The right to a private life²⁰⁷ is threatened by the constant tracking and surveillance that AI systems use for data collection. The lack of transparency about how AI systems operate creates uncertainty for individuals, whose data can reveal not only their interests but also their vulnerabilities. Companies possess extensive knowledge about users, while users remain uncertain about how their data is used and whose interests it serves.

The development and deployment of AI systems worldwide continue to raise significant human rights challenges, in particular owing to the risk of misuse of the relevant technologies by third parties and the absence of uniform international standards based on human rights principles. These challenges go beyond compliance with existing legal obligations and underline the need to apply the international standards on business and human rights to AI as well. To protect human rights along the entire supply and value chain, companies urgently need to integrate AI-specific risks into their existing corporate due diligence processes. They must also take appropriate measures to reduce human rights risks pre-emptively and to develop appropriate mitigation measures²⁰⁸. Companies that develop or use AI may be indirectly complicit in human rights violations (e.g., restriction of freedom of expression, discrimination against minorities), either through international cooperation or by providing technology, data, or software solutions to private and state actors. Another possibility is that human rights are not sufficiently

206. See for example GNCHR, [GNCHR Reference Report: “Human Rights Due Diligence. Responsible State and Business Conduct under Directive \(EU\) 2024/1760”](#), February 2025 and section “[Business and Human Rights](#)” on the GNCHR webpage.

207. ENNHRI, [Key human rights challenges of AI](#).

208. Global Compact Network Germany, [Report on Artificial Intelligence and Human Rights](#), 2024.

taken into account in the design of AI solutions, leading to adverse human rights consequences arising from the use of AI²⁰⁹.

3.16.3 Perspectives and recommendations

Corporate sustainability rests on a value system and a principles-based approach to doing business, under which companies must meet their fundamental responsibilities in the areas of human rights, labour, the environment and anti-corruption. By incorporating the Ten Principles of the UN Global Compact into strategies, policies and procedures, and establishing a culture of integrity, companies are not only upholding their basic responsibilities to people and planet but also setting the stage for long-term success²¹⁰. The Ten Principles of the United Nations Global Compact are derived from: the Universal Declaration of Human Rights, the International Labour Organization's Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development, and the United Nations Convention Against Corruption. Businesses are called upon to respect and protect internationally recognised human rights, not to contribute to their violation, to ensure freedom of association and the right to collective bargaining, to abolish all forms of forced and child labour and to eliminate discrimination in employment and occupation. At the same time, they are required to apply the precautionary principle in relation to environmental challenges, to promote environmental responsibility and to encourage the development and dissemination of environmentally friendly technologies.

In the context of an autonomous "AI Continent"²¹¹ and a State exercising digital sovereignty, it is important that AI systems and applications are developed by these actors themselves. Any excessive reliance on companies, other States or third parties may create dependencies that could lead to violations of broader aspects of human rights.

209. *Ibid* pp. 8-9.

210. United Nations Global Compact, [The Ten Principles of the UN Global Compact](#).

211. European Commission, [Shaping Europe's leadership in the field of artificial intelligence with the AI Continent Action Plan](#), 9 April 2025.

CHAPTER 4

The Principles of Artificial Intelligence as Safeguards for the Protection of Human Rights

4.1 Introduction

The GNCHR underlines the importance of an approach based on AI principles, as this makes it possible to address both the ethical and legal dimensions of AI²¹² and to understand how these principles relate to the corresponding human rights examined above under the thematic sections of this report. Accordingly, this chapter seeks to establish these connections by analysing the substance of the principles and selected examples of their application. References to AI principles also appear throughout the preceding chapters, alongside the discussion of challenges and opportunities for human rights. AI principles provide essential common ground and a shared language for all actors in the AI ecosystem, including public authorities, independent authorities, the technology sector, academia and civil society. While not all actors frame their work

212. GNCHR, [The GNCHR on ATHINA 9.84 radio on the legal and ethical dimension of artificial intelligence](#), 30 September 2025. See also examples of good practice, such as the one below, which refers to principles: UK, [Government Digital Service, Artificial Intelligence Playbook for the UK Government](#), February 2025.



explicitly through a human rights analysis, many refer to, and rely on, AI principles²¹³.

According to the EU AI Act and recital 27, although the risk-based approach constitutes the foundation for a proportionate and effective set of binding rules, it is important to recall the 2019 Ethics Guidelines for Trustworthy AI, developed by the independent AI HLEG appointed by the Commission²¹⁴. In these guidelines, the AI HLEG developed seven non-binding principles for AI that aim to help ensure the trustworthiness and ethical soundness of AI. The seven principles include (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability. Without prejudice to the legally binding requirements of the EU AI Act and any other applicable Union law, these guidelines contribute to the design of coherent, trustworthy and human-centric AI, in line with the Charter of Fundamental Rights of the European Union and the values on which the Union is founded.

Similarly, Articles 6–13 of the Council of Europe Framework Convention on Artificial Intelligence set out the principles applicable to activities within the AI system life cycle: human dignity and individual autonomy; transparency and oversight; accountability and responsibility; equality and non-discrimination; privacy and personal data protection; reliability; and safe innovation.

4.2 Principle of respect for human dignity and individual autonomy

The principle is enshrined in the Council of Europe Framework Convention on Artificial Intelligence, which in Article 7 provides that

213. This conclusion emerged during the public hearing on AI organised by the GNCHR. See above. Furthermore, the GNCHR also takes into account the work of the EU's European Group on Ethics in Science and New Technologies, including, for example: EGE, Values for the Future: The Role of Ethics in European and Global Governance, May 2021.

214. [European Commission High-level expert group on artificial intelligence | Shaping Europe's digital future](#), 6 May 2025.

each Party shall adopt or maintain measures to respect human dignity and individual autonomy in relation to activities within the life cycle of AI systems. The Explanatory Report to the Convention²¹⁵ highlights that activities within the life cycle of artificial intelligence systems should not lead to the dehumanisation of individuals, undermine their agency or reduce them to mere data points, or anthropomorphise artificial intelligence systems in a way which interferes with human dignity. Human dignity requires acknowledging the complexity and richness of human identity, experience, values, and emotions.

The Convention clarifies that respecting human dignity implies respecting the inherent value and worth of each individual, regardless of their background, characteristics, or circumstances and refers in particular to the manner in which all human beings should be treated. Since the dignity of the human person is universally agreed as constituting the basis of human rights, the reference to it as the first principle of Chapter III highlights the global character of the Framework Convention since all Parties recognise the inherent dignity of the human person as an underlying basis of human rights, democratic participation and the rule of law.

Individual autonomy is one important aspect of human dignity and refers to the capacity of individuals for self-determination; that is, their ability to make choices and decisions, including without coercion, and live their lives freely. In the context of AI, individual autonomy requires that individuals have control over the use and impact of AI technologies in their lives, and that their agency and autonomy are not thereby diminished. Human-centric regulation acknowledges the significance of allowing individuals to shape their experiences with artificial intelligence, ensuring that these technologies enhance rather than infringe upon their autonomy. The specific reference to individual autonomy is deemed necessary, particularly due to the capacity of these systems to mimic human behaviours and to influence or manipulate individuals.

215. Council of Europe, [Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law](#), 5 September 2024.

This is further illustrated by the data-protection framework under the Amending Protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data²¹⁶, which replaces the third recital of the Convention's preamble with the following: "Considering that it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control his or her personal data and the processing of such data."

Likewise, respect for the dignity of the individual²¹⁷ is embedded throughout Regulation (EU) 2024/1689. However, this concept becomes more necessary in Article 5 thereof concerning prohibited AI techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons.

Correspondingly, the World Health Organization²¹⁸ underlines that human dignity and the inherent worth of human beings are the central values on which all other ethical principles are based. It approaches the relationship between health and artificial intelligence through fundamental ethical principles governing the development, implementation and continuous evaluation of AI technologies in the health sector. These principles include the avoidance of causing harm, the promotion of well-being by minimising risks and maximising benefits, the fair treatment of all persons without discrimination, neglect, manipulation, domination or abuse, as well as respect for the autonomy of persons in making decisions concerning their life

216. Law 5169/2025 (Official Government Gazette 4 A 17.1.2025) Ratification of the Amending Protocol of 10 October 2018 to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

217. See recitals 27, 28, 31, 48, 58, 80.

218. World Health Organization, [Ethics and Governance on Artificial Intelligence for Health](#), 2021, p. 23 et seq.

and health, on the basis of adequate information on the nature, significance and possible consequences of the available options.

In this context, the World Health Organization²¹⁹ points out that the increasing use of AI must not shift decision-making from humans to machines. The principle of autonomy requires that any extension of machine autonomy not undermine human autonomy. In the context of health care, this means that humans should remain in full control of health-care systems and medical decisions AI systems should be designed demonstrably and systematically to conform to the principles and human rights with which they cohere; more specifically, they should be designed to assist humans, whether they be medical providers or patients, in making informed decisions. Human oversight may depend on the risks associated with an AI system but should always be meaningful and should thus include effective, transparent monitoring of human values and moral considerations. In practice, this could include deciding whether to use an AI system for a particular health-care decision, to vary the level of human discretion and decision-making and to develop AI technologies that can rank decisions when appropriate (as opposed to a single decision).

Respect for autonomy also entails the related duties to protect privacy and confidentiality and to ensure informed, valid consent by adopting appropriate legal frameworks for data protection. These should be fully supported and enforced by governments and respected by companies and their system designers, programmers, database creators and others. AI technologies should not be used for experimentation or manipulation of humans in a health-care system without valid informed consent. The use of machine-learning algorithms in diagnosis, prognosis and treatment plans should be incorporated into the process for informed and valid consent. Essential services should not be circumscribed or denied if an individual withholds consent and that additional incentives or inducements should not be offered by either a government or private parties to individuals who do provide consent. Data protection laws are one means of safeguarding individual rights and place

219. *Ibid.*

obligations on data controllers and data processors. Such laws are necessary to protect privacy and the confidentiality of patient data and to establish patients' control over their data. Construed broadly, data protection laws should also make it easy for people to access their own health data and to move or share those data as they like. Because ML requires large amounts of data – big data – these laws are increasingly important.

4.3 Principle of human-centric AI

The principle of human-centric AI is directly linked to the principles set out above and constitutes a fundamental pillar of the European and international regulatory framework. Recital 6 of the Regulation (EU) 2024/1689 on artificial intelligence already makes clear that AI should be developed and used through a human-centric approach, with the ultimate aim of increasing human well-being. This principle is also expressly enshrined in Article 1 of the Regulation, which provides that the development and use of trustworthy AI systems must be human-centric.

In the same spirit, the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) provides that human rights, fundamental freedoms and human dignity must be respected, protected and promoted throughout the life cycle of AI systems. More specifically, it is stated that no individual or social group should suffer physical, economic, social, political, cultural or mental harm as a result of the development or use of AI systems, while their use should contribute to improving people's quality of life.

At the same time, it is recognised that persons may interact with AI systems throughout their life cycle and receive assistance from them, such as care for vulnerable people or people in vulnerable situations, including but not limited to children, older persons, persons with disabilities or the ill. Within such interactions, persons should never be objectified, nor should their dignity be otherwise undermined, or human rights and fundamental freedoms violated or abused.

Finally, UNESCO stresses that human rights and fundamental freedoms must be respected, protected and promoted throughout

the life cycle of AI systems. Governments, private sector, civil society, international organisations, technical communities and academia must respect human rights instruments and frameworks in their interventions in the processes surrounding the life cycle of AI systems. New technologies need to provide new means to advocate, defend and exercise human rights and not to infringe them

4.4 Principle of respect for privacy and data governance

The principle of respect for privacy and data governance constitutes a core element of Regulation (EU) 2024/1689. Citizens must retain full and effective control over their personal data, which must not be used in a manner that causes them harm or introduces discrimination against them. In this context, the Regulation recognises that general-purpose AI models may entail systemic risks and provides that, where those risks exceed the applicable threshold, providers of the relevant models are subject to additional risk-management obligations.

For high-risk AI systems, the Regulation provides that, before they are put into service, an assessment of their impact on fundamental rights must be carried out in order to ascertain that such impacts are not disproportionate to the expected benefits²²⁰. The assessment concerning the inclusion of a practice among high-risk applications must be documented before the relevant system is placed on the market, with a view to ensuring guarantees for the protection of the privacy of future users. More broadly, the EU AI Act requires AI systems to be developed and used in accordance with the rules on the protection of personal privacy and personal data, while the data governance must meet high requirements of quality and integrity.

The UNESCO Recommendation on the Ethics of Artificial Intelligence emphasises that privacy is an essential prerequisite for the protection of human dignity, human autonomy and human agency. Data used by AI systems must be collected, used and deleted in accordance with

220. GNCHR, [The GNCHR on the Human Rights Impact Assessment of Artificial Intelligence systems at a Conference of the University of Piraeus](#), 27 June 2025. GNCHR, [The GNCHR at the ENNHRI FRIA for Artificial Intelligence Webinar](#), 11 April 2025.

international law and the principles of the Recommendation. At the same time, stress is placed on the need to establish an appropriate data protection framework and governance mechanisms, including impact assessments that take into account the social and ethical dimensions of the use of artificial intelligence systems, as well as the need to ensure the accountability of the relevant actors. UNESCO further observes that Respect, protection and promotion of diversity and inclusiveness should be ensured throughout the life cycle of AI systems, consistent with international law, including human rights law. This may be done by promoting active participation of all individuals or groups regardless of race, colour, descent, gender, age, language, religion, political opinion, national origin, ethnic origin, social origin, economic or social condition of birth, or disability and any other grounds. It further states that algorithmic systems require adequate privacy impact assessments, which also include societal and ethical considerations of their use and an innovative use of the *privacy by design approach*. AI Actors need to ensure that they are accountable for the design and implementation of AI systems in such a way as to ensure that personal information is protected throughout the life cycle of the AI system.

Article 11 of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law provides that Each Party shall adopt or maintain measures to ensure that, with regard to activities within the life cycle of artificial intelligence systems: (a) privacy rights of individuals and their personal data are protected, including through applicable domestic and international laws, standards and frameworks; and (b) effective guarantees and safeguards have been put in place for individuals, in accordance with applicable domestic and international legal obligations. The Explanatory Report notes that the protection of privacy and personal data constitutes a common principle for the effective implementation of the other principles of the Convention, since the collection and processing of personal data have become a key element of both commercial activity and the functioning of public authorities. Given that AI systems are based primarily on

data processing, the absence of appropriate safeguards may create serious risks for individuals' privacy.

The Convention further notes that the protection of privacy includes, *inter alia*, limiting access to a person's personal experiences, protecting the confidentiality of personal matters, control over personal information and data, protection of personality, dignity and individual autonomy, and the protection of the private sphere and of physical, psychological and moral integrity. Finally, specific reference should be made to the importance of existing international and Union data-protection frameworks, such as the Council of Europe Convention 108+ and the GDPR – Regulation (EU) 2016/679. Correspondingly, the CJEU²²¹ points out that AI solutions which are developed or used must respect the right to privacy and the protection of personal data, ensuring that personal data are processed in a secure and ethically sound manner.

4.5 Principle of trustworthiness in artificial intelligence

The trustworthiness of AI systems constitutes a fundamental principle of both Regulation (EU) 2024/1689 and the Council of Europe Framework Convention on Artificial Intelligence. From its opening recitals, namely recitals 1, 2, 3, 27, 59 and 123, the Regulation emphasises that its purpose is to promote the uptake of human-centric and trustworthy AI, to make the Union a leader in the development of trustworthy AI systems, and to ensure that such systems are developed and used in a manner compatible with fundamental rights. It is also pointed out that the adoption of divergent national rules could lead to fragmentation of the internal market and diminish legal certainty, which makes it necessary to establish a uniform and high level of protection throughout the Union in order to ensure the development of trustworthy AI without hampering innovation and the free movement of AI systems. The Regulation also refers to the 2019 Ethics Guidelines for Trustworthy AI, which set out seven non-binding ethical principles intended to strengthen trustworthiness and the ethical development of AI.

221. CJEU, [Artificial Intelligence Strategy](#), 2023.

It further recognises that trustworthiness and transparency are essential to preventing adverse impacts, maintaining public trust, ensuring accountability and enabling effective redress. High-risk AI systems must therefore be subjected to a conformity assessment before being placed on the market or put into service. In addition, Articles 1 and 50 of the EU AI Act require providers to ensure that their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible.

Correspondingly, Article 12 of the Council of Europe Framework Convention on Artificial Intelligence provides that each Party shall take, as appropriate, measures to promote the reliability of artificial intelligence systems and trust in their outputs, which could include requirements related to adequate quality and security throughout the life cycle of artificial intelligence systems. The Explanatory Report to the Convention highlights the role of technical standards, technical specifications, assurance mechanisms and conformity-assessment systems in documenting and verifying the reliability of AI systems. Particular emphasis is placed on ensuring the robustness, safety, security, accuracy and performance of systems, as well as the quality, integrity and security of data, and cybersecurity. The relevant standards must be developed through transparent and participatory processes, in accordance with international and national standards for the protection of human rights.

The Convention further emphasises that AI systems should be “secure and safe by design”, so that security and safety constitute fundamental requirements at all stages of their life cycle and not merely technical features. In certain cases, laying down rules is not sufficient; clear and reliable information must also be provided to stakeholders concerning compliance by entities developing and using AI systems, through transparency, documentation and accountability mechanisms. Quality assurance and conformity assessment systems contribute both to compliance with regulatory requirements and to the assessment of broader risks, whilst technical standards work in a complementary manner to address technical risks and enhance the reliability of systems.

Finally, the CJEU²²² points out that, as the applicable legal and ethical standards are continuously evolving, AI solutions must be continuously updated in order to meet new legal and ethical requirements.

4.6 Principle of transparency

The principle of transparency constitutes a fundamental precondition for the lawful development and use of AI, yet its application presents significant difficulties. The information and access to personal data obligations provided for by the GDPR (Articles 12–15) become difficult to fulfil, particularly due to the use of large amounts of data the complexity of algorithms and the difficulty of determining in advance the purpose of the processing. Of particular importance is the obligation of the data controller to explain the logic of automated processing, both when informing the data subject and when exercising the right of access, so that understanding and challenging the decision taken becomes possible²²³.

Regulation (EU) 2024/1689 highlights transparency²²⁴ as a core principle of trustworthy and human-centric AI. AI systems must be developed and used in a manner that ensures their traceability and explainability, making it possible to clearly identify when a person is interacting with an AI system, and to inform both deployers about the capabilities and limitations and affected persons about their rights. The Regulation provides for specific transparency obligations for providers and deployers, including the publication of a sufficiently detailed summary of the data used during the pre-training of models, as well as periodic evaluation of the transparency and oversight framework by the European Commission. Consequently, transparency is not a one-dimensional concept but manifests itself

222. *Ibid.*

223. Panagopoulou Fereniki, [The European Regulation on Artificial Intelligence. A first look at the Constitutional-Ethical perspective](#), Centre of European Constitutional Law, Electronic edition, 2025, p. 51 *et seq.*

224. See recitals 26, 27, 54, 68, 72, 107, 174 and Article 50.

at various levels and concerns different aspects of algorithmic functioning²²⁵.

UNESCO, in its aforementioned Recommendation, highlights transparency and explainability as fundamental principles for trustworthy AI. Providers must provide information on training data, technical documentation and the functioning of systems, particularly when it comes to high-risk applications. Individuals must be informed when a decision is taken or supported by an AI system, be able to request an explanation of the decision and be assured of accountability, effective judicial protection and trust in the systems, subject to the necessary balancing against privacy, security and other legitimate interests.

Correspondingly, Article 8 of the Council of Europe Framework Convention on AI imposes the establishment of appropriate transparency and oversight requirements throughout the life cycle of AI systems. Providing transparency about an artificial intelligence system could thus require communicating appropriate information about the system (such as, for instance, purpose(s), known limitations, assumptions and engineering choices made during design, features, details of the underlying models or algorithms, training methods and quality assurance processes). At the same time, it is recognised that explainability and interpretability are subject to technical constraints and must be balanced against the protection of privacy, confidentiality, national security and other legitimate interests.

The OECD AI Principles recognise transparency and explainability as basic preconditions for the responsible use of AI. AI Actors must provide clear and comprehensible information about the capabilities and limitations of AI systems, make it known when a person is interacting with AI and, where feasible, provide information on the data, factors and logic that led to a prediction or decision, so that affected persons can understand and challenge the outcome. Transparency does not necessarily entail disclosure of source

225. Vorras Apostolos, The application of the principle of transparency in Artificial Intelligence, *Nomiki Bibliothiki*, 2026, p. 203.

code or protected data, while explainability must be adapted to the respective context, taking into account possible impacts on accuracy, privacy, security and the cost of systems.

Correspondingly, the World Health Organization²²⁶ points out that AI applications in health must be transparent and understandable for developers, users and supervisory authorities. Transparency requires the disclosure of information on the design, data, assumptions, limitations and functioning of systems before and after their deployment, so as to facilitate public accountability, scrutiny and the protection of public health. In parallel, explainability must be adapted to the capacities of the recipients, while systems must undergo regular, transparent testing and independent oversight, with assessment of their performance across different characteristics, such as race, nationality, sex and age, and with disclosure of the uses, limitations and the manner in which relevant decisions are taken.

Correspondingly, Law 4961/2022 imposed on public-sector bodies the obligation to publish information on the AI systems used, their capabilities and technical characteristics, the categories of decisions they support and the conduct of an algorithmic impact assessment, while ensuring the right of interested parties to receive, in a comprehensible and accessible form, the parameters on which the decision was based and providing for the maintenance of a register of AI systems and oversight by the National Transparency Authority²²⁷. At the same time, Law 5169/2025 (Chapter II, Article 5) enshrines transparent and lawful processing of personal data, while the Blueprint for Greece's transition to the age of AI²²⁸ underlines that algorithms, data and decision-making processes must be sufficiently

226. WHO, [Ethics and Governance on Artificial Intelligence for Health](#), 2021, p. 27 et seq.

227. See the corresponding provision in Law 5321/2026 and the GNCHR comments on the register during the parliamentary debate: GNCHR, [The GNCHR in Parliament on the Ministry of Digital Governance draft bill on artificial intelligence](#), 13 July 2026.

228. High-Level Advisory Committee on Artificial Intelligence Blueprint for Greece's AI Transformation, 2024 p. 15.

accessible and explainable, so that AI systems operate with reliability, accountability and responsibility.

4.7 Principle of equality and non-discrimination in access to information

It is necessary to highlight the importance of equitable access to information and open science, by promoting the free exchange of scientific knowledge, data, software and research results for the benefit of scientific cooperation and evidence-based decision-making. Access to the benefits and opportunities offered by AI must be equitable for all, irrespective of sex, race, nationality, disability, language, religion or any other characteristic, while any restrictions must be proportionate and justified by reasons such as the protection of human rights, privacy, national security and public order. AI systems must also be designed and used so as to prevent bias and ensure that no population group is subject to disproportionate or unfair treatment.

The Blueprint for Greece's AI Transformation²²⁹ places particular emphasis on equal access to education through the creation of a central online platform for AI educational material, with a view to widening access to high-demand knowledge and skills and reducing educational and socio-economic inequalities. The development of an open and sustainable learning ecosystem is intended to promote equality of opportunity and broader participation in AI education.

UNESCO's Recommendation and Article 10 of the Council of Europe Framework Convention on Artificial Intelligence²³⁰ underline that activities throughout the AI system life cycle must respect equality, including gender equality, diversity and the prohibition of discrimination, as provided under applicable international and national law. States and developers must ensure the meaningful

229. See p. 70.

230. See the Convention and Explanatory Report, paragraph 72, concerning the provisions of the United Nations Covenants and other United Nations conventions and international instruments intended to provide protection.

participation of all social groups, address the digital divide, and take measures to prevent and mitigate algorithmic bias, which may originate in the persons developing a system, its training data, its design or the operation of systems. At the same time, policies that address existing structural inequalities are needed to ensure that the development and use of AI lead to fair and equitable outcomes for all.

The OECD AI Principles²³¹ underline that the development and use of trustworthy AI must promote inclusive growth, sustainable development and human well-being. AI should strengthen human capabilities and creativity and support the participation of under-represented groups contributing to the reduction of economic, social and gender inequalities while protecting the environment. At the same time, the risk of reproducing or reinforcing existing biases against vulnerable groups is recognised, which makes responsible governance, multi-stakeholder cooperation and continuous public dialogue essential to building trust in AI. Correspondingly, the CJEU²³² points out that data and algorithms must be designed in accordance with the principles of impartiality, fairness and non-discrimination, in order to ensure equal treatment for all without discrimination on grounds of race, sex or socioeconomic status.

The United Nations²³³ likewise notes that AI's benefits remain unevenly distributed, concentrated in a small number of powerful companies and countries and warns that, without appropriate safeguards, AI may intensify inequalities, the digital divide and threats to human rights. This underscores the need for international cooperation and inclusive AI governance so that the benefits of AI are shared equitably and for the benefit of all.

In the same spirit, Law 4961/2022 imposed, in the design, development and operation of AI systems, compliance with the applicable legal framework and, in particular, with the protection of human dignity, private life and personal data; the prohibition of discrimination; gender equality; freedom of expression; universal accessibility for

231. See Article 1.1 and the explanation thereto [here](#).

232. See the above relevant source.

233. United Nations, [Artificial Intelligence, Global Issues](#).

persons with disabilities; workers' rights; and the principle of good administration.

4.8 Principle of proportionality

The principle of proportionality constitutes a fundamental pillar of Regulation (EU) 2024/1689 and runs through all its provisions, reflecting the need for AI systems to be developed and used in a manner proportionate to the intended purpose and to the risks that they may cause. This principle is reflected both in the recitals and in individual provisions of the Regulation, such as those concerning human oversight, conformity assessment and the imposition of penalties. In determining administrative fines, account must be taken of the nature, gravity and duration of the infringement; its consequences; any previous penalties; and the size and market position of the operator, so that the penalty is proportionate to the circumstances of the individual case.

The principle of proportionality is also embedded in the Greek and international regulatory framework. Law 5169/2025 provides that any processing of data must be proportionate to the legitimate purpose pursued and strike a fair balance between public or private interests and the fundamental rights and freedoms of individuals. At the same time, any restriction of rights is permitted only where it is provided for by law, respects the essence of fundamental rights and constitutes a necessary and proportionate measure in a democratic society. The UNESCO Recommendation on the Ethics of Artificial Intelligence likewise underlines that AI systems must not exceed what is necessary to achieve legitimate aims, instead they must be based on risk assessment, balance benefits against potential risks for individuals and society, rely on sound scientific evidence and always remain subject to final human judgement, in order to prevent harm and ensure respect for fundamental rights.

4.9 Principle of accountability and responsibility

The principle of accountability is a basic precondition for the trustworthy development and use of artificial intelligence. Regulation

(EU) 024/1689 stipulates that there must be mechanisms in place to ensure that providers and users of AI systems are held accountable for their effect on human rights, through procedures for monitoring, human oversight, risk management and the reporting of serious incidents. Auditability plays a central role, as it enables the assessment of algorithms, data and development processes, particularly in high-risk applications, while effective and accessible redress mechanisms must also be available. For the purposes of implementing the Regulation each Member State must designate national competent authorities, including at least one market surveillance authority and at least one notifying authority.

The principle of accountability is further reinforced by other international and national instruments. The Council of Europe Framework Convention on Artificial Intelligence²³⁴ requires Parties to adopt or maintain mechanisms ensuring accountability and responsibility for adverse impacts on human rights, democracy and the rule of law arising from activities within the AI system life cycle. Those mechanisms include administrative and judicial remedies, civil and criminal liability regimes, and procedures enabling affected persons to contest decisions and ensuring that responsibility can be clearly attributed to the relevant actors.

The UNESCO Recommendation on the Ethics of Artificial Intelligence states that actors developing and using AI must respect, protect and promote human rights, while ultimate ethical responsibility for decisions and actions based on AI systems always remains with the human actors involved in their life cycle. UNESCO further stresses that risks and vulnerabilities must be addressed throughout the AI system life cycle, ensuring that systems remain resilient against errors, misuse and cyberattacks.

Correspondingly, the OECD AI Principles (Section 1.5) provide that AI Actors should be accountable for the proper functioning of AI systems and for compliance with the relevant principles. They should ensure traceability in relation to datasets, processes and decisions throughout the AI system life cycle, and apply a systematic

234. See the Explanatory Report, paragraphs 66-70.

risk-management approach on an ongoing basis to address risks, including harmful bias and risks to human rights, safety, security, privacy, labour and intellectual property rights.

Law 4961/2022 provided for the mandatory maintenance of a register of artificial intelligence systems used by public bodies, containing information on the purpose, technical characteristics, security measures and impact assessments, as well as corresponding registers for Internet of Things devices and risk-assessment plans in telecommunications, while Law 5321/2026 established the necessary framework governing the register²³⁵. Correspondingly, the CJEU points out that AI systems should be governed by traceability, auditability and explainability in order to ensure their compliance with legal and ethical requirements. Furthermore, Article 5 of Law 4961/2022 established the mandatory preparation of an algorithmic impact assessment before AI systems are put into operation by public-sector bodies. The assessment covers, among other matters, the system's purpose and the public interest it serves; its technical characteristics and operating parameters; the categories of decisions it supports; the data it processes; and the potential risks it may pose to the rights, freedoms and legally protected interests of natural and legal persons. Particular emphasis is placed on the potential impact of AI systems on vulnerable groups, such as persons with disabilities or chronic illnesses, while it is clarified that the algorithmic impact assessment does not replace the data protection impact assessment under Article 35 of the GDPR.

4.10 Human oversight

AI is a dynamic and multidimensional technology, which evolves continuously and requires a correspondingly flexible and adaptive governance framework.²³⁶ Policy and regulatory approaches must adapt to the new opportunities, risks and social challenges that arise, while maintaining a stable and predictable environment of trust. Given

235. See the GNCHR comments, [The GNCHR in Parliament on the Ministry of Digital Governance draft bill on artificial intelligence](#), 13 July 2026.

236. See Panagopoulou F., *ibid* p. 53,

that the impacts of AI extend beyond national borders, its effective regulation requires international cooperation through organisations such as the European Union, the United Nations and the OECD²³⁷. This cooperation is essential to ensure that the development and use of AI systems are aligned with democratic values, human rights and the public interest.

Regulation (EU) 2024/1689 establishes human oversight as a fundamental principle, according to which AI systems must function as tools supporting human beings, with respect for human dignity, autonomy and fundamental rights. To this end, the Act provides for mechanisms ensuring transparency, assessment and continuous review of oversight requirements.

At the international level, the guiding principles of UNESCO and the OECD²³⁸ underline the importance of accountability, impact assessment, traceability, safety and continuous human oversight throughout the life cycle of AI systems. The establishment of conformity assessment bodies is essential for preventing human rights violations and enhancing trust. Keeping human judgement and intervention at the forefront is of particular importance, as AI must not operate without control but under constant human oversight. Furthermore, this framework is also linked to the code of ethics of the relevant professional groups; for example, IT professionals have an ethical obligation to prevent socially harmful uses of technology²³⁹.

At the same time, Law 4961/2022 had established national governance mechanisms through the Coordinating Committee for AI and the Committee for Oversight of the National Strategy, which have competence for coordination, implementation, improvement of the strategy and the addressing of deviations or potential impacts

237. *Ibid.*

238. See principles 1.2, 1.4.

239. The contribution of of the Hellenic Informatics Union was taken into account during the hearing of stakeholders on Artificial Intelligence and Human Rights. See GNCHR [Greek National Commission for Human Rights, Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026.

on citizens' rights. The need to establish strong and independent supervisory authorities is further reinforced by Law 5321/2026, as discussed in this report and in other GNCHR texts as well as by Law 5169/2025, and the relevant international data-protection framework, which provide for powers of investigation, intervention, imposition of penalties and informing citizens. Supervisory authorities must have sufficient resources, independent status and the capacity to cooperate, in order to ensure compliance with data protection principles and fundamental freedoms.

4.11 Principle of societal and environmental wellbeing

The development and widespread use of powerful generative AI models create significant environmental challenges, mainly due to increased consumption of energy, water and computing resources. Training large AI models, such as those with billions of parameters, requires high computing power, which entails increased carbon dioxide emissions and a burden on energy networks. At the same time, the ongoing operation, optimisation and large-scale use of AI applications increase their energy footprint, while cooling requirements place additional pressure on water resources and local ecosystems. For this reason, the environmental factor must be integrated from the outset into the design, development and governance of AI systems²⁴⁰.

Despite this environmental cost, AI can be an important tool for addressing climate change and promoting sustainable development. Through big-data analysis, satellite monitoring, smart energy systems and the optimisation of renewable energy sources, AI can contribute to more effective management of natural resources and to the prediction of environmental changes. However, solutions do not rely exclusively on AI, but require cooperation with complementary technologies, such as the Internet of Things, robotics, electric vehicles and distributed energy resources. The use of AI for environmental purposes must therefore be accompanied by an assessment of the overall life cycle of the systems and of the cost of data processing.

240. See Panagopoulou F. *Ibid* pp. 54-55.

The regulatory framework of the European Union, UNESCO and the OECD principles underline that the development of trustworthy AI must be aligned with the goals of sustainable development and environmental protection. Regulation (EU) 2024/1689 recognises the need to avoid applications that cause long-term societal or environmental impacts, while UNESCO and the OECD emphasise the obligation to limit the carbon footprint, unsustainable use of natural resources and impacts on ecosystems.

4.12 Awareness and literacy

Public awareness and understanding of AI technologies and the value of data constitute basic preconditions for their democratic and responsible use. According to UNESCO, access to open and inclusive education, the development of digital skills, education on the ethics of AI and media and information literacy are essential if citizens can make informed decisions and be protected from undue influence. Education on AI must be grounded in understanding of its impacts on human rights, fundamental freedoms, the environment and society. Similarly, the Greek Blueprint for the transition to the age of AI²⁴¹ underlines the need for equal participation of all citizens through access to knowledge, technology, computing resources and data, ensuring that AI governance reflects the views of all stakeholders.

Strengthening participation of citizens also presupposes the development of appropriate mechanisms for vocational training and specialisation in AI. The creation of regional education centres, cooperation between universities and industry, and the use of online learning platforms can help build a workforce with the skills needed for the digital era. Particular importance is also attached to the protection of cultural and linguistic heritage through the development of reliable Greek data and AI models²⁴². The dominance of online data by Anglophone cultures often leads to biased models that do not reflect global cultural diversity. For this reason, the creation of a data space for the Greek language and culture constitutes an important

241. *Ibid* p. 15.

242. *Ibid* p. 22.

initiative, so that AI systems incorporate reliable Greek sources, produce more accurate results and respond more effectively to the needs of Greek society.

The amendment of Article 4 of the EU AI Act by the Digital Omnibus Regulation for AI concerning AI literacy²⁴³, which potentially differentiates the obligations of providers and deployers of AI systems, does not fully satisfy the above requirements.

4.13 The principle of safe innovation

Article 13 of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law²⁴⁴ recognises the need to foster innovation while safeguarding human rights, democracy and the rule of law. To this end, each Party is called upon to enable, as appropriate, the establishment of controlled environments for developing, experimenting and testing artificial intelligence systems under the supervision of its competent authorities. These environments enable the early integration of quality, privacy, safety²⁴⁵ and fundamental rights protection requirements from the initial stages of systems design, since many

243. See also recital 8 of the Digital Omnibus and in particular: “(...) *experience shared by stakeholders reveals that a solution imposing stringent obligations to ensure a sufficient level of AI literacy would not be suitable for all types of providers and deployers in relation to the promotion of AI literacy. Moreover, data indicates that imposing such obligations creates an additional compliance burden, particularly for smaller enterprises, whereas AI literacy should be a strategic priority, regardless of regulatory obligations and potential sanctions.*”

244. See also explanatory report paragraphs 90-93.

245. As Mr Giannis Assael, Special Advisor at the Ministry of Digital Governance and member of the National Council for Research, Technology and Innovation, observed during the hearing on Artificial Intelligence and Human Rights, there is an urgent need to develop national evaluation metrics and of a National AI Safety Institute. A model that is safe in English is not necessarily equally safe in Greek. This can leave protection gaps at the local level. See GNCHR [Greek National Commission for Human Rights, Hearing of stakeholders on Artificial Intelligence and Human Rights](#), 29 January 2026.

of the risks associated with AI can be addressed more effectively before their wide-scale deployment.

The purpose of such mechanisms is not to constrain technological development, but to create a safe framework that enables responsible innovation. Controlled environments, including regulatory sandboxes, allow AI developers to test new applications in real-world conditions while benefiting from guidance provided by supervisory authorities. In this way, legal certainty is enhanced, cooperation between businesses, researchers and regulatory bodies is facilitated, and the collection of knowledge regarding the opportunities and risks of new technologies is enabled. At the same time, authorities may assess the effectiveness of different regulatory approaches and adapt the governance framework to the rapidly evolving developments in AI.

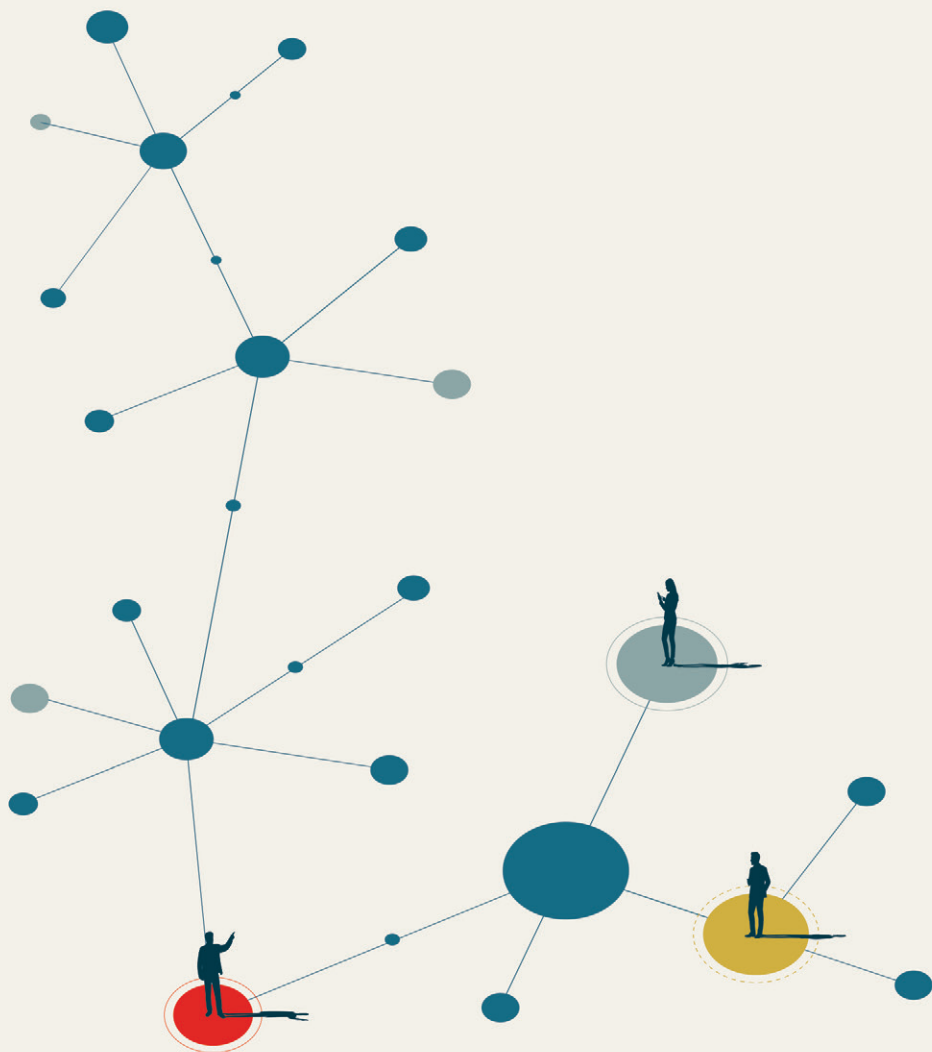
Controlled environments can therefore help strike a balance between innovation and the protection of the public interest. Continuous assessment, transparency and cooperation with stakeholders can strengthen public and market confidence in the use of AI. Particularly for smaller enterprises and organisations with limited resources, these frameworks may operate as mechanisms supporting compliance, reducing barriers to entry to innovation and promoting the development of AI systems that are safe, reliable and compatible with fundamental European values.

CHAPTER 5

The added value of the Greek National Commission for Human Rights in the context of artificial intelligence governance

5.1 Article 77 of EU Regulation 2024/1689 – Principles for the protection of fundamental rights and the role of the GNCHR

The GNCHR takes into account Article 77 of Regulation 2024/1689, as amended by Regulation 2026/1744, concerning the powers of the authorities responsible for the protection of fundamental rights. Article 77 should be interpreted in conjunction with the other relevant provisions of the EU AI Act, including Article 73(7) on the reporting of serious incidents; Article 78 on confidentiality; Article 79(2) on national procedures for dealing with AI systems presenting a risk; and Article 82 2(1) on compliant AI systems presenting a risk. Account should also be taken of Article 6, “Classification rules for high-risk AI systems”, and Annex III, “High-risk AI systems referred to in Article 6(2)”, particularly as regards biometrics; critical infrastructure; education and vocational training; employment, workers management and access to self-employment; access to and enjoyment of essential private services and essential public services and benefits; law enforcement; migration, asylum and border-control management; and the administration of justice and democratic processes.



5.2 List of national authorities referred to in Article 77 of the Regulation

According to a Ministry of Digital Governance press release entitled “Authorities Protecting Fundamental Rights in Relation to the Use of Artificial Intelligence in Greece”²⁴⁶, the Ministry has published, in the context of the EU AI Act, a list of national authorities and bodies that enforce or monitor compliance with Union obligations protecting citizens’ fundamental rights, including the right to non-discrimination, in relation to the use of high-risk AI systems. By compiling and publishing this list, Greece has fulfilled the first national obligation for implementing the EU AI Act at national level. As the press release states, Greece fully and actively supports the European Union’s vision for the uptake of human-centric and trustworthy AI, while fostering innovation and ensuring a high level of protection of health, safety and fundamental rights. The authorities included in the list are as follows: the Hellenic Data Protection Authority (HDPa); the Greek Ombudsman; the Hellenic Authority for Communication Security and Privacy (ADAE); and the Greek National Commission for Human Rights (GNCHR).

As the press release explains, the authorities listed above will receive additional powers, including access to any documentation created or maintained by an organisation to demonstrate compliance with the EU AI Act, where such access is necessary for the effective fulfilment of those authorities’ mandate and within the limits of their jurisdiction. The list was notified to the European Commission and will be updated in light of future needs and developments.

The GNCHR also appears on the European Commission’s website in the consolidated list of all competent authorities with specific powers for the protection of human rights in the framework of the EU²⁴⁷, as the European Commission has been informed by the Ministry of Digital Governance and Artificial Intelligence, according to the Ministry’s press

246. Ministry of Digital Governance, [Authorities Protecting Fundamental Rights in Relation to the Use of Artificial Intelligence in Greece](#), 12 November 2024.

247. European Commission, [Fundamental rights protection authorities with special powers under the EU AI Act](#) (access 29 June 2026).

release of November 2024. Recently, the GNCHR took part in the 2nd forum in April 2026, which presented the AI governance system in Greece; the event was organised by the Ministry²⁴⁸. The forum reaffirmed the participation of the GNCHR, together with the other authorities referred to above, in the governance system as an authority designated under Article 77 of the EU AI Act. The GNCHR is likewise listed on the [website of the Special Secretariat for Artificial Intelligence and Data Governance](#) in the context of AI regulation and the AI ecosystem in Greece. Nevertheless, no references are made to the GNCHR, the Greek Ombudsman and the Hellenic Authority for Communication Security and Privacy in the draft law on measures implementing the EU AI Act²⁴⁹ nor to the provisions of Article 77 of the Regulation.



Ministry of Digital Governance and AI, GNCHR participation in the 2nd Consultation Forum on the implementation of the EU AI Act in Greece organized by the Special Secretariat for Artificial Intelligence and Data Governance

-
248. GNCHR, [GNCHR participation in the 2nd Consultation Forum on the implementation of the EU AI Act in Greece organized by the Special Secretariat for Artificial Intelligence and Data Governance](#), 2 April 2026. The GNCHR had also participated in the 1st forum.
249. GNCHR, [The GNCHR in Parliament on the Ministry of Digital Governance draft bill on artificial intelligence – Submission of Memorandum](#), 13 July 2026.

5.3 Competences and tasks of the GNCHR in the framework of the Regulation

It is clear that the competences of the GNCHR, as set out in its enabling legislation, are largely in line with the requirements of the Regulation concerning the authorities referred to in Article 77, a fact that reinforces the GNCHR role in this context, since there is also a more specific elaboration of the competences that, in any event, derive from the Regulation. Here's a brief overview of the main competences of the GNCHR.

Pursuant to Article 10 (2) of Law 4780/2021 ("Constitution and legal status"), the GNCHR is the National Human Rights Institution and the independent advisory body to the State on matters pertaining to human rights protection and promotion. Moreover the reference in Article 10 according to which: "the GNCHR as the National Human Rights Institution and the independent advisory body to the State on matters pertaining to human rights protection and promotion" constitutes a key element demonstrating the GNCHR broad mandate in respect of all human rights, without any limitation or prohibition. This recognition must also be taken into account in the context of the implementation of the Regulation and in relation to the specific competences of the GNCHR as the National Human Rights Institution in Greece.

Pursuant to Article 11 of Law 4780/2021, the GNCHR has as its mission: (a) the constant monitoring of matters pertaining to human rights protection, the informing of the public and the advancement of research in this connection; and (...) (c) the formulation of policy proposals on matters related to its scope of work.

Pursuant to Article 12 of Law 4780/2021 ("Competences"), the GNCHR shall, in particular: (a) examine issues regarding human rights protection put before it by the Government or the Conference of Presidents of the Parliament, or proposed to it by its members or civil society; b) submit recommendations and proposals, carry out research and deliver an opinion on the adoption of legislative, administrative and other measures which contribute to the improvement of human rights protection; (c) examine the adaptation

of Greek legislation to the provisions of international and EU law on human rights protection and deliver an opinion in this connection to the competent bodies of the State; (d) monitor and express recommendations to the State for the permanent and constant impact assessment of policy measures on human rights; (e) monitor and express recommendations to the State for the operation of a reliable and effective system for recording incidents of discrimination, racism and intolerance; (f) undertake initiatives for the cultivation of respect for human rights within the framework of the educational system; (g) deliver an opinion on reports which the country is to submit to the European Union and international organisations on matters related to its scope of work, and draw up and submit its own independent reports; (h) communicate and cooperate with the independent authorities, as well as the competent bodies of the European Union, international organisations, similar bodies of other States, and national or international non-governmental organisations; (i) make its positions publicly known by every appropriate means; (j) develop initiatives for raising public awareness, as well as awareness in the media, on matters of respect for human rights; and (k) organise a Documentation Centre for human rights.

The reference to 'in particular' in the article suggests a broader definition of competences within the established objectives of the GNCHR. The competence under Article 12(a), whereby the GNCHR examines issues relating to human rights protection put before it by the Government, may be applied *mutatis mutandis* in conjunction with the framework of Articles 73 (7) and 77 of the Regulation. The GNCHR has the expertise to undertake an examination and deliver an opinion on human rights protection issues where it receives the relevant information from the market surveillance authority.

Points (b) and (c) of Article 12, concerning the competence to submit recommendations and proposals, carry out research and deliver an opinion on the adoption of legislative, administrative and other measures contributing to improved human rights protection, and to examine the adaptation of Greek legislation to international and EU law on human rights protection and deliver an opinion in this connection to the competent bodies of the State, directly cover the

framework of competences provided for in the Regulation and Article 77 thereof. This follows directly from the functions of issuing opinions and examining adaptation to EU law and the Charter of Fundamental Rights of the European Union. Furthermore, within the framework of the Memorandum of Cooperation with the National Coordination Authority of the General Secretariat for Public Investments and the Partnership Agreement, the GNCHR provides assistance, including training activities for the services involved, assuming the monitoring and safeguarding of the compatibility of procedures and individual actions with the Charter of Fundamental Rights of the European Union. It should be recalled that the GNCHR was designated as the competent body to ensure fulfilment of Enabling Condition 3, entitled “Effective application and implementation of the Charter of Fundamental Rights”, at all stages of the implementation of the NSRF 2021–2027 programmes²⁵⁰.

The framework for the implementation of international and European legislation on the protection of human rights also includes the encouragement of the ratification of international agreements and the application of international standards relating to artificial intelligence and new technologies. In practice, whenever the GNCHR deals with a specific issue —whether it is commenting on a draft bill or existing legislation or addressing administrative practices or failures— it always examines whether, and to what extent, Greece complies with the relevant international human rights and EU standards. In this context, the GNCHR calls on the State to sign and ratify relevant international human rights conventions on artificial intelligence and the digital world in general, which prioritise the role of human rights law.

250. [The GNCHR at the MOU S.A. seminar on the implementation of the Charter of Fundamental Rights in the NSRF 2021-2027, 28 April 2025](#), [The GNCHR at the MOU S.A. seminar in Thessaloniki on the implementation of the Charter of Fundamental Rights in the NSRF 2021-27, 28 March 2025](#), [Working meeting of the National Coordination Authority and the GNCHR on training staff in the application of the EU Charter of Fundamental Rights 24 January 2025](#).

In examining the international and EU legal framework, the GNCHR also draws on the case-law of international and European courts, such as the CJEU of the European Union, as well as decisions and reports of international treaty bodies, such as the General Comments of the UN Human Rights Committee or decisions of ILO supervisory bodies.

Another tool available to the GNCHR for this purpose is the power of public consultation enabled by its pluralistic composition within the framework of its independence. The organisation of public hearings enables consultation with relevant stakeholders and persons active in the field in each instance. In this context, the GNCHR invites, at its discretion, persons who may assist its work by sharing personal experiences or expressing views relating to the protection of human rights to be heard before it (Article 18(4) of Law 4780/ 2021). The findings and outcomes of the hearings are incorporated into the GNCHR reports and help to the formulation of comprehensive recommendations to the State, including recommendations on ratifying international human rights conventions and protocols or on properly giving effect to international norms in the domestic legal order. The powerful tool of public consultation as well as the coordination of persons and stakeholders during the January 2026 hearing on AI and human rights, was presented as a good practice at the GANHRI Annual Conference 2026, held on 1 April 2026, on “The Role of National Human Rights Institutions in Promoting and Protecting Human Rights in the Digital Space”²⁵¹. Furthermore, as a bridge between civil society and the State, the GNCHR must stress the need to involve civil society organisations in AI-related fora and working groups., since such organisations can contribute specialised knowledge and expertise on human rights generally and digital rights in particular.

The National Commission’s competence to “monitor and express recommendations to the State for the permanent and constant impact assessment of policy measures on human rights” Article

251. GNCHR, [Participation of the GNCHR in the GANHRI Annual Meeting 2026 in Geneva](#), 3 April 2026. See also GANHRI, [Outcome Statement: The role of National Human Rights Institutions in promoting and protecting human rights in the digital space](#), 1 April 2026.

12(d)] is directly linked to the Human Rights Impact Assessment (HRIA) framework developed under international and European human rights law. More specifically, it is linked to the FRIA required under Article 27 of the EU AI Act for certain high-risk AI systems²⁵² as well as to the Council of Europe’s HUDERIA methodology²⁵³. In line with the Paris Principles, the GNCHR and other NHRIs are well placed to provide recommendations and guidance on human rights and artificial intelligence in the context of long-term strategic foresight, in cooperation with the competent authorities and services²⁵⁴.



GNCHR, 2nd seminar of the GNCHR Educational Seminar Series, entitled: “AI & Human Rights”

252. FRA, [Assessing High-Risk Artificial Intelligence: Fundamental Rights Risks](#), 2025.
253. Council of Europe, [HUDERIA - risk and impact assessment of AI systems](#). See also the national reports as good practices: DIHR, [A guide to Fundamental Rights Impact Assessments under the EU Artificial Intelligence \(AI\) Act](#), 15 December 2025.
254. Finland – Human Rights Centre, [Report on human rights foresight, resilience and preparedness during transformations in society](#), 4/2023. See also Special Secretary of Foresight Strategy and GNCHR [Successful completion of the 2nd seminar of the GNCHR Educational Seminar Series entitled: “AI & Human Rights”](#), 16 October 2025.



The GNCHR has long advocated the adoption of HRIAs as a tool for developing and measuring the impact of public policies. To this end, the GNCHR was expressly entrusted with this competence in 2021. In order to fulfil this mandate, the National Commission launched a series of reference reports on issues, such as the rights of refugees and migrants, women's rights, and LGBTIQ+ rights. These reports establish a baseline for the current level of enjoyment of human rights by specific groups or in specific (exceptional) situations in Greece. The selected issues must be addressed by the State as a matter of priority. The GNCHR reference reports contain primary and secondary data that State authorities can use to derive appropriate indicators for developing future evidence-based policies (*ex ante*) or for measuring the impact of current policies (*ex post*). At the same time, the GNCHR uses them as a starting (reference) point for its documented, actionable recommendations which are subsequently addressed to the State.

Having developed a HRIA methodology, the GNCHR has the expertise to apply a corresponding framework in the context of implementing the Regulation and to monitor the compliance of actors with the above framework. Furthermore, the GNCHR participates in the [Artificial Intelligence Working Group – European Network of National Human Rights Institutions](#)) with active involvement in relevant issues, considering the contributions of other NHRIs and from in a comparative context²⁵⁵.



*ENNHRI, ENNHRI Strengthening the NHRI's work
on Artificial Intelligence and Human Rights Meeting*

255. In addition to the reports, opinions and statements of other NHRIs that have been included elsewhere in the text, the GNCHR mentions the following examples: EHRC, [An update on our approach to regulating artificial intelligence](#), 30 April 2024. EHRC, [Artificial intelligence in public services](#), 1 September 2022. EHRC, [Department for Science, Innovation and Technology - A pro-innovation approach to AI regulation White Paper consultation response](#), 23 June 2023, 26 June 2023. Republic of Slovenia – Human Rights Ombudsman, [Summary of the work of the Human Rights Ombudsman of the Republic of Slovenia for 2024](#), 2025. NIHR, [Annual Statement 2025 – Human Rights in Northern Ireland](#), 12 December 2025. Defensor del Pueblo, [Informe anual 2025](#). ENNHRI, [Report on the Rule of Law – Belgium](#), 2025. CNCDH, [Opinion on the Impact of Artificial Intelligence on Fundamental Rights](#), 7 April 2022.

With regard to Article 12(e), and within the framework of its competence to monitor and express recommendations to the State for the operation of a reliable and effective system for recording incidents of discrimination, racism and intolerance, the GNCHR has the safeguards and expertise needed to collect and record data in full confidentiality, through the Racist Violence Recording Network (see also Article 78 of the Regulation concerning the confidentiality obligations)²⁵⁶. Accordingly, the Recording Mechanism of Informal Forced Returns also collects similar data, using a corresponding methodology.

Taking into account also its composition (see below of Law 4780/2021 Article 13), which includes other independent authorities, the competence of the GNCHR to communicate and cooperate with independent authorities, as well as the competent bodies of the European Union, international organisations, similar bodies of other countries, and national or international non-governmental organisations [Article 12(h)], establishes a decisive system of different competences and opportunities for cooperation and coordination. First, the GNCHR already cooperates with other independent authorities within the framework of its composition and highlights, in a coordinated manner, the relevant issues concerning human rights and independent authorities. Consequently, a framework for the cooperation of these authorities already exists under the coordination of the GNCHR. Second, the GNCHR serves as a forum and platform for dialogue between EU bodies and

256. On 1 October 2011, the Racist Violence Recording Network launched the pilot phase of the systematic recording of racially motivated violence. It uses a common methodology and a standard Racist Incident Recording Form in order to generate the clearest and most comprehensive possible picture of quantitative and qualitative trends in racist violence in Greece. The Network consists of bodies which provide medical, social and legal services and/or come into direct contact with victims of racist violence or victims of other violent attacks motivated by hatred or prejudice, and, finally, organisations established by the groups which are themselves usually targeted by racist violence.

civil society²⁵⁷. Third, the GNCHR engages directly with bodies of international organisations²⁵⁸.



*GNCHR, GNCHR meeting with the AMKE Homo Digitalis
on issues of digital rights and artificial intelligence*

The GNCHR is entitled to participate in national and European initiatives on AI and human rights, in international fora such as the United Nations, the Council of Europe, the European Union, the Organization for Security and Co-operation in Europe, and the Organisation for Economic Co-operation and Development, as well as in conferences and seminars organised by academic institutions

257. See, for example, [the working meeting and consultation between civil society organisations and the European Commission's Directorate-General for Migration and Home Affairs \(DG HOME\), held at the premises of the GNCHR on 14 May 2025](#); . and the GNCHR meeting with the AMKE Homo Digitalis on issues of digital rights and artificial intelligence, on 19 May 2025.

258. See for instance, [GNCHR meeting with the Council of Europe Commissioner for Human Rights, Mr Michael O' Flaherty, on 12 February 2025](#), , and its meeting with a delegation of the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) on 3 February 2025.

and human rights networks abroad, thereby promoting the interplay between AI, new technologies and human rights.

On the basis of the above competences, the GNCHR has carried out significant work on artificial intelligence and human rights²⁵⁹. It monitors technological developments, the evolution of artificial intelligence and digital transformation, and draws the attention of the competent State authorities to new challenges, their impacts on human rights and potential risks.

Pursuant to Article 13 of Law 4780/2021 (“Composition”), the GNCHR is composed of a plurality of members and bodies, while, pursuant to Article 14(2) of the above Law (“Appointment and legal status of the members”): 2. “The members of the GNCHR shall be persons with proven knowledge and experience in the field of protection and promotion of human rights.”.

Its pluralistic composition constitutes an important advantage for the joint formulation of policies for the protection of human rights. Consequently, when the Commission’s positions are shaped by independent authorities, organisations and confederations, civil society, and universities, the result has added value and needs to be taken into account with regard to the framework of the GNCHR background in terms of coordination and cooperation with all the above-mentioned bodies and members of the National Commission.

The members’ expertise in various rights-related issues can cover the different aspects of issues linked to artificial intelligence and human rights. Here are some examples of references, which cover many different aspects: justice, the environment, employment, education, asylum and migration, public administration, independent authorities, discrimination, gender and gender identity, women’s rights, the rights of LGBTIQ persons, the rights of persons with disabilities, children’s rights, the rights of Roma persons, racist violence, racist crime and hate speech, academic freedom and academic issues—science and AI, ethics in the context of AI and technoethics. Furthermore, on the basis of its composition and the mandate assigned to it by Law, the

259. See the Field “[Artificial Intelligence and New Technologies](#)”.

GNCHR covers horizontally all matters concerning the protection of human rights. It has developed expertise across a wide range of thematic human rights areas. This is also reflected in Article 20 of the Law, concerning the Sections established within the framework of the operation of the GNCHR²⁶⁰.

Having Liaison Officers in accordance with Article 16 ("Liaison Officers") of the aforementioned Law, brings further added value to GNCHR. Pursuant to Article 21 of the above Law ("Assistance provided by agencies and operators in the public and private sectors"): "Public services must facilitate the work of the National Commission. In order to fulfil its mission, the GNCHR may conduct on-site investigations, as well as seek from both public services and individuals, any information, document or any other material relating to the protection of human rights. The President of the GNCHR may examine documents and other material, which are classified as confidential, unless they are affiliated with national defence, state security and international relations of the State."

The authority to carry out on-site investigations and to submit requests to public authorities and private individuals for information, documents or any other material relating to the protection of human rights constitutes a framework of actions and powers required by the Regulation. The explicit provision in the Law of the GNCHR imposes an obligation on public authorities to cooperate in its work. This provision imposes an obligation on the public administration to respond to requests from the GNCHR for information or access to documents and premises. It also obliges them to facilitate the smooth conduct of on-site investigations. The power of the President to examine documents and other information classified as confidential, unless these relate to national defence, state security and the country's international relations, also highlights the

260. Article 20 (Sections) – In the context of the operation of the Commission, the following Sections shall be established: (a) the Section for Civil and Political Rights; (b) the Section for Economic, Social and Cultural Rights; (c) the Section for Application of Human Rights to Aliens; (d) the Section for Promotion of Human Rights; and (e) the Section for International Communication and Cooperation.

respective powers of the individual bodies within the GNCHR. This is a unique competence that has already been exercised and may be exercised in the future.

With regard to this unique competence, the work of the GNCHR would be supported by more specific provisions on artificial intelligence and methodology for the implementation of the Regulation, as well as by a prompt response from authorities and private individuals, so as to meet the requirements for promptness, effectiveness and high-quality implementation, grounded in the protection of human rights. The European Network of NHRIs, with the cooperation of the GNCHR, has published similar relevant statements regarding the competences and expertise of NHRIs²⁶¹, while it is understood that, in seeking the compliance of all involved bodies at a practical level, the protection of fundamental rights, the rule of law and the AI principles should undoubtedly be taken into account by all actors²⁶².

261. See in detail ENNHRI, [Artificial Intelligence](#) and indicatively ENNHRI, [ENNHRI calls on the European Commission to ensure effective FRIA under the EU AI Act](#), April 2025. See GNCHR [The GNCHR at the ENNHRI FRIA for Artificial Intelligence Webinar](#), 11 April 2025.

262. Zagganas Christos and Karkalemi Stelina , *AI Act Handbook: Compliance Guide for Legal Counsel and the Compliance Officer*, Nomiki Bibliothiki, 2025, pp. 34 et seq 196 etc.

CHAPTER 6

Conclusions – Recommendations

6.1 Summary of the Report's purpose and structure

The GNCHR Human Rights and Artificial Intelligence Reference Report attempts to map the main challenges and perspectives arising from the development and use of AI systems in terms of human rights. Its purpose is to present the key positions of the GNCHR, highlight the international, European and national regulatory framework, address the implications of AI in individual areas of political and societal life, and propose a human-centric governance framework linking innovation with democracy, accountability, and respect for human dignity.

The report is structured around four main pillars: (a) the international, European and national legal frameworks, (b) the perspectives and challenges of AI in individual thematic areas, (c) the AI principles as safeguards for the protection of human rights, and (d) the role of the GNCHR in the context of national AI governance and the implementation of Regulation (EU) 2024/1689. The report sets out conclusions and recommendations for the State to ensure the reliable and legally compliant use of artificial intelligence.

6.2 Thematic conclusions and recommendations

Taking into account the above analysis and references focusing on the conclusions regarding the challenges and perspectives, as well as the recommendations by thematic area, by right and by principle governing the AI the GNCHR summarises and concludes as follows: As explained in the introduction, and in line with the purposes of this reference report,



the GNCHR's objective is for more specific texts and positions to follow, by thematic pillar and by right, on the basis of the prioritisation that the National Commission will give to the relevant issues. As previously mentioned, this report links the related issues of artificial intelligence and human rights, and sets out the original positions of the GNCHR, focusing on key aspects of its work. The following is a summary of what has been discussed in the previous chapters:

1. Work and Artificial Intelligence

- AI is transforming the world of work through task automation and algorithmic management, creating both opportunities for increased productivity and risks to the quality and stability of employment.
- The protection of workers from excessive digital surveillance, constant monitoring mechanisms and non-transparent automated assessment and decision-making processes are issues of critical importance.
- The transition to the era of AI requires extensive skills upgrading and lifelong learning, allowing workers to adapt to the new demands of the labour market and changes in job roles.
- Particular attention must be paid to preventing algorithmic discrimination in recruitment, evaluation of employees and career progression, particularly against women, older persons, migrants and other vulnerable groups.
- The GNCHR highlights the need to strengthen the regulatory framework and safeguards for the protection of workers' rights, placing emphasis on transparency, accountability and human oversight.

2. Health and Artificial Intelligence

- AI can play a significant role in medical diagnosis, prognostic analysis, personalised treatment, telemedicine and the improvement of healthcare services.
- A key challenge is the processing of sensitive health data, which is directly linked to the protection of patients' privacy and personal data.

- The quality and representativeness of the training data used in AI systems are crucial for avoiding bias and ensuring reliable results.
- The doctor-patient therapeutic relationship remains fundamental and must not be replaced by automated decision-making processes.
- The development of AI applications in healthcare must be grounded in the principles of transparency, accountability, human oversight and respect for patient autonomy.

3. Justice, Public Administration and the Rule of Law

- The use of AI tools has the potential to accelerate processes, reduce administrative burdens and improve the delivery of services to citizens.
- At the same time, the increasing use of algorithmic systems in decision-making raises serious issues regarding transparency, justification and the ability to challenge decisions.
- The principle of human oversight is a crucial prerequisite for technology to function in a supportive capacity rather than replacing human judgement.
- The implementation of high-risk systems must be accompanied by monitoring mechanisms of their impact on fundamental rights and by clear lines of accountability.
- The protection of the right to sound administration, to a fair trial and to an effective remedy must be at the heart of every digital transformation initiative.

4. Migration and Asylum

- The use of AI in border control, surveillance and asylum case examination procedures carries an increased risk of arbitrary or non-transparent decisions.
- The principle of non-refoulement and the right of access to the asylum procedure must be safeguarded regardless of the extent to which automated systems are used.

- Refugees and migrants are among the groups most vulnerable to the risks of algorithmic bias and erroneous assessments.
- Specific safeguards are required to ensure transparency and the right to challenge decisions based on AI systems.
- Human assessment needs to maintain its role as the final decision-making stage in processes that affect fundamental rights.

5. Education – Child – Vulnerable groups

- AI can serve as a tool to enhance learning, creativity and personalised educational support.
- Children face specific risks relating to privacy, manipulation, exposure to inappropriate content and data collection.
- Persons with disabilities can significantly benefit from accessibility and assistive technology applications, provided that the systems are designed in an inclusive manner.
- Equal opportunities in access to digital technologies is a crucial prerequisite for AI not to widen existing social inequalities.
- The state must invest in digital literacy, education and skills development for all.

6. Gender, Discrimination and Participation in Democracy

- The report highlights that AI systems often replicate or reinforce current social and gender stereotypes.
- Algorithmic bias can lead to unequal access to opportunities, goods and services, undermining the principle of equality.
- Disinformation, deepfakes and manipulative techniques threaten the public sphere, democratic participation and trust in institutions.
- Effective fight against discrimination requires transparent systems, qualitative data and regular assessment of their impact on human rights.
- A human-centric approach, accountability and non-discrimination are key prerequisites for the sustainable development and use of AI.

6.3 The role of the GNCHR in the context of AI governance in Greece

The GNCHR has a particular institutional role in the national AI governance ecosystem, as it is the official National Human Rights Institution and the body that bridges the field of fundamental rights with the development and application of new technologies. The report underlines that the added value of the GNCHR lies precisely in its power to assess the impact of AI on human rights and to incorporate the relevant perspective into the national debate on innovation, regulation and implementation of Regulation (EU) 2024/1689. Its pluralistic composition, which brings together independent authorities, academic institutions, social partners and civil society organisations, enables it to function as a forum for dialogue, coordination and institutional consultation between the State and society.

At the same time, the GNCHR has a wide range of competences and tools, such as hearings of stakeholders, formulation of recommendations, monitoring of developments, interventions in legislative processes, training actions and international networking through ENNHRI and GANHRI. The report stresses that these competences make the GNCHR a crucial institutional mechanism for the protection of rights against the risks associated with high-risk AI systems and the application of Article 77 of the EU AI Act. Through this role, the GNCHR contributes to a coherent, human-centric AI governance framework in Greece placing human rights at its core.

Moreover, as has been emphasised on other occasions, strengthening the wider ecosystem of independent authorities and supervisory bodies must be made a priority for the State, with the aim of safeguarding independence, improving infrastructure, and reinforcing the staffing and expertise of the authorities concerned, so that this ecosystem is effective and provides the appropriate guarantees of respect for human rights, as required by the aforementioned international, European and national instruments.

In conclusion, the GNCHR stresses that when the above framework is not implemented or is implemented in a fragmented way, human

rights challenges, as analysed, will lead to human rights violations. The key role of the GNCHR within the scope of its competences and the cooperation with the co-competent authorities in conjunction with the consultation of relevant stakeholders are crucial elements for the effective functioning of the ecosystem with respect to human rights.



Law Publishers in Europe

NOMIKI BIBLIOTHIKI represents Greece in the European network "Law Publishers in Europe". LPE was founded in 1983 by some of the best-known European legal publishers, aiming at the exchange of know-how, co-publishing opportunities and the development of various levels of cooperation serving the legal and business communities in Europe and worldwide.

LPE network includes the following publishing houses: **Almedina** (Portugal), **C.H. Beck** (Germany), **Giuffrè Francis Lefebvre** (Italy), **Karnov** (Denmark), **Larcier** (Belgium), **Legitech** (Luxembourg), **Lexis Nexis** (France), **Manz** (Austria), **Nomiki Bibliothiki** (Greece), **Stämpfli** (Switzerland), **Thomson Reuters** (United Kingdom), **Tirant lo Blanch** (Spain), **Wolters Kluwer Law** (Netherlands), **Wolters Kluwer Polska** (Poland).