CDDH(2025)R103 Addendum 3
12 January 2026

STEERING COMMITTEE FOR HUMAN RIGHTS

(CDDH)

_____

CDDH HANDBOOK ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

Table of Contents

1. INTRODUCTION 5
2. AI SYSTEMS: KEY TECHNICAL CONCEPTS RELEVANT FOR HUMAN RIGHTS 6
2.1 Artificial Intelligence System 6
2.1.1 AI systems lifecycle 7
2.1.2 Machine-based system 7
2.1.3 Autonomy 7
2.1.4 Adaptiveness 7
2.1.5 AI system objectives 8
2.1.6 Environment or Context 8
2.1.7 Input 8
2.1.8 Inference 8
2.1.9 Output 8
2.2 Further technical concepts relevant for AI and human rights 9
2.2.1 Transparency 9
2.2.2 Explainability 9
2.2.3 Interpretability 10
3. HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE 10
3.1 General Issues 10
3.1.1 The European Convention on Human Rights (ECHR) 10
3.1.2 The European Social Charter (ESC) 11
3.1.3 The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law 11
3.1.4 ECHR and ESC General Principles in the Context of AI 12
Effective Protection of Rights 13
Subsidiarity and the margin of appreciation 13
Evolutive Interpretation and the ‘Living Instrument’ Doctrine 14
Positive Obligations 14
Human Dignity 15
Personal Autonomy and Self-Determination 15
Lawfulness, Legitimate Aim, Necessity, Proportionality, and Fair Balance 15
3.1.5 Core human rights issues across public governance sectors 16
Non-Discrimination and Equality 16
i. The Prohibition of Discrimination 16
ii. Risks to Non-Discrimination and Equality 17

The Right to Privacy and Personal Data Protection 18
i. The Right to Privacy and Data Protection in the ECHR and other relevant instruments 18
ii. Privacy and Data Protection Risks 19
Effective remedies 19
i. The right to an effective remedy in the ECHR, ESC, and other relevant instruments 20
ii. Risks to the Right to an Effective Remedy 20
3.2 Business and Human Rights 21
3.2.1 Positive obligations under the ECHR and the ESC 21
Obligations to regulate and supervise business activities 23
Procedural positive obligations to enable public participation and informed public decision making 23
Obligations relating to the provision of effective remedies 24
Margin of appreciation in the context of positive obligations 24
3.2.2 Balancing Rights of Businesses in the Context of AI Governance 25
3.2.3 Key Non-Binding Frameworks on Business, Human Rights and AI 25
Relevant non-binding instruments 25
Corporate Responsibility to Respect Human Rights 26
4. PUBLIC GOVERNANCE SECTORAL ANALYSIS 27
4.1. Administration of Justice 27
Key AI use cases 27
Relevant human rights and principles 28
Privacy and data protection in the context of administration of justice 32
4.2. Law Enforcement and Public Security 33
Key AI use cases 33
Relevant human rights and principles 34
Privacy and data protection; Freedom of Expression and Freedom of Assembly and Association 34
Non-discrimination and equality 38
Right to an effective remedy 38
4.3. Immigration and Border Control 39
Key AI use cases 39
Relevant human rights and principles 40
Right to Privacy and Data Protection 40
Non-discrimination 42
Right to an effective remedy 42

4.4. Democratic Processes 43
Key AI use cases 43
Relevant human rights and principles 44
Non-discrimination and equality 48
Transparency and Accountability 48
Right to Privacy and Data Protection 49
Business and Human Rights 49
4.5. Healthcare 50
Key AI use cases 50
Relevant human rights and principles 51
Right to Privacy and Data Protection 52
Non-Discrimination and Equitable Access to Health Care 53
Informed Consent, Autonomy and Decision-Making 54
4.6. Social services and welfare 55
Key AI use cases 55
Relevant human rights and principles 56
Right to Privacy and Data Protection 57
Non-discrimination and equality 57
Transparency and Accountability 58
Accessibility and Quality of Care 58
4.7. Education 59
Key AI use cases 59
Relevant human rights and principles 60
Right to Privacy and Data Protection 61
Non-discrimination and equality 62
Transparency and Accountability 64
Business and Human Rights 64
4.8. Labour and Employment 66
Key AI use cases 66
Relevant human rights and principles 66
Right to Privacy and Data Protection 67
Non-discrimination and equality 68
Transparency and Accountability 69
Freedom of Expression; Freedom of Assembly and Association 70

1. INTRODUCTION

1. Artificial intelligence (AI) is increasingly being adopted across society, unlocking new opportunities for innovation and progress. This includes the potential to advance human rights by, for example, expediting judicial proceedings, enhancing healthcare through predictive diagnostics, and personalising education to meet individual learning needs. Yet alongside these opportunities come risks to human rights.

2. The potential threat to human rights from the development and use of AI systems has been acknowledged by the international community and has driven global efforts to regulate this set of technologies.[1] The Council of Europe began working on the theme of AI a decade ago and has intensified its efforts in recent years, with several Council of Europe bodies and committees issuing a number of policy documents, recommendations, declarations, guidelines and other legal instruments.[2] The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law ("the Framework Convention") is the first international treaty on AI and human rights.[3] It establishes principles and obligations to ensure that AI systems are fully consistent with human rights, democracy, and the rule of law throughout their lifecycle while being conducive to technological progress and innovation.[4]

3. Existing Council of Europe human rights instruments, such as the European Convention on Human Rights and its Protocols (ECHR) and the European Social Charter (ESC), remain applicable in the context of AI: member States must align their frameworks on AI with their obligations under the ECHR and ESC. These instruments, interpreted by the European Court of Human Rights (the Court) and the European Committee on Social Rights (ECSR) respectively, establish basic standards for the protection of human rights, including in areas that are not covered by the Framework Convention as well as for those member States that are not States parties to the Framework Convention.[5]

4. This Handbook on Human Rights and Artificial Intelligence ('Handbook') has been designed as an accessible tool primarily to support government officials and policymakers in Council of Europe member States in applying ECHR, ESC and other human rights standards to the use of AI. Given the diverse audience of policymakers and government officials working across various areas of public governance, this Handbook does not assume extensive prior knowledge of human rights law or AI-related issues. Nor does it aim to provide an exhaustive analysis of every topic addressed. As a practical resource, it provides insights into how these standards, along with instruments like the Framework Convention, may apply to activities in AI systems' lifecycle. Focusing on key AI use cases in public governance, both current and reasonably foreseeable, it offers a framework to

---

[1] See for example, the Regulation (EU) 2024/1689 of the European Parliament and the Council ("AI Act") of the European Union; the OECD "Recommendation on Artificial Intelligence" adopted in 2019, revised in 2023 and 2024; UNESCO's "Recommendation on the Ethics of Artificial Intelligence", adopted in 2021. The United Nations General Assembly Resolution A/RES/78/265 "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development" (21 March 2024); and Resolution A/RES/78/311 on "Enhancing International Cooperation on Capacity-building of Artificial Intelligence" (1 July 2024).

[2] For an overview of the work done so far, or planned, by the intergovernmental committees and other entities of the Council of Europe in the area of AI, see Council of Europe and Artificial Intelligence

[3] Status of signatures and ratifications - see https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225

[4] Article 1 – Object and purpose, § 1.

[5] See section 3.1.3. below.

assess AI's human rights impacts considering ECHR and ESC standards, without predicting specific outcomes of future cases.[6]

5. Part 2 of the Handbook introduces key technical concepts linking the technological aspects of AI to existing or potential human rights implications. Part 3 outlines general human rights principles under the ECHR and ESC that may be relevant to AI across selected public sectors. It addresses first cross-cutting issues relevant to all sectors. The Handbook also considers the role of businesses in AI governance and the application of human rights standards in this context. Part 4 then provides a sectoral analysis of key AI use cases in public governance, examining human rights impacts, relevant legal principles, and good practices from Council of Europe member States.

2. AI SYSTEMS: KEY TECHNICAL CONCEPTS RELEVANT FOR HUMAN RIGHTS

6. This part provides a working definition of "artificial intelligence systems", with an explanation of their basic functions, and identifies further technical concepts that are relevant in the context of this Handbook. The definitions provided below are examples of definitions from a variety of sources.[7] These definitions are not exhaustive or universal.[8]

2.1 Artificial Intelligence System

7. "Artificial intelligence system" means a **machine-based system** that, for **explicit** or **implicit objectives**, **infers**, from the **input** it receives, how to generate **outputs** such as predictions, content, recommendations or decisions that may influence **physical or virtual environments**. Different artificial intelligence systems vary in their levels of **autonomy** and **adaptiveness** after **deployment**.[9]

8. This definition reflects a broad understanding of what artificial intelligence systems (AI systems) are, specifically as opposed to other types of simpler traditional software systems based on the rules defined solely by natural persons to automatically execute operations.[10] It was drafted for the purposes of the Framework Convention, drawing upon the 2023 OECD definition,[11] and aims at ensuring legal precision and certainty, while also remaining sufficiently abstract and flexible

[6] Those will be based on their specific factual circumstances, in the light of the relevant domestic legislation and practice of the member State concerned, and within the scope of the relevant European standards that will exist at the time when the case is examined, see *Zavodnik v. Slovenia,* No. 53723/13, 21 May 2015, § 74.
[7] Framework Convention; Explanatory Memorandum accompanying the updated definition of an artificial intelligence system in the OECD Recommendation on Artificial Intelligence (OECD/LEGAL/0449, 2019, amended 2023 [the definition itself was amended in 2023 but the Recommendation underwent further amendments in 2024], EU Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act); CEPEJ Cyberjustice Glossary, ISO/IEC 22989:2022 – Information technology — Artificial intelligence — Artificial intelligence concepts and terminology.
[8] The definitions correspond to the CEPEJ Cyberjustice Glossary which is based on a range of further sources.
[9] Framework Convention, Article 2.
[10] Framework Convention Explanatory Report, § 24.
[11] Updated definition of an artificial intelligence system in the OECD Recommendation on Artificial Intelligence (OECD/LEGAL/0449, 2019, amended 2023). A simplified overview of an AI system can be found in the OECD Explanatory Memorandum, p.7. This definition is also used in the EU AI Act, Article 3 (1).

to stay valid despite future technological developments. However, it is not meant to give universal meaning to the relevant term.[12]

2.1.1 AI systems lifecycle

9. The lifecycle of an AI system may encompass a range of activities, depending on the type of technology and other contextual elements and change over time. The following are non-exhaustive relevant examples of activities: (1) planning and design, (2) data collection and processing, (3) development of artificial intelligence systems, including model building and/or fine-tuning existing models for specific tasks, (4) testing, verification and validation, (5) supply/making the systems available for use, (6) deployment, (7) operation and monitoring, and (8) retirement.[13] These activities often take place in an iterative manner and are not necessarily sequential. They may also start all over again when there are substantial changes in the system or its intended use. The decision to retire an AI system from operation may occur at any point during the operation and monitoring phase.[14]

2.1.2 Machine-based system

10. The term 'machine-based' refers to the fact that AI systems are developed with and run on machines. The term 'machine' can be understood to include both the hardware and software components that enable the AI system to function. The hardware components refer to the physical elements of the machine, such as processing units, memory, storage devices, networking units, and input/output interfaces, which provide the infrastructure for computation. The software components encompass computer code, instructions, programs, operating systems, and applications that handle how the hardware processes data and performs tasks.[15]

2.1.3 Autonomy

11. AI system autonomy means the degree to which a system can learn or act without human involvement following the delegation of autonomy and process automation by humans. Human supervision can occur at any stage of the AI system lifecycle.[16] Some AI systems can generate outputs without these outputs being explicitly described in the AI system's objective and without specific instructions from a human.[17]

2.1.4 Adaptiveness

12. Adaptiveness refers to the capability of an AI system to evolve and modify its behaviour through direct interaction with input and data before or after deployment. Examples include a speech recognition system that adapts to an individual's voice or a personalised music recommender system. AI systems can be trained once, periodically, or continually, and operate by

---

[12] Explanatory Report, § 24. While this definition provides a common understanding between the Parties to the Framework Convention as to what artificial intelligence systems are, Parties can further specify it in their domestic legal systems for further legal certainty and precision, without limiting its scope.
[13] Framework Convention Explanatory Report, § 15.
[14] Idem.
[15] EU Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), para 11.
[16] OECD Explanatory Memorandum, p. 6.
[17] Idem.

inferring patterns and relationships in data. Through such training, some AI systems may develop the ability to perform new forms of inference not initially envisioned by their programmers.[18]

2.1.5 AI system objectives

13. AI systems are designed to operate according to one or more objectives. The objectives of the system may be explicitly or implicitly defined. Explicit objectives refer to clearly stated goals that are directly encoded by the developer into the system. For example, they may be specified as the optimisation of some cost function, a probability, or a cumulative reward. Implicit objectives refer to goals that are not explicitly stated but may be deduced from the behaviour or underlying assumptions of the system. These objectives may arise from the training data or from the interaction of the AI system with its environment.[19]

2.1.6 Environment or Context

14. An environment or context in relation to an AI system is an observable or partially observable space perceived using data and sensor inputs and influenced through actions (through actuators). The environments influenced by AI systems can be physical or virtual and include environments describing aspects of human activity, such as biological signals or human behaviour. Sensors and actuators are either humans or components of machines or devices.[20]

2.1.7 Input

15. Input is used both during development and after deployment. Input can take the form of knowledge, rules and code that humans put into the system during development or data. Humans and machines can provide input. During development, input is leveraged to build AI systems, e.g., with machine learning that produces a model from training data and/or human input. Input is also used by a system in operation, for instance, to infer how to generate outputs. Input can include data relevant to the task to be performed or take the form of, for example, a user prompt or a search query.[21]

2.1.8 Inference

16. The concept of “inference” generally refers to the step in which a system generates an output from its inputs, typically after deployment. “Infer how to generate outputs” should be understood as also referring to the build phase of the AI system, in which a model is derived from inputs/data.[22]

2.1.9 Output

17. Outputs generally reflect different tasks or functions performed by AI systems. They can be broadly categorised as recommendations, predictions, content and decisions. These categories correspond to different levels of human involvement, with “decisions” being the most autonomous type of output (the AI system affects its environment directly or directs another entity to do so) and

---

[18] Idem.
[19] EU Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), para 4;. see also OECD Explanatory Memorandum, p. 7.
[20] Idem
[21] Idem, p. 8.
[22] Idem, p. 9; see also EU Commission Guidelines, para. 26 and following.

"predictions" the least autonomous. They include, but are not limited to, recognition (identifying and categorising data, e.g., image, video, audio and text, into specific classifications as well as image segmentation and object detection), event detection (connecting data points to detect patterns, as well as outliers or anomalies), forecasting (using past and existing behaviours to predict future outcomes), personalisation (developing a profile of an individual and learning and adapting its output to that individual over time), interaction support, interpreting and creating content to power conversational and other interactions between machines and humans, possibly involving multiple media such as voice text and images), content generation (including but not limited to goal-driven optimisation (finding the optimal solution to a problem for a cost function or predefined goal) and reasoning with knowledge structures (inferring new outcomes that are possible even if they are not present in existing data, through modelling and simulation).[23]

2.2 Further technical concepts relevant for AI and human rights

2.2.1 Transparency

18. In the context of AI, transparency refers to openness and clarity in the governance of activities within the lifecycle of AI systems. It means that the decision-making processes and general operation of AI systems should be understandable and accessible to appropriate AI actors and, where necessary and appropriate, relevant stakeholders.[24] The means of ensuring transparency would depend on many different factors such as, for instance, the type of artificial intelligence system, the context of its use or its role, and the background of the relevant actor or affected stakeholder. Moreover, relevant measures include, as appropriate, recording key considerations such as data provenance, training methodologies, validity of data sources, documentation and transparency on training, testing and validation data used, risk mitigation efforts, and processes and decisions implemented, in order to aid a comprehensive understanding of how the artificial intelligence system's outputs are derived and impact human rights, democracy and the rule of law.[25]

19. To this end, the use of open-source software and interoperable technical standards should be encouraged for AI systems, insofar as it contributes to the transparency and verifiability of the systems, and contestability of the outcomes.[26] AI systems used in contexts that may impact human rights, such as electoral processes, should maintain complete and tamper-proof audit logs, allowing the tracing of all decisions and actions carried out.[27] These logs should be preserved in accordance with the legal time limits applicable and remain accessible to the competent oversight authorities, subject to appropriate data protection safeguards.[28]

2.2.2 Explainability

---

[23] OECD Explanatory Memorandum, p. 9; see also EU Commission Guidelines, para. 52 and following.
[24] See Framework Convention Explanatory Report , § 57. See also the OECD AI principle on Transparency and Explainability (Recommendation of the OECD Council on Artificial Intelligence, OECD/LEGAL/0449; and ISO/IEC 22989:2022, 5.15.8.
[25] Framework Convention Explanatory Report, § 57
[26] OECD *Recommendation of the Council on Artificial Intelligence* (OECD AI Principles) and OECD Report, *Advancing Accountability in AI Governing and Managing Risks Throughout The Lifecycle For Trustworthy* AI (2023).
[27] OECD Report, *Advancing Accountability in AI Governing and Managing Risks Throughout The Lifecycle For Trustworthy AI* (2023); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* §§ 47 & 77 ; See *Interpretative Declaration on Digital Technologies & AI in Electoral Matters* (CDL-AD(2024)044), European Commission for Democracy through Law (Venice Commission), §45
[28] UNESCO Recommendation on the Ethics of Artificial Intelligence, § 51.

20. Explainability is a particularly important component of transparency. AI systems integrating machine learning (ML) rely on mathematical models derived from automatic processing of data, rather than by explicit programming by humans. This makes it difficult even for AI experts, including the developers of the systems, to understand how their outputs are subsequently produced.[29] The resulting opacity, or "**black box**" effect, not only makes decisions more difficult to understand, but it can also have direct impact on individuals since it can hide deficiencies in AI systems, such as the existence of bias, inaccuracies, so-called "hallucinations".

21. "Explainability" therefore refers to the capacity to provide, subject to technical feasibility and taking into account the generally acknowledged state of the art, sufficiently understandable explanations about why an AI system provides information, produces predictions, content, recommendations or decisions as well as a general understanding of its capabilities and limitations.[30] It is the idea that the outcome of an automated system or algorithm can be explained in a way that "makes sense" to people, enabling those who have been affected by an output to understand and challenge it. This includes providing – in clear and simple terms, and as appropriate in the context – the main factors included in a decision, the determinant factors, and the data, logic or algorithm used to reach a decision.[31]

2.2.3 Interpretability

22. Interpretability refers to the ability to understand how an AI system makes its predictions or decisions or, in other words, the extent to which the outputs of AI systems can be made accessible and understandable to experts and non-experts alike. It involves making the internal workings, logic, and decision-making processes of artificial intelligence systems understandable and accessible to human users, including developers, stakeholders, and end-users, and persons affected.[32]

3. HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

3.1 General Issues

23. This section provides an overview of the ECHR, the ESC, and the Framework Convention, outlining the general principles of the ECHR and the ESC that may govern the protection of rights in the context of AI. It also highlights relevant principles from the Framework Convention where they offer valuable guidance within ECHR and the ESC framework. Additionally, it examines recurring human rights challenges that may arise in relation to the use of AI systems.

3.1.1 The European Convention on Human Rights (ECHR)

---

[29] TechDispatch: Explainable Artificial Intelligence, European Data Protection Supervisor (2023), citing Peters, U. 'Explainable AI lacks regulative reasons: why AI and human decision-making are not equally opaque', (AI and Ethics 2023); see also CDDH-IA(2024)09, Summary of the exchange of views with external independent experts and representatives of Council of Europe intergovernmental committees (25 September), key points made by Marko Grobelnik; and CDDH-IA(2024)07, Compilation of written contributions and presentations received from experts of the exchange of views of the 1st meeting, pp. 3-16.

[30] Framework Convention Explanatory Report, § 60; see also ISO/IEC 22989:2022, 5.15.6.

[31] OECD (2025), *AI and the future of social protection in OECD countries*, OECD Artificial Intelligence Papers, No. 42, p. 20

[32] Explanatory Report, § 61.

24. The ECHR is the core human rights instrument of the Council of Europe. It sets binding standards for public authorities in member States. The European Court of Human Rights ensures the observance of the ECHR by the States. Individuals, groups, legal persons, and non-governmental organisations (NGOs) can bring complaints of alleged human rights violations before the Court once all domestic remedies have been exhausted.

3.1.2 The European Social Charter (ESC)

25. As the core instrument for economic and social rights within the Council of Europe, the ESC guarantees fundamental protections that complement the ECHR. The Revised European Social Charter (RESC) incorporates new rights and amendments. 42 out of the 46 member States of the Council of Europe are parties to either the ESC or the RESC.[33] The ESC is monitored by the European Committee of Social Rights (ECSR) through two mechanisms: (i) regular reporting by States parties on their implementation of the ESC, and (ii) collective complaints lodged by the social partners and non-governmental organisations (NGOs), for those States having ratified the 1995 Additional Protocol Providing for a System of Collective Complaints.[34] Insofar as they refer to binding legal provisions and are adopted by a monitoring body established by the ESC, the conclusions and decisions of the ECSR represent an authoritative, although not legally binding interpretation of the ESC's provisions. States Parties have an obligation to cooperate with the ESCR and to take into account its decisions and conclusions, that arises from the application of the principle of good faith to the observance of their treaty obligations under the ESC.

3.1.3 The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

26. The Framework Convention reinforces existing international standards (such as the ECHR and the ESC) as may be applicable to each Party.[35] It adopts a technology-neutral approach, focusing on principles rather than regulating specific technologies. It applies to activities within the lifecycle of AI systems undertaken by public authorities (including private actors acting on their behalf).[36] With regard to activities by private actors acting independently, State Parties undertake to address risks and impacts in a manner conforming with the object and purpose of the Framework Convention, either by applying directly the principles and obligations set forth in the Convention or by taking "other appropriate measures".[37] In addition, matters relating to national defence are exempted from the scope of the treaty,[38] as well as (i) activities related to the protection of the State Parties' "national security interests" with the understanding that such activities are conducted in a manner consistent with applicable international law, including international human rights law obligations, and with respect for each Party's democratic institutions and processes;[39] and (ii) research and development activities, unless testing or similar activities are undertaken in such a way that they have the potential to interfere with human rights, democracy and the rule of law.[40]

---

[33] Liechtenstein, Monaco, San Marino and Switzerland are not parties to either of these treaties.
[34] 16 of the 42 Parties to the ESC have ratified this Additional Protocol.
[35] In the EU, the Framework Convention is to be implemented exclusively through the Regulation (EU) 2024/1689 of the European Parliament and the Council (AI Act), and other relevant Union acquis, where applicable.
[36] Framework Convention, Article 3 subparagraph 1 (a).
[37] Article 3 subparagraph 1 (b).
[38] Article 3 paragraph 4. Also note that under Article 1.d. of its Statute, "Matters relating to national defence do not fall within the scope of the Council of Europe".
[39] Article 3 paragraph 2.
[40] Article 3 paragraph 3.

27. Activities within the lifecycle of AI systems must comply with the following principles:[41]

- Human dignity and individual autonomy
- Transparency and oversight
- Accountability and responsibility
- Equality and non-discrimination
- Respect for privacy and personal data protection
- Reliability
- Safe innovation

28. Key requirements include the availability of remedies, to the extent any remedies are required by a Party's international obligations for AI-related violations of human rights,[42] ensuring procedural safeguards for affected persons, including seeking to ensure as appropriate for the context the provision of notice to persons interacting with AI systems;[43] conducting risk and impact assessments[44] on human rights, democracy, and the rule of law; and enabling the possibility of bans, moratoria or other appropriate measures in respect of certain uses of AI systems that the State Party considers incompatible with respect for human rights, the functioning of democracy or the rule of law.[45] The Framework Convention also provides for follow-up mechanisms and cooperation and introduces an obligatory monitoring mechanism.[46]

29. In view of technical complexity of the subject matter, the Council of Europe's HUDERIA (Risk and impact assessment of AI systems from the point of view of human rights, democracy and the rule of law)[47] provides supplementary non-legally binding guidance on how to operationalise and implement the Framework Convention's obligations regarding the assessment of risks and impacts of AI systems.[48] It sits at the intersection of international human rights standards and existing technical frameworks on risk management in the AI context promoting the development of safe, secure and trustworthy AI that is both performant and promotes respect for human rights, democracy and the rule of law. This Handbook may provide useful supplementary information to those applying HUDERIA.

3.1.4 ECHR and ESC General Principles in the Context of AI

[41] Chapter III (Articles 6-13).
[42] Chapter IV (Article 14).
[43] Article 15. Where an artificial intelligence system substantially informs or takes decisions impacting on human rights, effective procedural guarantees should, for instance, include human oversight, including *ex ante* or *ex post* review of the decision by humans (Explanatory Report, § 103).
[44] Chapter V (Article 16).
[45] Article 16, paragraph 4.
[46] Chapter VII (Articles 23-26).
[47] The HUDERIA is a stand-alone, non-legally binding guidance that does not have legal effect. It is not mandatory, nor intended as an interpretive aid for the Framework Convention. In addition, whilst the HUDERIA has a facilitative role, it is not a means to implement the Framework Convention. Many existing or future frameworks, policies, guidance, standards or tools may be used to assist in conducting AI risk and impact management, including the HUDERIA. Parties to the Framework Convention have the flexibility to use or adapt the guidance, in whole or in part, to develop new approaches to risk assessment or to use or adapt existing approaches in keeping with their applicable laws, provided that Parties fully meet their obligations under the Framework Convention, including the baseline for risk and impact management set out in its Chapter V. The HUDERIA complements, without being legally binding, the Framework Convention. It is to be supplemented by the HUDERIA Model – supporting materials such as tools and scalable recommendations to serve as a resource for risk management activities.
[48] Framework Convention, Article 16.

30. There is as yet only limited guidance from the Court and ECSR on the impact of AI technologies on rights under the ECHR and ESC.[49] However, established principles from the ECHR and the ESC can inform how these treaties may apply to AI-related human rights challenges. While some principles are common to both, others are specific to one or the other treaty.[50]

Effective Protection of Rights

31. The ECHR and the ESC are intended to guarantee rights that are not merely theoretical or illusory but practical and effective.[51] National authorities must ensure that rights holders can effectively enjoy their rights, which may involve adopting legislation, ensuring its effective application, providing adequate resources, and establishing appropriate operational procedures. Accordingly, States should safeguard the effective protection of human rights against harms related to activities within the lifecycle of AI systems through measures which may include adopting or implementing laws, providing resources, establishing, or designating existing national human rights structures, such as national human rights institutions (NHRIs), as independent oversight mechanisms, and ensuring effective cooperation between such mechanisms and other national human rights structures.

Subsidiarity and the margin of appreciation

32. Subsidiarity means that the States bear the primary responsibility to secure to everyone within their jurisdiction the rights and freedoms defined in the ECHR.[52] The Court authoritatively interprets the ECHR and acts as a safeguard for individuals whose rights and freedoms are not secured at the national level.[53]

33. National authorities may enjoy a "margin of appreciation" in how they apply and implement the ECHR, depending on the circumstances of the case and the rights and freedoms engaged. This reflects that the ECHR system is subsidiary to the safeguarding of human rights at national level and that national authorities are in principle better placed than an international court to evaluate local needs and conditions.[54] Under the ESC, States Parties also have discretion in determining the steps to comply with its provisions, balancing general interests with the needs of specific groups and available resources. With respect to new technologies, in particular, any State claiming a pioneer role in their development bears special responsibility for striking the right balance between the potential benefits of their extensive use against protected rights.[55]

---

[49] While the Court has yet to directly address AI, it has examined cases involving new technologies and their impact on human rights, including technologies integrating AI features, such as facial recognition systems (see *Glukhin v. Russia*, Application No. 11519/20, 4 July 2023; see also Factsheet – New technologies).

[50] The ECHR and ESC treaty systems are complementary and interdependent. The Court has clarified that there is no watertight division separating civil and political rights from economic, social and cultural rights. See *Airey v Ireland*, No. 6289/73, 9 October 1979, § 24; see also Digest of Case Law of the European Committee of Social Rights, December 2022, p. 33.

[51] *Airey v Ireland*, No. 6289/73, 9 October 1979, § 24; *International Commission of Jurists (ICJ) v. Portugal*, Complaint No. 1/1998, decision on the merits of 9 September 1999, §32; *European Federation of National Organisations working with the Homeless (FEANTSA) v. Slovenia*, Complaint No. 53/2008, decision on the merits of 8 September 2009, §28.

[52] ECHR, Preamble, recital 7.

[53] Explanatory Report, Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 213), para 8.

[54] Idem, para. 9.

[55] *S. and Marper v. UK* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, § 112: "The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."

Evolutive Interpretation and the 'Living Instrument' Doctrine

34. The ECHR and the ESC are "living instruments", interpreted dynamically in the light of present-day conditions to address evolving societal and technological issues.[56] The Court's past rulings on issues like data interception,[57] biometric data,[58] the internet and digital tools,[59] or facial recognition technology[60] highlight its capacity to adapt the application of existing rights to modern challenges. Likewise, the ECSR has addressed the right to privacy in the context of emerging new technologies.[61] By applying this doctrine, both the Court and the ECSR are expected to apply the ECHR and the ESC to AI-related cases in the future.

Positive Obligations

35. States have a duty under both the ECHR and the ESC to refrain from unjustified interference with human rights ("negative obligations") and to ensure their effective realisation and protection ("positive obligations"). Substantive positive obligations require the basic measures needed for full enjoyment of the rights guaranteed (e.g., proper rules governing intervention by the police or prohibiting ill-treatment). Procedural positive obligations require domestic procedures to ensure the protection of rights holders (e.g. conducting an effective investigation).

36. Positive obligations can apply even in cases where threats originate from private individuals or entities beyond direct state control as these instruments can address both vertical relationships – between national authorities and individuals – and horizontal relationships[62], between individuals or entities. States may be required to protect human rights in the sphere of the relations between individuals themselves (horizontal effect). This duty becomes particularly important in the context of the deployment of AI systems, where public-private partnerships and procurement from private actors are prevalent.

37. States must act diligently and reasonably, taking appropriate measures within their resources and capacities. Positive obligations may require the State to ensure the existence of adequate and effective mechanisms under which sanctions may be imposed in particular cases, enact specific legal rules, and/or take operational steps to protect individuals from foreseeable risks to their rights.[63]

---

[56] *Tyrer v. the United Kingdom*, No. 5856/72, 25 April 1978, § 31; *Transgender-Europe and ILGA-Europe v. Czech Republic*, Complaint No. 117/2015, decision on the merits of 15 May 2018, §75; *Defence for Children International (DCI) v. the Netherlands*, Complaint No. 47/2008, decision on the merits of 20 October 2009, §29.

[57] *Big Brother Watch and Others v. United Kingdom* [GC], Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.

[58] *S. and Marper v. United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008.

[59] *Ahmet Yıldırım v. Turkey*, No. 3111/10, 18 March 2013; *Magyar Helsinki Bizottság v. Hungary* [GC], No. 18030/11, 8 November 2016.

[60] *Glukhin v. Russia*, No. 11519/20, 4 July 2023.

[61] ECSR, Conclusions 2012, Statement of Interpretation on Article 1§2.

[62] The Court has recognised States' duty to protect human rights in these horizontal contexts, such as the right to respect for private and family life (Article 8 ECHR), see *X and Y v. Netherlands,* No. 8978/80, 26 March 1985, § 23; freedom of expression (Article 10 ECHR), see *Platform "Ärzte für das Leben" v. Austria*, No. 10126/82, 21 June 1986, § 23; and freedom of association (Article 11 ECHR), see *Khurshid Mustafa and Tarzibachi v. Sweden*, No. 23883/06, 16 December 2008, § 32; *Christian Democratic People's Party v. Moldova* (No. 2), No. 25196/04, 2 February 2010, § 25.

[63] For the ECHR see e.g., *Osman v. The United Kingdom* [GC], Nos. 87/1997/871/1083, § 115. For the ESC see, e.g., ECSR, Conclusions 2020, Albania on Article 1§2, Conclusions 2005, Statement of Interpretation on Article 11, *International Planned Parenthood Federation – European Network (IPPF EN) v. Italy*, Complaint No. 87/2012, decision on the merits of 10 September 2013, §66; see also *Confederazione Generale Italiana del Lavoro (CGIL) v. Italy*, Complaint No. 91/2013, decision on the merits of 12 October 2015, §162 and 190.

38. States' positive obligations[64] therefore may require them to take the necessary measures to safeguard human rights, including where necessary to assess the relevant risks and potential impacts to human rights that may be posed by AI systems and consider measures to address those potential harms effectively, and/or to implement measures to mitigate identified risks. The Framework Convention contains a dedicated provision prescribing the need to identify, assess, prevent and mitigate *ex ante* and, as appropriate, iteratively throughout the lifecycle of the AI system the relevant risks and potential impacts to human rights, democracy and the rule of law by following and enabling the development of a methodology with concrete and objective criteria for such assessments.[65]

Human Dignity

39. In the ECHR system, human dignity is invoked by the Court to affirm individuals' intrinsic worth and equality.[66] The Court has held that "[r]espect for human dignity forms part of the very essence of the Convention".[67] The ESC system too recognises that human dignity is the fundamental value and indeed the core of positive European human rights law – whether under the European Social Charter or under the European Convention of Human Rights.[68]

40. The Framework Convention also requires that the respect for human dignity be among the principles that govern artificial intelligence.[69] Activities within the AI lifecycle must not dehumanise individuals, undermine their autonomy, or reduce them to data points, and AI should not be anthropomorphised in ways that infringe on human dignity.[70]

Personal Autonomy and Self-Determination

41. Personal autonomy is an important principle underlying the interpretation of ECHR guarantees.[71] It is an 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.[72] The Framework Convention also specifically requires that the respect for individual autonomy is among the principles that govern AI.[73]

Lawfulness, Legitimate Aim, Necessity, Proportionality, and Fair Balance

42. Certain ECHR rights are absolute and cannot be subject to derogations in times of emergency, exceptions, or permissible interference. However, States Parties are allowed to restrict

---

[64] See further below under Section 3.2.1.
[65] Framework Convention Article 16, see also Explanatory Report, § 105.
[66] *Lăcătuş v Switzerland*, application, No. 14065/15, Merits and Just Satisfaction, 19 January 2021.
[67] *Magyar Helsinki Bizottság v Hungary* [GC], No. 18030/11, Merits and Just Satisfaction, 8 November 2016 at para 155.
[68] *International Federation of Human Rights (FIDH) v. France*, complaint No. 14/ 2003, decision on the merits of 8 September 2004, §31.
[69] Framework Convention, Article 7.
[70] Explanatory Report, § 53.
[71] *Pretty v. United Kingdom*, No. 2346/02, § 61, 29 July 2002, and [GC] judgment of 11 January 2006, *Sorensen and Rasmussen v. Denmark*, Nos. 52562/99 and 52620/99, 11 January 2006, § 54. See also the preamble to the data protection Convention 108, as it will be amended following the entry into force of the amending protocol.
[72] Framework Convention Explanatory Report, §55.
[73] Framework Convention, Article 7.

certain rights in the ECHR[74] and the ESC,[75] known as “qualified rights”, which allow for a balance between individual and general interests. There are some general requirements in both the ECHR and the ESC which must be satisfied for an interference to be justified. The interference must be (i) ‘prescribed by law’ or ‘in accordance with the law’ (requirement of lawfulness).[76] This means that it must have a clear basis in domestic law, ensuring it is rooted in established legal frameworks. Additionally, the legal basis must be accessible to the public, meaning individuals can know and understand the laws that affect their rights.[77] The interference must also be foreseeable, allowing people to anticipate how and when their rights might be restricted.[78] Lastly, it must be free from arbitrariness and implemented with proper procedural safeguards to ensure fairness and due care.[79] The interference with the right must (ii) pursue a legitimate aim[80] and it must be (iii) necessary (in a democratic society) to achieve the legitimate aim pursued.[81] The test of necessity requires that the limitation is proportionate to the legitimate aim pursued, responds to a pressing social need, and uses the least restrictive means.

43. States will have to ensure that any restrictions on qualified ECHR or ESC rights resulting from activities within the AI systems lifecycle satisfy all of these requirements.

3.1.5 Core human rights issues across public governance sectors

44. The use of AI systems can impact a range of human rights, with certain issues consistently emerging across contexts. These include risks for (i) non-discrimination and equality; (ii) personal data protection and privacy; and (iii) the ability to effectively challenge AI-based decisions and effective remedies. Competing human rights obligations in the context of AI may also be an issue across sectors. These recurring challenges are cross-cutting human rights concerns in the lifecycle of AI systems and are therefore not limited to one or more public sectors.

Non-Discrimination and Equality

i. The Prohibition of Discrimination

---

[74] No derogation in time of emergency is permitted from certain provisions of the ECHR and its protocols: the right to life under Article 2 (except in respect of deaths resulting from lawful acts of war); the prohibition on torture and inhuman or degrading treatment or punishment under Article 3; the prohibition of slavery and servitude under Article 4 (but not the prohibition on forced or compulsory labour under Article 4(2)); the prohibition on punishment without law under Article 7; the abolition of the death penalty in time of peace (Protocol No. 6, Article 1); the right not to be tried or punished twice (ne bis in idem) (Protocol No. 7, Article 4); and the abolition of the death penalty in all circumstances (Protocol No. 13, Article 1). The Convention provides for exceptions in relation to certain rights, such as the right not to be arbitrarily deprived of liberty under Article 5. In such cases, the Court has clearly established that the list of exceptions in a given article is exhaustive and that only a narrow interpretation of those exceptions is consistent with the aim of that article.

[75] States Parties are allowed to restrict the rights enshrined in the ESC. The conditions for the restriction are laid down in Article 31 of the ESC and Article G of the RESC.

[76] *Leyla Şahin v. Turkey* [GC], Application No. 44774/98, 10 November 2005, § 88; *Biržietis v. Lithuania*, Application No. 49304/09, 14 June 2016, § 50.

[77] *The Sunday Times v. the United Kingdom* (No. 1), Application No. 6538/74, 26 April 1979, § 48.

[78] Idem.

[79] *R.Sz. v. Hungary,* Application No. 41838/11, 2 July 2013, § 36.

[80] *S.A.S. v. France* [GC], Application No. 43835/11, 1 July 2014, § 114; *Merabishvili v. Georgia* [GC], No. 72508/13, 28 November 2017, §§ 295-296.

[81] *Vavřička and Others v. the Czech Republic* [GC], Nos. 47621/13 and 5 others, 8 April 2021, § §§ 273-275; *Association internationale Autisme-Europe (AIAE) v. France*, Complaint No. 13/2000, decision on the merits of 4 November 2003, §52.

45. The ECHR[82] and the RESC[83] themselves prohibit discrimination but only in relation to the enjoyment of rights and freedoms set out in the respective treaty. In addition, Article 1 of Protocol No. 12 ECHR introduces a general prohibition against discrimination covering "any right set forth by law".[84] The grounds for discrimination mentioned in these instruments include sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. The notion 'other status' means that the grounds listed are not exhaustive. The Court has interpreted the expression 'other status' in an extensive way and in light of present-day conditions to include characteristics including nationality, ethnic origin, sex, sex-based, sexual orientation, gender identity and expression, sex characteristics, age, state of health, disability, marital status, migrant or refugee status.[85] Discrimination can be direct or indirect. Direct discrimination arises from "a difference in the treatment of persons in analogous, or relevantly similar, situations"[86] [and] where this difference is "based on an identifiable characteristic".[87] Discrimination can also result from a failure to treat differently persons whose situations are significantly different.[88] Indirect discrimination occurs when seemingly neutral laws, policies or practices disproportionately and unjustifiably affect a particular group of persons.[89]

46. The Framework Convention's principle on equality and non-discrimination[90] refers to "the real and well-documented risk of bias that can constitute unlawful discrimination arising from the activities within the lifecycle of artificial intelligence systems",[91] and its provision on non-discrimination explicitly prohibits discrimination in the implementation of the Convention.[92] It draws directly from established international norms, including the ECHR and the ESC.[93]

ii. Risks to Non-Discrimination and Equality

47. AI systems may pose risks to equality and non-discrimination, as they may be built upon and sustained by data and models that reproduce, perpetuate, and exacerbate existing bias, stereotypes, stigma, prejudice, and false assumptions about individuals based on actual or perceived personal characteristics and their intersections. These effects can be further compounded by information asymmetries and can be more severe for persons in vulnerable situations or marginalised groups. Among other things, such effect may lead to an increase in online and offline violence against such persons, as well as against women and girls who may be disproportionately targeted due to existing gender inequalities, stereotypes, and power imbalances that AI systems may inadvertently amplify.[94]

---

[82] ECHR Article 14.
[83] RESC Article E. The ESC refers to the prohibition of discrimination in its preamble.
[84] This Protocol has been ratified by 20 member States of the Council of Europe.
[85] See Explanatory Report to the Recommendation CM/Rec(2024)7 of the Committee of Ministers to member States on the effective protection of human rights in situations of crisis.
[86] *Burden v. the United Kingdom* [GC], No. 13378/05, 29 April 2008, § 60.
[87] *Biao v. Denmark* [GC], No. 38590/10, § 89; for ESC see *Equal Rights Trust v. Bulgaria*, Complaint No. 121/2016, decision on the merits of 16 October 208, §80.
[88] *Thlimmenos v. Greece* [GC], No. 34368/97, 6 April 2000, § 44.
[89] *D.H. and Others v. the Czech Republic* [GC], No. 57325/00, 13 November 2007.
[90] Framework Convention, Article 10.
[91] Explanatory Report, § 75.
[92] Framework Convention, Article 17.
[93] Explanatory Report, § 71.
[94] Such violence has been addressed by several soft-law instruments, including the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) General Recommendation No. 1 on the digital dimension of violence against women. The Council of Europe [has also developed] a specific instrument on [combating] technology-facilitated violence against women and girls.

48. AI systems may be prone to discrimination by proxy. This means that seemingly neutral pieces of information that indirectly correlate with protected characteristics can disguise bias, making it increasingly difficult to trace and detect an AI-based discrimination. For example, the use of data like postal codes or spending habits seem neutral but as proxies may indirectly reflect characteristics such as ethnicity, gender or socio-economic status, resulting in difficulties to trace and detect discrimination.[95] Another concern is AI systems' capacity for intersectional discrimination where multiple grounds of discrimination intersect.[96]

The Right to Privacy and Personal Data Protection

i. The Right to Privacy and Data Protection in the ECHR and other relevant instruments

49. Article 8 ECHR (the right to respect for private and family life), through the protection of private life, applies to the collection and processing of personal data.[97] Private life includes, among other things, one's image, identity, personal development, and relationships, and extends also to professional or business activities. Personal data covers information such as names, addresses, IP addresses, and sensitive data like information relating to health and ethnicity. Article 8 is also engaged in relation to the interception of communications, such as emails and phone calls. Such measures constitute an interference with the right to respect for private life and any such interference must be lawful, pursue a legitimate aim, be necessary and proportionate.

50. Council of Europe Convention No. 108[98] protects individuals with regard to automatic processing of personal information relating to them and is the only legally binding international treaty dealing exclusively with this issue.[99] Convention No. 108 defines personal data as "any information relating to an identified or identifiable individual".[100] Key principles of personal data

---

[95] Other examples of proxies would include shoe size as a proxy for gender, names as a proxy for ethnicity or age, occupation as a proxy for gender, etc. See Fundamental Rights Agency, Bias in Algorithms – Artificial Intelligence and Discrimination (2022), p. 24. For further examples, see the report of the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance A/HRC/56/68, published 3 June 2024, paragraphs 18, 32, 40.; *Discrimination, Artificial intelligence and algorithmic decision-making,* Directorate General of Democracy, Council of Europe, 2018; Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Gender Equality Commission (GEC) and the Steering Committee on Anti-discrimination, Diversity and Inclusion (CDADI) (2023), pp 17, 56-57, 63, 88

[96] See Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, pp. 57-58, "[b]ecause of the granularity of algorithmic profiling, AI systems are able to infer several protected social memberships and potentially cluster users according to different problematic classifications. For example, algorithmic profiles might contain information regarding gender, age, ethnic background, religious beliefs, sexual orientation or gender identity based on the analysis of online behaviours, consumer preferences, etc".

[97] For the Court's caselaw on the protection of personal data see T-PD(2023)1 Case Law on Data Protection (December 2022) and Guide on Article 8 of the European Convention on Human Rights.

[98] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). The Convention is amended by the 2018 Protocol (CETS No. 223), not yet in force, which addresses the challenges to privacy resulting from the use of new information and communication technologies and strengthens the Convention's mechanism to ensure effective implementation. Convention 108 as will be amended by the Protocol, upon the latter's entry into force, is often referred to as "Convention 108+".

[99] Among them, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, amended in 2013) and 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/GDPR).

[100] Article 2. See also Article 1 of Convention 108+, which states that "the purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy."

processing include lawfulness, necessity, proportionality, fairness, transparency, purpose limitation, data minimization, accuracy, data security, accountability, and user control over their information. Individuals must be informed of how their data is collected and processed and retain the right to request correction or erasure. Personal data should be processed on a valid legal basis and for pre-selected legitimate purposes. The Court has on several occasions referred to the standards of Convention No. 108 in its judgments concerning data protection.[101]

51. The protection of privacy rights and personal data protection is a common principle required for effective realisation of many other principles in the Framework Convention.[102] The Framework Convention obliges Parties to adopt or maintain measures ensuring the protection of privacy and personal data throughout the lifecycle of AI systems.[103] This includes compliance with applicable domestic and international laws, such as the ECHR and Convention No. 108.[104] Other instruments of the Council of Europe also stress the necessity of effective safeguards to address risks to privacy and data protection arising in relation to the use of AI systems.[105]

ii. Privacy and Data Protection Risks

52. AI systems may pose significant risks to privacy and data protection, particularly due to their reliance on large volumes of personal data for training and operation purposes. AI systems often collect, analyse, and infer sensitive information—sometimes without the individual's knowledge—raising concerns about valid legal basis, data minimization, and purpose limitation. The use of AI in areas like targeted advertising, social media monitoring, and biometric identification can lead to pervasive surveillance, including mass surveillance, and profiling, potentially violating individuals' rights to privacy and autonomy.

53. Additional risks include the risk of exposing personal data through re-identification and data leaks. When personal data is processed by opaque or complex models, it becomes difficult to assess how the data is used or whether individuals' rights are being respected. This lack of transparency undermines accountability and makes it harder for individuals to exercise their rights under data protection laws, such as access, correction, or deletion of their data, or the new generation of data subject rights. These risks are amplified and can have serious human rights implications in contexts such as law enforcement or border control.[106]

Effective remedies

---

[101] *Z. v. Finland*, No. 22009/93, 25 February 1997, § 95; *Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000, § 65; *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000, § 43; *P.G. and J.H. v. the United Kingdom*, No. 44787/98, 25 December 2001, § 57; *Sofianopoulos and Others v. Greece* (dec.), Nos. 1977/02, 1988/02 and 1997/02, 16 February 2000; *Peck v. the United Kingdom*, No. 44647/98, 28 April 2003, § 78,; *Von Hannover v. Germany*, No. 59320/00, 24 September 2004, § 42; *Cemalettin Canlı v. Turkey*, No. 22427/04, 18 February 2009, §§ 17 and 34,; *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, §§ 41, 66, 68, 76, 103, 104, and 107; *Uzun v. Germany*, No. 35623/05, 2 September 2010, § 47.

[102] Framework Convention Explanatory Report, § 79.

[103] Framework Convention, Article 11.

[104] Explanatory Report, §§ 80-83.

[105] See the 2019 Guidelines on Artificial Intelligence and Data Protection adopted by the Consultative Committee of Convention 108; Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems; Recommendation CM/Rec(2021)8 of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of profiling highlight the right of individuals to object to profiling and require robust safeguards, especially where profiling significantly affects their rights

[106] Adopted by the Consultative Committee of the Convention 108.

i. The right to an effective remedy in the ECHR, ESC, and other relevant instruments

54. Article 13 of the ECHR guarantees everyone the right to an effective remedy when their rights and freedoms under the ECHR are violated. Remedies must be available, accessible and affordable, effective in both law and practice, and capable of addressing the substance of the alleged violation and providing appropriate redress.[107] They can include judicial mechanisms or a quasi-judicial body such as an ombudsman[108], or a political authority such as a parliamentary commission.[109] If not before a judicial authority, they should nevertheless be independent and procedural safeguards should be afforded to the applicant.[110] In certain circumstances, however, a remedy before a judicial authority may be essential (for example concerning review and supervision of secret surveillance measures) or desirable.[111] States' positive obligations[112] may require them to provide an effective remedy also with respect to human rights abuses by private actors, including businesses. [113]

55. The ESC does not contain an explicit right to an effective remedy, however, the ESCR has interpreted the ESC as requiring an effective remedy in certain cases.

56. In line with its Article 9, Parties to the Framework Convention are required to adopt new frameworks or mechanisms or maintain existing ones in order for all actors responsible for activities within the lifecycle of AI systems, irrespective of whether they are public or private organizations, to be answerable for adverse impacts on human rights, democracy and the rule of law resulting for said activities. This may include judicial and administrative measures, civil, criminal and other liability regimes and, in the public sector, administrative and other procedures so that decisions can be contested, or the placement of specific responsibilities on operators[114]. In addition, Parties to the Framework Convention are required to adopt or maintain measures to ensure the availability of accessible and effective remedies, to the extent that remedies are required by a Parties' obligations for violations of human rights resulting from activities within the lifecycle of AI systems.[115]

ii. Risks to the Right to an Effective Remedy

57. Exercise of the right to an effective remedy may be hindered in relation to alleged violations related to AI systems due to a lack of transparency and explainability about those systems' use

---

[107] *Boyle and Rice v. the United Kingdom*, 27 April 1988, Nos. 9659/82 and 9658/82, § 52; *Powell and Rayner v. the United Kingdom*, 21 February 1990, § 31; M.S.S. *v. Belgium and Greece* [GC], No. 30696/09, January 21 2011, § 288; *De Souza Ribeiro v. France* [GC], 2012, No. 22689/07, 13 December 2012, § 78; *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], 17 July 2014, § 148, *Paulino Tomás v. Portugal*, (dec), No. 58698/00.
[108] *Leander v. Sweden*, No. 9248/81, 26 March 1987.
[109] *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, § 67
[110] *Khan v. the United Kingdom*, No. 35394/97, 12 May 2000, §§ 44-47.
[111] See for e.g., *Big Brother Watch and Others v. the United Kingdom* [GC], Nos. 58170/13, 62322/14, and 24960/15, 25 May 2021, § 336: "In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure". See also *Ramirez Sanchez v. France* [GC], No. 59450/00, 4 July 2006, §§ 165-166; *Danilczuk v Cyprus*, No. 21318/12, 3 April 2018, §§ 44.
[112] On positive obligations, see below, section 3.2.1.
[113] *Z and Others v. the United Kingdom* [GC], No. 29392/95, 10 May 2001, § 109; *Keenan v. the United Kingdom*, No. 27229/95, 3 April 2001, § 129; *Paul and Audrey Edwards v. the United Kingdom*, No. 46477/99, 14 June 2002, § 97.
[114] Explanatory Report, §§ 66-68.
[115] Framework Convention, Article 14. This includes documenting and making relevant information available where appropriate and applicable to affected individuals, enabling them to understand and exercise their rights. See Framework Convention Explanatory Report, §99.

and to their technical complexity, opacity, and reliance on vast datasets and various upstream actors in the supply chain. Individuals may lack the knowledge or access to information necessary to identify violations and the responsible person or entity. They may also remain unaware of the extent of interference with their rights or struggle to understand the underlying decision-making processes. As noted above, remedies should be accessible – available and comprehensible to individuals – and effective, meaning that they can adequately address and afford redress in respect of violations of human rights related to AI systems.

58. Moreover, overreliance on AI may lead to the unintentional shift of responsibility onto the system itself, creating accountability gaps. Without clear legal frameworks or oversight mechanisms, individuals may face barriers in accessing justice, including delays, lack of information, or inadequate review processes.

3.2 Business and Human Rights

59. This section explores the intersection of AI-related business activities and human rights obligations, focusing on States' positive obligations under the ECHR and ESC, the balancing of human rights of businesses and individuals, and the corporate responsibility to respect human rights within the broader framework of non-binding international standards.

3.2.1 Positive obligations under the ECHR and the ESC[116]

60. The ECHR and ESC do not impose human rights obligations directly on to businesses not carrying out a public function. While individuals cannot directly raise complaints against businesses before the Court or the ECSR, they may, depending on the right adversely impacted, bring claims against States for failing to prevent or address abuses resulting from business-related activities.

61. Under the ECHR and caselaw of the Court, States may, for example, be expected to be held accountable where they acquiesce or connive in acts of private actors that abuse human rights[117] or when they fail to properly regulate private industry.[118] The concrete scope and content of State obligations developed through the Court’s caselaw depend to some extent on the human right in question and the factual circumstances. Recommendation CM/Rec(2016)3 on human rights and business states that positive obligations consist of requirements to prevent human rights violations where the competent authorities had known or ought to have known of a real risk of such violations; to undertake an independent and impartial, adequate and prompt official investigation where such violations are alleged to have occurred; to undertake an effective prosecution, and to take all appropriate measures to establish accessible and effective mechanisms which require that the victims of such violations receive prompt and adequate reparation for any harm suffered.[119] A failure to take reasonably available measures which could have had a real prospect of altering the outcome or mitigating the harm is sufficient to engage the responsibility of the State.[120]

---

[116] It is also possible for States to breach their negative obligations, in cases where business-related human rights abuses are attributable to the State. This could occur, for instance, where a business is owned or controlled by the State; or a business is acting as an agent of the State. Nevertheless, this Handbook focuses on positive obligations given that, at present, relevant activities within the lifecycle of AI systems lifecycle are largely conducted by the private sector.
[117] *Ilaşcu and Others v. Moldova and Russia* [GC], No. 48787/99, 8 July 2004, § 318.
[118] *Hatton and others v. the United Kingdom* [GC], No. 30622/1997, 8 July 2003, § 98
[119] Committee of Ministers Recommendation CM/Rec(2016)3 on human rights and business, §15.
[120] *E. and Others v. the United Kingdom*, No. 33218/96, 26 November 2002, §§99-100.

62. The ESC also affords protection against business-related human rights abuses, particularly regarding the rights of workers. Member States that have ratified the ESC should take all appropriate national and international measures to ensure the effective realisation of the rights and principles of the ESC and consider increasing the number of accepted provisions.[121]

63. Positive obligations under the ECHR may arise in a wide range of situations, such as media businesses interfering with freedom of expression;[122] abuses in private hospitals[123] and schools;[124] workplace dress restrictions affecting the right to manifest religion;[125] providing workers with information to assess occupational health and safety risks;[126] or environment-related human rights harms caused by business activities.[127] Under the ESC, positive obligations may arise, for example, with regard to the right to health under Article 11,[128] the prevention of forced labour and other forms of labour exploitation,[129] or taking appropriate preventive measures (information, awareness-raising and prevention campaigns in the workplace or in relation to work) in order to combat moral harassment.[130]

64. The Court's caselaw, in specific circumstances, highlights (i) positive obligations to regulate and control business operations; (ii) procedural positive obligations to enable public participation and informed decision making; and (iii) positive obligations to provide effective remedies for business-related human rights violations. With regard to positive obligations under the ESC, the ECSR has examined the obligations of States to regulate and supervise the conduct of private actors in relation to environment[131], education[132] and energy[133]. The ECSR has highlighted that private sector involvement in relation to ESC rights-related services must not result in the enjoyment or achievement of ESC rights being undermined.[134]

---

[121] Recommendation CM/Rec(2016)3 on human rights and business, §16; see also *Marangopoulos Foundation for Human Rights (MFHR) v. Greece*, Complaint No. 30/2005, decision on admissibility of 10 October 2005, §14, the ECSR decided that the State is responsible for enforcing the rights embodied in the Charter within its jurisdiction, even if the State has not acted as an operator but has simply failed to put an end to the alleged violations in its capacity as regulator. In Statement of Interpretation on Article 17§2 – Private sector involvement in education, Conclusions 2019, states Parties are required to regulate and supervise private sector involvement in education strictly, making sure that the right to education is not undermined.

[122] *Von Hannover v. Germany* [No. 2]
[GC], Nos. 40660/08 and 60641/08, 7 February 2012.

[123] *Storck v. Germany*, o. 61603/00, 16 June 2005.

[124] *Costello-Roberts v. the United Kingdom*, No. 13134/87, 25 March 1993.

[125] *Eweida and Others v. the United Kingdom*, Nos. 48420/10 and 3 others, 27 May 2013.

[126] *Vilnes and Others v. Norway*, Nos. 52806/09 and 22703/10, 24 March 2014.

[127] *Lopez Ostra v. Spain,* No. 16798/90, 9 December 1994; *Guerra and Others v. Italy* [GC], No. 116/1996/735/932, 19 February 1998, § 58; *Taşkin and Others v. Turkey*, No. 46117/99, 30 March 2005; *Fadeyeva v. Russia*, No. 55723/00, 9 June 2005, § 89.

[128] ECSR, Conclusions 2005 - Statement of interpretation - Article 11.

[129] ECSR, Conclusions 2020, Albania.

[130] ECSR, Conclusions 2014, Azerbaijan; Conclusions 2005, Republic of Moldova.

[131] *Marangopoulos Foundation for Human Rights (MFHR) v. Greece*, Complaint No. 30/2005, decision on admissibility of 10 October 2005, §14.

[132] Conclusions 2019, Statement of Interpretation on Article 17§2 – Private sector involvement in education.

[133] *Defence for Children International (DCI), European Federation of National Organisations working with the Homeless (FEANTSA), Magistrats Européens pour la Démocratie et les Libertés (MEDEL), Confederación Sindical de Comisiones Obreras (CCOO) and International Movement ATD Fourth World v. Spain*, Complaint No. 206/2022, decision on the merits of 11 September 2024, §§55-57.

[134] *Defence for Children International (DCI), European Federation of National Organisations working with the Homeless (FEANTSA), Magistrats Européens pour la Démocratie et les Libertés (MEDEL), Confederación Sindical de Comisiones Obreras (CCOO) and International Movement ATD Fourth World v. Spain*, Complaint No. 206/2022, decision on the merits of 11 September 2024, §57.

Obligations to regulate and supervise business activities

65. Within the context of their positive obligations as previously explained, States have a duty to protect against human rights abuses by third parties, including business enterprises, and take reasonable and appropriate measures to secure an individual's human rights. Depending on the circumstances and the specific context of each case, questions arising include whether the national authorities could reasonably be expected to act so as to prevent or put an end to the alleged infringement[135], and whether they took the necessary steps to ensure the effective protection of the applicants' rights.[136] States have an obligation to provide protection against human rights violations committed by third parties, including commercial enterprises, through mandatory human rights due diligence obligations, effective regulations and oversight mechanisms throughout the AI lifecycle.

66. States may also be accountable for failure to inform the public about risks of dangerous activities and to issue warnings.[137] In the context of Articles 8 (the right to private and family life) and 2 (the right to life), there is an obligation to provide essential information to the public about dangerous activities involved in the business activity.[138] Moreover, the public's right to information should not be confined to risks that have already materialised but should count among the preventive measures to be taken.[139]

67. States should consider whether businesses involved in the AI lifecycle are subject to adequate oversight. The question of whether the State could reasonably be expected to act so as to prevent or put an end to the alleged infringement of the applicant's rights could apply to State failures to address, for example, "algorithmic bias" or opaque AI decision-making processes.

Procedural positive obligations to enable public participation and informed public decision making

68. State decisions in relation to business activities – such as granting a licence – may also impact on human rights and so the risks and potential impact should be assessed before decisions are taken. Decision-making processes "concerning issues of cultural, environmental and economic impact […] must necessarily involve appropriate investigations and studies in order to allow [public authorities] to strike a fair balance between the various conflicting interests at stake".[140] To afford due respect for the interest protected by, for example, Article 8 ECHR, the decision-making process leading to measures of interference should "consider all the procedural aspects, including the type of policy or decision involved, the extent to which the views of individuals were taken into account throughout the decision-making process, and the procedural safeguards available".[141] In environmental cases, this requires investigations and studies "'to predict and evaluate in advance the effects of those activities which might damage the environment and infringe individuals' rights".[142] State regulation "must also provide for appropriate procedures, taking into account the

[135] *Fadeyeva v. Russia*, No. 55723/00, 9 June 2005, § 89.
[136] *López Ostra v. Spain*, § 55; *Guerra and Others v. Italy*, § 58.
[137] *Tătar v. Romania*, Application No. 67021/01, 27 January 2009, §§ 113-116, 121-124.
[138] *Vilnes and Others v. Norway*, Nos. 52806/09 and 22703/10, 24 March 2014, § 235; *Roche v. the United Kingdom* [GC], No. 32555/96, 19 October 2005 § 162.
[139] *Vilnes and Others v. Norway*, Nos. 52806/09 and 22703/10, 24 March 2014, § 235.
[140] *Zammit Maempel v. Malta*, Application No. 24202/10, 22 November 2011, § 62.
[141] *Taskin and Others v. Turkey*, § 118.
[142] Idem.

technical aspects of the activity in question, for identifying shortcomings in the processes concerned and any errors committed by those responsible at different levels".[143]

69. In the Framework Convention, the principles of transparency and oversight[144] require "openness and clarity in the governance of activities within the lifecycle of artificial intelligence systems and mean that the decision-making processes and general operation of artificial intelligence systems should be understandable and accessible to appropriate artificial intelligence actors and, where necessary and appropriate, relevant stakeholders".[145]

70. In order to ensure full enjoyment of human rights and democratic freedoms, Committee of Ministers Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems recommends that States should foster general public awareness of the capacity, power and consequential impacts of algorithmic systems, including their potential use to manipulate, exploit, deceive or distribute resources, with a view to enabling all individuals and groups to be aware of their rights and to know how to put them into practice, and how to use digital technologies for their own benefit. In addition, all relevant actors, including those in the public, private and civil society sectors in which algorithmic systems are contemplated or are in use, should promote, encourage and support in a tailored and inclusive manner (taking account of diversity with respect to, for instance, age, gender, race, ethnicity, cultural or socio-economic background) a level of media, digital and information literacy that enables the competent and critical consideration of and use of algorithmic systems.[146]

Obligations relating to the provision of effective remedies

71. States may be required to provide effective remedies for business-related human rights abuses. This may include amending laws if the legal framework is inadequate[147] and ensuring that businesses comply with domestic law. Of relevance here is the right to an effective remedy (Article 13 ECHR).

Margin of appreciation in the context of positive obligations

72. It is important to note that States generally enjoy a wide margin of appreciation in deciding how to fulfil their obligations regarding business activities potentially impacting human rights. The margin of appreciation shrinks, however, if State measures interfere with a particularly intimate aspect of the individual's private life,[148] depending on the seriousness of the threats to the right at issue.[149] Moreover, the onus is on the State to justify, using detailed and rigorous data, a situation in which individuals bear a heavy burden on behalf of the rest of the community.[150]

73. Thus, while a margin of appreciation in regulating AI technologies in the context of businesses activities is expected, it could be significantly limited when AI systems present serious risks to human rights.

---

[143] *Öneryıldız v. Turkey* [GC], § 90.
[144] See Framework Convention Article 8.
[145] Framework Convention Explanatory Report, para 57.
[146] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, section B, para 1.3.
[147] *Fadeyeva v. Russia*, No. 55723/00, 9 June 2005, §§ 89 and 92; see also *Powell and Rayner v. the United Kingdom*, No. 93101/81, 21 February 1990.
[148] *Hatton & Others v United Kingdom* [GC], No. 36022/97, 8 July 2033, § 102.
[149] *Brincat and Others v. Malta*, Application No. 60908/11 et al., 24 July 2014, § 116.
[150] *Dubetska and Others v. Ukraine*, Application No. 30499/03, 10 February 2011, § 145.

3.2.2 Balancing Rights of Businesses in the Context of AI Governance

74. Transparency and explainability requirements in relation to, for example, bias mitigation raise questions around the intersection of the rights of individuals and intellectual property and trade secrecy laws. A business's own AI system may be covered by intellectual property and trade secrecy legislation. In addition, in some contexts, businesses may be entitled to the protection of some specific rights under the ECHR, such as property rights (Article 1 Protocol 1 ECHR, which includes intellectual property)[151] or the freedom of expression (Article 10 ECHR)[152].

75. If rights holders claim that AI systems operated by private businesses abuse their rights, the State's response may need to balance these competing interests. For instance, the obligation to provide essential information for the public may conflict with a business's intellectual property rights (protected by the right to property – Article 1 of Protocol 1 of the ECHR). Domestic courts or regulators should carefully weigh these interests to ensure a fair and proportionate outcome.

76. The Framework Convention's drafters noted in connection with the principle of transparency (article 8 of the Framework Convention) that "in implementing this principle, Parties are required to strike a proper balance between various competing interests and make the necessary adjustments in the relevant frameworks without altering or modifying the underlying regime of the applicable human rights law".[153]

77. In the context of algorithmic systems, the Recommendation of the Committee of Ministers CM/Rec(2020)1 on the human rights impacts of algorithmic systems provides that legislative frameworks for intellectual property or trade secrets should not preclude transparency or be exploited to obstruct accountability, nor should confidentiality or trade secrets inhibit effective human rights impact assessments.[154] Furthermore, States should establish appropriate levels of transparency with regard to the public procurement, use, design, and basic processing criteria and methods of algorithmic systems implemented by and for them, or by private sector actors.[155]

3.2.3 Key Non-Binding Frameworks on Business, Human Rights and AI

Relevant non-binding instruments

78. Relevant global and regional governance frameworks include the **UN Guiding Principles on Business and Human Rights (UNGPs)**. The UNGPs provide for a set of principles that states and businesses ought to apply or consider applying (depending on the circumstances), using the "Protect, Respect and Remedy" framework: (i) the State duty to protect against abuses, (ii) corporate responsibility to respect human rights, and (iii) access to remedies for victims.

79. Building on the UNGPs, the Committee of Ministers of the Council of Europe adopted Recommendation CM/Rec(2016)3 on human rights and business. It provides specific guidance to

---

[151] *Anheuser-Busch Inc. v. Portugal* [GC], No. 73049/01, 11 January 2007, § 72.
[152] *Axel Springer AG v. Germany* [GC], No. 39954/08, judgment of 7 February 2012.
[153] Explanatory Report Framework Convention, § 62.
[154] CM/Rec(2020)1, § 5.2
[155] Idem, § 4.1 The transparency levels in question should be as high as possible and proportionate to the severity of adverse human rights impacts. The use of such systems in decision-making processes that carry high risk to human rights should be subject to particularly high standards.

assist member States in preventing and remedying human rights abuses by business enterprises and insists on measures to induce business to respect human rights.

80. Another relevant instrument is the **OECD Guidelines for Multinational Enterprises on Responsible Business Conduct**, which provides detailed recommendations on responsible business conduct addressed by governments to multinational enterprises.

81. Council of Europe member States' duty to protect against business-related human rights abuses and to provide effective remedies is best explained by the jurisprudence of the Court and the decisions and conclusions of the ECSR, as detailed above. The responsibilities of businesses to respect human rights in the context of AI can be examined through the framework of the UNGPs, as will be explained below.

Corporate Responsibility to Respect Human Rights

82. The UNGPs advocate for businesses to put in place policies and processes, including (i) policy commitments to meet their responsibility to respect human rights; (ii) human rights due diligence to identify, prevent, and address adverse human rights impacts; (iii) processes to enable the remediation of their adverse human rights impacts.[156] Businesses are expected to use both qualitative and quantitative indicators, integrating this tracking into internal processes and seeking stakeholder feedback (Principle 20). When businesses cause or contribute to adverse impacts, they should provide or cooperate in remediation through legitimate processes (Principle 22). If impacts are linked to the company's operations but not directly caused by it, the enterprise is not required to provide remedies itself but may play a supporting role in broader efforts. In cases where prioritisation is necessary, businesses should focus first on the most severe or irremediable impacts to minimise harm (Principle 24). Communication about these measures should be transparent and accessible, balancing legitimate confidentiality concerns with the need for accountability (Principle 21).

83. To date, no AI-specific general guidance on corporate responsibility for human rights has been developed.[157] The UNGPs may provide a framework for addressing human rights impacts across the AI value chain. Businesses should assess and mitigate human rights risks throughout the AI lifecycle, from design to deployment, with transparency and accountability as central principles. Human rights due diligence should evaluate direct and indirect impacts, focusing on risks to individuals, and should be adapted dynamically to the evolving nature of AI technologies. Arguably, AI-specific human rights impact assessments to identify human rights risks, including those arising from third-party uses of AI systems, should be developed and applied.

84. In the AI specific context, the HUDERIA Methodology,[158] while not a specific instrument on corporate responsibility to respect human rights, is addressed to both public and private actors. It

---

[156] UNGPs, Principle 15-24.

[157] The OECD is developing guidance on responsible business conduct due diligence in the development and use of trustworthy AI systems and has already provided guidance with respect to finance and platform companies. In addition, the UN Human Rights B-Tech Project has identified three broad headlines and associated practical recommendations for how lawmakers, standard setters, businesses and civil society can leverage the UNGPs to foster governance and business practices capable of tackling human rights impacts and risks of generative AI, see Advancing Responsible Development and Deployment of Generative AI: A UN B-Tech foundational paper | OHCHR.

[158] The Council of Europe applies the HUDERIA in its capacity-building activities, such as the HUDERIA Academy, which provides training sessions for government officials, sectoral regulators, public institutions, sectoral professionals, academy and civil society representatives. The HUDERIA is also used as a basis for engagement with private-sector AI developers on issues relevant to the implementation of the Framework Convention.

connects international human rights standards and existing technical frameworks on risk management in the AI context and provides a structured approach to risk and impact assessment of AI systems specifically tailored to the protection and promotion of human rights, democracy and the rule of law.

85. Recommendation CM/Rec(2016)3 on human rights and business calls upon member States to apply such measures as may be necessary to encourage or, where appropriate, require that businesses domiciled within their jurisdiction with activities within the AI lifecycle apply human rights due diligence throughout their operations and carry out human rights due diligence in respect of such activities; including project-specific human rights impact assessments, as appropriate to the size of the business and the nature and context of the operation.[159] States should encourage and, where appropriate, require such businesses to display greater transparency in order to enable them better to "know and show" their corporate responsibility to respect human rights and where appropriate, require such businesses to provide regularly, or as needed, information on their efforts on corporate responsibility to respect human rights in the context of AI.[160]

4. PUBLIC GOVERNANCE SECTORAL ANALYSIS

86. This part examines the impact of AI systems in key areas of public governance, focusing on its implications for human rights. Drawing on the ECHR and the ESC, and other international instruments where appropriate, it explores sectors where AI system integration may lead to serious threats to human rights and where such integration is advanced or is reasonably in prospect. The sectoral descriptions at the beginning of each sector are not exhaustive and may include further activities, depending on national contexts or future developments.

87. In all these sectors, the Council of Europe's HUDERIA Methodology may be used as a framework for identification, assessment, prevention, mitigation as well as broader regulatory governance of AI risks to human rights, democracy and the rule of law.

4.1. Administration of Justice

88. Administration of justice encompasses the systems, processes, and institutions responsible for upholding the law, resolving disputes and ensuring fairness and justice. It includes courts, judges, prosecutors and lawyers and it relates to law enforcement agencies.

Key AI use cases

89. At the time of writing, 160 AI-integrated systems have been documented as being used or piloted within justice systems across Europe and other participating countries to the European Cyberjustice Network of the Council of Europe.[161] AI systems could present new opportunities and a chance for a better human rights protection and observance of the right to a hearing within a reasonable time if they are appropriately developed and used, for instance in so far as the ECHR standards and case-law are integrated in the AI-facilitated search and analysis or decision-support

[159] CM/Rec(2016)3, para 20.
[160] Idem.
[161] The Resource Centre on Cyberjustice and AI serves as a publicly accessible focal point for reliable information on AI systems and other cyberjustice tools, aiming at providing a starting point for further examination of their risks and benefits for professionals and end-users. It is monitored by the CEPEJ Artificial Intelligence Board (https://www.coe.int/en/web/cepej/ai-advisory-board).

tools. While AI systems designed for ancillary administrative tasks pose minimal risk,[162] those directly assisting judicial authorities in researching, interpreting facts, and applying the law to specific cases present significant risks to fair trial rights and related human rights. Administration of justice was among the first public governance sectors for which the Council of Europe addressed the implications of the use of AI systems on human rights, through the publication of its European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" ("the Ethical Charter").[163]

90. Key AI use cases in this context include:

- *AI-facilitated search, review, analysis and Large-Scale Discovery*: AI systems that create a searchable collection of case-law descriptions, legal text and other insights to be shared with legal experts for further analysis and large-scale discovery on high volumes of electronic documents. Examples include search engines with interfaces applied to case law and judicial files.
- *Decision support*: Systems that facilitate or automate stages in the decision-making processes. Examples include summarising texts, extracting specific information in application, providing guidelines and benchmark and calculating scales for sentencing and compensation. Fully automated decision-making processes without any human supervision have not been reported in Europe so far.
- *Prediction of judicial outcomes*: Systems that learn from large datasets to identify patterns in the data that are consequently used to visualize, simulate or predict new litigation outcomes.
- *Online dispute resolution (ODR)*: These cover technologies used for the resolution of disputes between parties with limited human intervention. It concerns mainly alternative dispute resolution, but also dispute resolution in the context of courts.
- *AI based judge appointments and case allocation*: Systems used to complete or facilitate tasks such as allocating cases to courts and judges and attaching levels of priority.

91. Other applications, such as the use of AI for interpretation during hearings or recording, transcription or translation could also challenge elements of the right to a fair trial depending on the circumstances.

Relevant human rights and principles

92. The principles identified in the Framework Convention[164] and the European Ethical Charter on the Use of Artificial Intelligence correspond to significant, real concerns vis-à-vis the use of AI in administration of justice and its possible negative impacts on of human rights as protected in the ECHR, as well as in Convention 108(+). Principles of the Ethical Charter include respect for fundamental rights, non-discrimination, quality and security, transparency, impartiality and fairness; and the principle of "under user control".[165]

---

[162] Such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel and the automation of other administrative tasks.
[163] The Ethical Charter, adopted by the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, is one of the first regulatory documents on AI that provides a set of principles to be implemented by public and private stakeholders responsible for the design and development of AI tools and services in administration of justice.
[164] Framework Convention (Articles 4 to 13).
[165] The principle of "under user control" precludes a prescriptive approach and ensuring that users are informed actors and in control of their choices.

93. The human right primarily impacted in this sector is the right to a fair trial, guaranteed by Article 6 ECHR.[166] The right to liberty and security, guaranteed by Article 5 ECHR, is also engaged insofar as it involves special rules on judicial protection against arbitrary deprivation of liberty.

The right to a fair trial

94. Article 6 ECHR applies to proceedings involving the determination of civil rights and obligations or of any criminal charge. The key principle governing Article 6 is fairness.[167] As highlighted by the Court, what constitutes a fair trial cannot be the subject of a single unvarying rule but must depend on the circumstances of each case and in light of the overall fairness of the proceedings.[168] Certain subsidiary principles of fairness are also particularly relevant in the AI context:

(i) Independence and impartiality

95. Article 6 guarantees a fair and public hearing by an independent and impartial tribunal established by law.[169] The tribunal should be independent both from other branches of government, such as the executive and legislature, and from the parties involved in a case.[170] The tribunal must also be impartial, namely subjectively free of personal prejudice or bias and must offer sufficient guarantees to exclude any legitimate doubt in this respect.[171]

96. Bias in AI systems may not be easily discernible by the judge due to the generalised perception of algorithmic/mathematic "neutrality" and judges' own technology bias. This could lead to discriminatory outcomes. Extensive reliance on AI could lead to a "standardisation" of judicial decisions, with judges feeling compelled to follow AI recommendations due to the perceived "superiority", particularly in systems where their terms of office are not permanent but subject to popular vote,[172] or in which their personal liability (disciplinary, civil or even criminal) is likely to be incurred.[173]

(ii) Presumption of innocence

97. The principle of presumption of innocence in criminal proceedings requires, among other things, that: (i) judges (and jurors where applicable) must approach their duties without any preconceived notion of the accused's guilt; (ii) the burden of proof is on the prosecution, and (iii) any doubt should benefit the accused.[174]

---

[166] Also other international human rights instruments (articles 10 and 11 of the Universal Declaration of Human Rights, article 14 of the International Covenant on Civil and Political Rights, article 47 of the Charter of Fundamental Rights of the European Union, article 8 of the American Convention on Human Rights-Pact of San José, article 7 of the African Charter of Human and Peoples' Rights) and in the constitutional legal order of democratic countries.
[167] *Vacher v. France*, No. 20368/92, 17 December 1996.
[168] *Ibrahim and Others v. the United Kingdom* [GC], Nos 50541/08, 50571/08, 50573/08, 40351/09, 13 September 2016, § 250.
[169] See *Deweer v. Belgium*, No. 6903/75, 27 February 1980, § 49; *Kart v. Turkey* [GC], No. 8917/2005, 3 December 2009, § 67.
[170] *Beaumartin v. France*, No. 15287/89, 24 November 1994, § 38; *Sramek v. Austria*, No. 8790/79, 22 October 1984, § 42.
[171] *Findlay v. the United Kingdom*, No. 22107/93, 25 February 1997, § 73.; *Micallef v. Malta* [GC], No. 17056/06, 15 October 2009 § 93
[172] Of Council of Europe member States, this may be the case for appointment of cantonal judges in Switzerland.
[173] CEPEJ, *Ethical Charter*, para 140.
[174] *Barberà, Messegué and Jabardo v. Spain*, 6 December1988, Application No. 10590/83, § 77

98. As a result of algorithmic bias, the potential inclusion in AI systems of variables such as criminal history and family background means that the outcome of an individual's case may be affected by the past behaviour of a certain group without appropriate attention to the accused individual's specific background, motivations and, eventually, guilt. This could result in interfering with a person's right to be presumed innocent until proven guilty by a court of law. While the use of predictive tools by judges in criminal trials is very rare in Europe,[175] in other jurisdictions there are real-life examples of the negative effects.[176]

(iii) Equality of arms and adversarial proceedings

99. Equality of arms is an inherent feature of a fair trial. It requires that each party be given a reasonable opportunity to present a case on conditions that do not place him or her at a disadvantage vis-à-vis the opponent and applies to criminal and civil proceedings.[177] In a criminal context, the right to adversarial proceedings further means that the accused have the opportunity to familiarise themselves with and to comment on all evidence adduced or observations filed with a view to influencing the court's decision, its existence, contents and authenticity in an appropriate form and within an appropriate time.[178] Failure to disclose to the defence material evidence which could enable the accused to exonerate themselves or have their sentence reduced would constitute a refusal of facilities necessary for the preparation of the defence, and therefore a violation of Article 6.[179] The right to adversarial proceedings may not be disregarded to save time and expedite the proceedings.[180]

100. In the context of the use of AI systems, equality of arms suggests that in every case, the party should be aware of the role of the system in the proceedings, the criteria for its operation and the possible impact on the outcome of the case. Concerns may arise if a party is denied sufficient access for scrutiny of AI-analysed data used as evidence.[181] The right to adversarial proceedings is likely to require the ability to challenge an AI system's scientific validity, biases, and potential errors. However, intellectual property rights and trade secret laws may restrict access to privately-owned proprietary AI systems used by law enforcement authorities. Even without these obstacles, the complexity of the models used ("the black box problem") may present a major challenge for the defendant. Furthermore, while AI systems may expedite proceedings by saving time, the right to adversarial proceedings cannot be disregarded for this purpose.

101. In civil proceedings, equality of arms could be undermined by a possible imbalance between the parties to the dispute in their understanding and ability to use AI tools, with respect to their available means, including financial means, or even their digital literacy level. In that context, Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human

---

[175] CEPEJ, Ethical Charter, para 124.
[176] Idem, paras 128-131.
[177] *Öcalan v. Turkey* [GC], No. 46221/99, 12 May 2005, § 140; *Foucher v. France*, No. 22209/93, 18 March 1997, § 34; *Bulut v. Austria*, No. 17358/90, 22 February 1996; *Faig Mammadov v. Azerbaijan*, No. 60802/09, 26 January 2017, § 19.
[178] *Rowe and Davis v. the United Kingdom* [GC], No. 28901/95, 16 February 2000, § 60; *Kress v. France* [GC], No. 39594/98, 7 June 2001, § 74; *Krčmář and Others v. the Czech Republic*, No. 35376/97, 3 March 2000, § 42.
[179] *Natunen v. Finland,* No. 21022/04, 31 March 2009, Application No. 21022/04, §43.
[180] *Nideröst-Huber v. Switzerland*, No. 18990/91, 18 February 1997, § 30.
[181] See *Sigurður Einarsson and Others v. Iceland,* No. 39757/15, 4 September 2019. In that case, the applicants complained of not having access to the full collection of data processed by an e-Discovery system used by the prosecution. The Court acknowledged that denying access with respect to at least one of the evidentiary sets raises an issue under Article 6 § 3(b) (§91) but concluded on non-violation due to the fact that the prosecution was not aware of the contents of the full collection of data either, and that the applicants had not at any time formally sought a court order for access to the full collection of data (§§89-93). See also the partly dissenting opinion of Judge Pavli, focusing on questions of the use of AI systems.

rights and business highlights that when alleged victims of business-related human rights abuses bring civil claims related to such abuses against business enterprises, member States should ensure that their legal systems sufficiently guarantee an equality of arms within the meaning of Article 6 of the ECHR. In particular, they should provide in their legal systems for legal aid schemes regarding claims concerning such abuses. Such legal aid should be obtainable in a manner that is practical and effective.[182] In this context, the AI tools could also be developed to provide legal information and assistance and may facilitate seeking human rights protection by users, but again, appropriate safeguards should be put in place when designing such schemes.

(iv) Access to court

102. The right of access to a court is an inherent aspect of the safeguards enshrined in Article 6 and is no more absolute in criminal than in civil matters. Everyone has the right to have any claim relating to his "civil rights and obligations" brought before a court or tribunal.[183] An individual must have a clear, practical opportunity to challenge an act that is an interference with his rights.[184] The practical and effective nature of this right may be impaired by, for instance, excessive formalistic interpretation of procedural rules.

103. Within that context, resorting to AI systems, should not hinder the right of access to a court within the meaning of Article 6[185] ; human oversight over decision-making should be ensured.[186] Access to court should also not be hindered by technical hurdles related to a specific AI system. In that respect, by not considering the practical obstacles linked to the required use of an e-filing system and by not allowing for alternative (paper) submission, a domestic court may be taking an excessively formalistic approach amounting to a violation of Article 6§1.[187]

Right to liberty and security

104. The key purpose of Article 5 is to prevent unlawful, arbitrary or unjustified deprivations of liberty.[188] In order to meet the requirement of lawfulness, deprivation of liberty must be in accordance with a procedure prescribed by law and subject to review of its lawfulness by a court. While flaws in a detention order do not automatically render the detention unlawful,[189] the reasoning of the decision ordering a person's detention is a relevant factor in determining whether the detention must be deemed arbitrary under Article 5 § 1.[190]

---

[182] CM/Rec(2016)3, para 41.
[183] *Golder v. the United Kingdom*, No. 4451/70, 21 February 1975, § 36.
[184] *Bellet v. France*, No. 23805/94, 4 December 1995, § 38,
[185] See Resolution 2081 (2015) of the Parliamentary Assembly of the Council of Europe, "Access to justice and the Internet: potential and challenges", wherein PACE called to ensure that *"parties engaging in ODR procedures retain the right to access a judicial appeal procedure satisfying the requirements of a fair trial pursuant to Article 6 of the Convention*". Also CEPEJ *Guidelines on online alternative dispute resolution* (2023).
[186] The right to human oversight is set out also in Article 9(1)(a) of Convention 108+.
[187] See *Xavier Lucas v. France*, 9 June 2022, No. 15567/20, § 57, where the Court found a violation of Article 6 § 1 with respect to the fact that the French Court of Cassation had not taken into consideration the practical hurdles, including technical and substantive faults, of an e-Barreau platform that had stopped the applicant from electronically submitting a requirement to issue proceedings. See also *Farcaş and Others v. Romania,* No. 30502/05, 5 June 2018, where the Court found that the applicants' right of access to court had become illusory due to the fact that court documents had been served solely by publication (in paper and on line) in the Bulletin of Insolvency Proceedings whereas the applicants had neither the financial resources to consult the paper-version or access to the internet to consult the electronic version.
[188] *Selahattin Demirtaş v. Turkey* (No. 2) [GC], No. 14305/17, 22 December 2020, § 311.
[189] *Ječius v. Lithuania*, 2000, No. 34578/97, 31 July 2000, § 68
[190] *S., V. and A. v. Denmark* [GC], No. 35553/12, 36678/12, and 36711/12, 22 October 2018, § 92.

105. Deprivation of liberty is also unlawful under Article 5 if it results from a conviction following proceedings which were "manifestly contrary to the provisions of Article 6 or the principles embodied therein", to the point of constituting a "flagrant denial of justice".[191] A trial that is summary in nature and does not allow for a thorough and objective assessment of the case of a person who is then sentenced to imprisonment could thus amount to a violation of not only Article 6, but also Article 5 ECHR[192].

106. Issues arising under Article 6 (see above) will also apply to the judicial guarantees against arbitrary detention set out in Article 5 §§ 3 and 4, which respectively provide that criminal detainees shall be brought promptly before a judge and that everyone may challenge the lawfulness of their detention before a court. Lack of transparency or accountability in potential AI-systems could undermine the fairness of decisions on deprivation of liberty. They risk perpetuating biases, leading potentially to unjust pre-trial detention, disproportionate sentencing, or unfair parole denials. Additionally, their opacity challenges individuals' ability to contest decisions effectively, raising concerns about fairness and accountability.

Privacy and data protection in the context of administration of justice

107. Courts and authorities involved in the administration of justice handle and retain personal data, including sensitive data whose misuse could lead to data and privacy breaches and discrimination.[193] Article 8 is violated when sensitive data is retained without adequate safeguards. A fair balance must be maintained between the need to make judicial decisions public and respect for the fundamental rights of parties or witnesses.[194]

108. Anonymisation or pseudonymisation tools integrating AI technology such as those already in place in several Member States of the Council of Europe can prove useful in systematically concealing any information making individuals identifiable. However, general concerns about the risk of AI systems for privacy and data protection continue to apply as these tools are developed. The best approach to enhancing privacy is by "minimizing or eliminating the need for an organization training an AI model to collect personal data."[195]

Further reading

- Resolution 2081 of the Parliamentary Assembly of the Council of Europe, *Access to Justice and the Internet: potential and challenges*, 2015
- Resolution 2342 of the Parliamentary Assembly of the Council of Europe, *Justice by Algorithm – The Role of Artificial Intelligence in policing and criminal justice system*, 2020
- Council of Europe European Commission for the efficiency of justice (CEPEJ), *European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2018

---

[191] *Willcox and Hurford v. the United Kingdom* (dec.), Nos. 43759/10 and 43771/12, 8 January 2013, § 95; *Othman (Abu Qatada) v. the United Kingdom*, No. 8139/2009, 17 January 2012, § 259; *Stoichkov v. Bulgaria*, No. 9808/02, 24 March 2005, §§ 51, 56-58. What is required is a breach of the principles of a fair trial so fundamental as to amount to a nullification, or destruction of the very essence, of the right guaranteed by Article 6 (*Othman,* § 260).

[192] See Vorontsov and Others v. Ukraine, 2021, §§ 42-49.

[193] Convention 108(+), Article 6.

[194] Except in cases where the necessity of protecting the confidentiality of certain types of personal data is outweighed by the interest in the investigation and prosecution of crime and in the publicity of court proceedings. *Avilkina and Others v. Russia*, 7 October 2013, § 45; *Z v. Finland*, No. 22009/93, 25 February 1997, § 97.

[195] "Sharing trustworthy AI models with privacy-enhancing technologies", *OECD Artificial Intelligence Papers*, No. 38, 2025.

- Council of Europe European Commission for the efficiency of justice (CEPEJ), *Glossary on Cyberjustice and AI*
- Council of Europe European Commission for the efficiency of justice (CEPEJ), *Guidelines on electronic court filing (e-filing) and digitalization of courts*, 2021
- Council of Europe European Commission for the efficiency of justice (CEPEJ), *Guidelines on online alternative dispute resolution*, 2023, including good practices related to the Guidelines.
- Council of Europe European Commission for the efficiency of justice (CEPEJ), *Information Note on the use of Generative AI by judicial professionals in a work-related context*, 2024
- European Committee on Legal Cooperation (CDPC), Council of Europe, *Artificial Intelligence and Administrative Law*, Comparative Study, *Resource Centre on Cyberjustice and AI*, 2022. Detailed information on the deployment and usage of digital tools in administration of justice can be found in the individual country profiles
- Council of Europe Consultative Council of European Judges (CCJE), *Moving Forward: the use of assistive technology in the judiciary*, Opinion nº 26, 2023
- On AI systems geared towards the private sector: Liquid Legal Institute (LLI), *First Global Report on the State of Artificial Intelligence in Legal Practice*, 2023
- OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, 2025
- UNESCO Global Judges' Initiative: Survey on the Use of AI Systems by Judicial Operators, 2024
- Spanish Ministry of Justice, *Policy on the Use of Artificial Intelligence in the Administration of Justice*, 2024
- United Kingdom, Courts and Tribunals Judiciary, *Artificial Intelligence (AI), Guidance for Judicial Office Holders*, 2025

4.2. Law Enforcement and Public Security

109. This sector involves police,[196] intelligence and assimilated services[197], including such issues as identification of individuals for law enforcement purposes, crime prevention, crime investigation, programmes regarding protection of persons in danger (e.g. victims of domestic violence or protected witnesses), arrests and detentions, prison and probation, crowd management during public events and maintenance of public order, counterterrorism, national security operations, measures entailing surveillance of communications, restrictions, bans, prohibitions, lockdowns, various forms of supervision, including those affecting the freedom of movement.

Key AI use cases[198]

- *Digital forensics*: several tools and techniques for decryption, data recovery and analysis have been developed with AI components. These tools can recover deleted files, access data from damaged devices, restore fragmented pieces of information into coherent formats and investigate the digital footprint of criminals.
- *Surveillance systems*: technologies such as image classification, computer vision and biometrics including automated facial and voice recognition, or fingerprints.

[196] In the context of this Handbook, "police" refers to traditional police forces or services and other publicly authorised and/or controlled services granted responsibility by a State for the delivery of policing services.
[197] Government departments or units that are considered equivalent to the intelligence services in terms of their function.
[198] Based on the following report: Europol: AI and policing - The benefits and challenges of artificial intelligence for law enforcement.(2024).

- *Data analytics* employing statistical methods to extract insights from vast datasets, for instance on crime records, events and environmental factors identified in criminological insights and also unstructured data originating from open-source intelligence and social media intelligence sources.
- *Natural language processing*: performing tasks through processing textual data, such as text classification and clustering, text summarisation and machine translation, such as transcribing witness statements, analysing legal documents or extracting key information from case files.

Relevant human rights and principles

110. The development and use of AI systems in law enforcement and public security could present particular human rights risks. This is because of the strong human rights impact of actions or decisions that might be taken based on AI systems output such as surveillance, search and seizure, or arrest and detention. The use of AI systems in this sector may interfere, in particular with Articles 5 (Right to liberty and security), 8 (Right to respect for private and family life), 10 (Freedom of expression), and 11 (Freedom of assembly and association) of the ECHR, as well Article 2 of Protocol no. 4 to the ECHR (Freedom of movement).[199] States may justify interference with Articles 8, 10 and 11 ECHR by the legitimate aims listed in the texts of these articles which include national security, public safety, or the prevention of disorder or crime.

The right to liberty and security

111. Predictive policing systems make estimations and predictions that may be turned into concrete actions or decisions by the criminal justice system, including on arrest and detention. Due to the decisions that could be made based on such systems output, Article 5 ECHR (the right to liberty and security) issues may arise. Decisions on arrest or detention must be based on reasonable suspicion based on verifiable and objective facts directly linked to a criminal activity.[200] Should information provided by predictive policing systems be used to corroborate reasonable suspicion for a decision or arrest and detention, explainability and interpretability issues (the "black box problem") concerning AI systems may pose difficulties to meet the criteria required for verifiability and objectivity. Predictive policing methods must not lead to unlawful decisions on deprivation of liberty. Such operations carried out by public authorities must be lawful, necessary, and proportionate to their intended purposes and be based on clear, foreseeable, and accessible domestic law, pursuing a legitimate aim while ensuring adequate safeguards.[201]

Privacy and data protection; Freedom of Expression and Freedom of Assembly and Association

112. The use of AI systems in law enforcement may impact Articles 8 (Right to respect for private and family life), 10 (Freedom of expression), 11 (Freedom of assembly and association), as well Article 2 of Protocol no. 4 to the ECHR (Freedom of movement). The Court's jurisprudence highlights the risks for the full enjoyment of these rights presented by the broad use of AI systems in this sector.

[199] Applicable to those States that have ratified this Protocol.
[200] *Akgün v. Turkey*, No. 19699/18, 20 July 2021, §§ 156 and 175.
[201] See also Article 5.(d) of the EU AI Act, which concerns the use of AI systems in policing.

113. The storing or release of data relating to the private life of an individual by a law enforcement authority or security service amounts to an interference with the right under Article 8[202] and the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned, especially when such data are used for law enforcement purposes.[203]

114. Convention 108(+) also allows exceptions to personal data protection provisions on grounds of national security, public safety and the investigation of criminal offences; however, it requires States Parties to establish safeguards and limitations to ensure that any exceptions remain necessary and proportionate.[204] Additionally, processing activities for national security purposes must be subject to independent and effective review and supervision under the domestic legislation of the respective Party.[205]

Interception of communications and secret surveillance

115. AI-system based surveillance technologies, including facial recognition and remote biometric identification, introduce new challenges in the protection of human rights. These technologies significantly enhance the scope, speed, and scale of surveillance, including bulk interceptions, increasing risks of, for example, mass data collection, serious privacy breaches, or the potential for profiling. At the same time AI systems may be opaque, biased, or be prone to errors.

116. Surveillance of an individual by law enforcement or security services will generally involve an interference in private life, protected by Article 8 ECHR.[206] Powers of secret surveillance of citizens are permissible under the ECHR only in so far as strictly necessary for safeguarding the democratic institutions.[207] There must be relevant and sufficient reasons for the surveillance and it must be proportionate to the legitimate aim pursued.[208] Secret surveillance must be undertaken in accordance with the law. In general, this entails, that the impugned measure must have some basis in domestic law, which law must be adequately accessible and be formulated with sufficient precision to enable those to whom it applies to regulate their conduct and, if need be with appropriate advice, to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[209] In the special context of secret measures of surveillance, such as the interception of communications, “foreseeability” means that the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in

[202] *Leander v. Sweden*, No. 9248/81, 26 March 1987, § 48.
[203] *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, § 103.
[204] Article 11(1)(a), (3).
[205] Ibid.
[206] *Amann v. Switzerland* [GC], No. 27798/95, §§ 69-70, ECHR 2000-II; *Kopp v. Switzerland*, No. 23224/94, 25 March 1998, § 53.
[207] *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000, § 47; *Szabó and Vissy v. Hungary*, no 37138/14, 12 January 2016, § 54 with further reference.
[208] *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006, § 88.
[209] *Vavřička and Others v. the Czech Republic* [GC], nos 47621/13 and 5 others, 8 April 2021, §266 with further references. See also *Plechlo v. Slovakia*, No. 25132/13, 18 April 2017, § 43; see also *Big Brother Watch and Others v. the United Kingdom* [GC], nos 58170/13, 62322/14 and 24960/15, 25 May 2021, §332; *Roman Zakharov v. Russia* [GC], No. 47143/06, 4 December 2015, § 228; see also, among many other authorities, *Rotaru v. Romania* [GC], No. 28341/95, § 52, ECHR 2000-V; *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, § 95; *Kennedy v. the United Kingdom*, No. 26839/05, 18 May 2010, § 151.

which and the conditions on which public authorities are empowered to resort to any such measures.[210]

117. Measures of secret surveillance must also be "necessary in a democratic society" in pursuit of a legitimate aim. The national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aims of, among other things, protecting national security.[211] However, "in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it", guarantees against abuse which are adequate and effective are required.[212] Factors such as the "nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law" are relevant to determine compliance with the ECHR.[213]

118. Six minimum safeguards are required to prevent abuses of power when communications are intercepted in the course of criminal investigations: the nature of the offence warranting interception, categories of individuals affected, time limits, data handling procedures, safeguards for data sharing, and conditions for erasure.[214] In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge,[215] though supervision by non-judicial bodies may also be considered ECHR-compliant if the supervisory body is independent of the authorities carrying out the surveillance and is vested with sufficient powers to exercise an effective and continuous control.[216] Moreover, where a supervising judge or court adopts a passive attitude and merely endorses, without genuinely checking the facts, the actions of security services, such supervision is not compatible with Article 8.[217]

119. AI systems-based surveillance should be grounded in accessible and foreseeable legislation, pursue a legitimate aim, and include robust oversight, including judicial protection where appropriate, to protect the right to respect for private life (Article 8), freedom of expression (Article 10), and freedom of assembly and association (Article 11).

120. AI driven surveillance technologies, including biometric monitoring and behaviour-tracking, may be used also to enhance prison security. Placing a person under permanent video surveillance whilst in prison – which already entails a considerable limitation on a person's privacy – has to be regarded as a serious interference with the right to respect for privacy, as protected by Article 8 ECHR.[218] Recommendation CM/Rec(2024)5 regarding the ethical and organisational aspects of the use of AI and related digital technologies by prison and probation services emphasises that the use of such systems for maintaining safety, security and good order should be strictly necessary,

---

[210] *Big Brother Watch and Others v. the United Kingdom* [GC], Nos. 58170/13, 62322/14, and 24960/15, 25 May 2021, § 333; *Leander v. Sweden*, No. 9248/81, 26 March 1987, § 51.
[211] Ibid; *Škoberne v. Slovenia*, No. 1310/10, 12 December 2017, § 124.
[212] *Plechlo v. Slovakia*, No. 25132/13, 18 April 2017, § 43.
[213] *Škoberne v. Slovenia*, No. 1310/10, 12 December 2017, § 124; see also *Roman Zakharov v. Russia* [GC], No. 47143/06, 4 December 2015, § 232; *İrfan Güzel v. Turkey*, No. 35285/08, 7 February 2017, § 85; *Ekimdzhiev and Others v. Bulgaria*, No. 70078/12, 11 January 2022, §§ 418-419; see also *Big Brother Watch and Others v. the United Kingdom* [GC], Nos. 58170/13, 62322/14, and 24960/15, 25 May 2021; *Centrum för rättvisa v. Sweden* [GC], No. 35252/08, 25 May 2021; *Podchasov v. Russia*, No. 33618/19, 2024, § 64.
[214] *Big Brother Watch and Others*, § 335, with further references.
[215] *Big Brother Watch and Others*, § 336.
[216] *Roman Zakharov v. Russia* [GC], No. 47143/06, 4 December 2015, § 275.
[217] *Zoltán Varga and 2 others v. Slovakia*, No. 58361/12, 20 July 2021, §§ 155-163.
[218] *Vasilică Mocanu v. Romania*, No. 43545/13, 6 December 2016.

proportionate to the purpose, should avoid any negative effects on the privacy and well-being of offenders and staff and under no circumstances cause intentional physical or mental harm or suffering to a person.

121. Violations of Article 8 related to secret surveillance have been identified in cases involving human rights activists[219], members of non-governmental organisations,[220] lawyers,[221] journalists.[222] With regard to journalists, targeted surveillance measures with a view to discovering their journalistic sources may also infringe their right to freedom of expression (Article 10 ECHR), in the absence of adequate safeguards in the law or any overriding requirement in the public interest justifying such measures in the concrete case.[223] The right of journalists to protect their sources is part of the freedom to "receive and impart information and ideas without interference by public authorities" protected by Article 10 and serves as one of its important safeguards.[224]

Facial recognition

122. Facial recognition is the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates.[225] The privacy concern is that public surveillance technology enables the gathering of vast amounts of information about citizens that could be used for different, unauthorised and unlawful purposes.[226] Minimum safety measures regarding the duration, storage, usage and destruction of (biometric) personal data collected with facial recognition technology are required to ensure appropriate safeguards. The use of facial recognition technology to identify participants in peaceful demonstrations may also violate the right to respect for private life (Article 8) and freedom of expression (Article 10),[227] and freedom of assembly (Article 11). Personal data revealing political opinions falls within the special category of sensitive data attracting a heightened level of protection.[228] In the context of implementing facial recognition technology, it is essential to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards is greater where there is use of live facial recognition technology.[229] In addition to the Article 8 concerns, the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect[230] in relation to the rights to freedom of expression (Article 10 ECHR) and assembly (Article 11 ECHR).[231]

123. Facial recognition technologies, especially real-time systems, require heightened safeguards against abuse and chilling effects on freedom of expression and assembly. Member

---

[219] *Shimovolos v. Russia*, No. 30194/09, 21 June 2011.
[220] *Association "21 December 1989" and Others v. Romania*, No. 33810/07, 24 May 2011.
[221] *Vasil Vasilev v. Bulgaria*, No. 7610/15, 16 November 2021.
[222] *Azer Ahmadov v. Azerbaijan*, No. 3409/10, 22 July 2021.
[223] See Committee of Ministers Recommendation CM/Rec(2016)4 on the protection of journalism and safety of journalists and other media actors, §§ 7 & 38.
[224] *Sanoma Uitgevers B.V. v. The Netherlands* [GC], No. 38224/03, 14 September 2010, § 50.
[225] Consultative Committee of Convention 108 (T-PD), Guidelines on Facial Recognition, p. 3.
[226] OECD (2025), Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions, p. 262.
[227] *Glukhin v. Russia*, No. 11519/20, 4 July 2023, § 85.
[228] Ibid, § 76 and 86.
[229] Ibid., § 82.
[230] While the Court does not provide for a definition of chilling effect, when addressing it, it refers to measures resulting in natural and legal persons being dissuaded from exercising their rights for fear of being subject to these measures, see for example, *Wille v. Liechtenstein* [GC], no. 28396/95, 28 October 1999, § 50.
[231] *Glukhin v. Russia*, § 88.

States should provide clear rules, independent scrutiny, and effective remedies to prevent arbitrary or unlawful surveillance practices that risk violating human rights and the principles of human dignity and personal autonomy. The Guidelines on facial recognition of the Council of Europe[232] provide further elaboration of measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect human rights.

Non-discrimination and equality

124. The application of AI system in law enforcement and public security also raises concerns about algorithmic bias leading to discrimination. For example, it has been shown in several cases that bias is embedded in facial recognition systems, resulting in the misidentification of suspects and, in some instances, the wrongful incarceration of innocent individuals.[233] Moreover, AI tools to enhance facial recognition technology, when trained on inadequate or skewed datasets, may reduce the accuracy of identification for some groups.[234] States should exercise caution with respect to identifying, assessing, preventing, and mitigating risks of discrimination arising from the use of, for example, facial recognition technologies or remote biometric identification systems in the law enforcement and security sectors. States may assess whether new regulations are necessary or if specific measures, including explicit prohibitions, should be implemented to prevent discrimination.[235]

125. In the context of prison and probation services, Recommendation CM/Rec(2024)5 underlines that safeguards must be in place to prevent discrimination, ensure procedural fairness, and uphold human dignity, ensuring that AI-driven prison management remains compatible with fundamental rights and the rule of law. When developing AI and related digital technologies in order to increase the accuracy and objectivity of risk assessment, the challenges of algorithmic biases and quality and representativeness of data should be addressed. Sensitivity to all kinds of diversity, including to gender perspective, different forms of disabilities and multiculturalism, should inform the design and use of risk assessment tools in order to avoid any discrimination. 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, in line with Recommendation CM/Rec(2018)5 of the Committee of Ministers to member States concerning children with imprisoned parents.

Right to an effective remedy

126. The application of AI system in law enforcement and public security raises concerns about the right to an effective remedy (Article 13 ECHR) in this context.

Further reading

[232] Adopted by the Consultative Committee of the Convention 108 in 2021.
[233] GEC/CDADI Study (2023), pp. 22-23. More examples can be found in Resolution 2342 (2020) "Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems', paragraph 7.
[234] OECD (2025), Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions, p. 262
[235] See also EU AI Act, preamble (33).

- Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling
- Report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, *Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems*, Doc. 15156, 2020
- European Court of Human Rights, *Factsheet – Mass Surveillance*,
- European Court of Human Rights, *Factsheet – Personal data protection*
- European Court of Human Rights, *Factsheet – New Technologies*
- European Court of Human Rights, *Guide on Terrorism*
- European Court of Human Rights, *National Security and European case-law*, Research Division, 2013
- Jim Murdoch & Ralph Roche, , The European Convention on Human Rights and Policing, 2015
- Venice Commission, *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware*, CDL-AD(2024)043, 2024
- EUROPOL, *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*, 2023
- European Parliament, *Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights*, 2020
- UN Human Rights Council Resolution on Freedom of Opinion and Expression, A/HRC/RES/50/15, 8 July 2022
- UN Human Rights Council Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/47/16, 7 July 2021
- OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, 2025

4.3. Immigration and Border Control

127. This sector includes activities relating to border control, conditions and modalities of entrance to and removal from the territory of the State, including issuance of visas or other kind of travel authorisations, residence permits, expulsion and deportation, asylum and refugee status and adjustments of status, translation/interpretation services, production of transcripts, collection and assessment of evidence, with due respect for international human rights obligations, including protection against refoulement, non-discrimination, privacy and procedural safeguards.

Key AI use cases

128. AI is increasingly used at all stages in immigration and border control, with the most significant deployment in pre-departure and arrival phases. Its role in the return phase remains limited in comparison.

- *Identification and verification systems*: AI supported identity checks using biometrics (e.g. automated fingerprint identification, iris scans, and facial recognition), including identification of asylum-seekers without documentary evidence of identity.
- *Predictive analytics and risk assessment systems*: forecasting and early warning tools in the context of immigration and border control.

- *AI-powered surveillance systems*: refugee camps, migrant accommodation facilities and border surveillance and monitoring using AI-powered cameras, facial recognition and AI-powered drones; AI-supported risk-assessments, search and rescue operations.
- *AI-assisted decision-making and automation*: AI-supported asylum claims verification and processing (e.g. face, speech, dialect recognition, name transliteration, and analysis of mobile phone data); generative AI to support case workers to synthesise and analyse large volumes of documentation; AI systems that provide information on immigration formalities to be completed and the living and working conditions they may expect in the country of destination.

Relevant human rights and principles

129. The ECHR does not guarantee a right to enter, settle, or reside in a specific country,[236] however, in exercising control of their borders, member States must act in conformity with their obligations under the ECHR. Non-nationals which are on the territory or subject to the extraterritorial jurisdiction of a State party will enjoy the protection of the ECHR. Caselaw also imposes certain limitations on the right of States to turn someone away from their borders, for example where this would amount to *refoulement*.[237]

130. The ESC does not grant foreign nationals a right of entry or stay in other Parties' territories either. The ESCR affirmed that ESC protections may be extended to foreign nationals from non-Party States,[238] as Parties have already guaranteed identical or inseparable rights under human rights treaties, particularly the ECHR. However, it noted that such obligations do not generally fall within its supervisory functions. The ESC obliges States Parties to adopt flexible immigration policies, easing employment regulations[239] and facilitating family reunification.[240]

131. In addition to the ECHR and the ESC, the Council of Europe has adopted several other relevant legal instruments.[241]

132. The use of AI systems in immigration and border control may raise important issues, in particular under Article 3 (Prohibition of torture), Article 8 (Right to respect for private and family life), Article 14 (Prohibition of discrimination), Article 13 (Right to an effective remedy), as well as, where applicable, Article 1 Protocol no. 7 (Procedural safeguards relating to the expulsion of aliens) and Article 4 Protocol no. 4 (Prohibition of collective expulsion of aliens) to the ECHR. Nevertheless, if appropriately implemented, it also offers chances for a better protection of human rights of persons in need thanks to a more effective migration management and time-efficient conduct of the proceedings.

Right to Privacy and Data Protection

---

[236] *Jeunesse v. the Netherlands* [GC], No. 12738/10, 3 October 2014, § 103; *Maslov v. Austria* [GC], No. 1638/03, 23 June 2008, § 68; *Üner v. the Netherlands* [GC], No. 46410/99, 18 October 206, § 54; *Boujlifa v. France*, No. 25404/94, 21 October 1997, § 42; *Abdulaziz, Cabales and Balkandali v. the United Kingdom*, Nos. 9214/80, 9473/81, and 9474/81, 28 May 1985, § 67.
[237] *F.G. v. Sweden* [GC], no. 43611/11, 23 March 2016, § 117.
[238] Conclusions 2004, Statement of Interpretation.
[239] ESC, Article 18 §§1-3.
[240] ESC, Article 19 §6.
[241] See https://www.coe.int/en/web/migration-and-refugees/council-of-europe-reference-documents-and-resources1

133. The general principles concerning privacy and data protection apply to non-nationals who find themselves within the State's jurisdiction.

134. The use of AI systems for border management, such as AI-powered drones, sensors, facial recognition and predictive analytics using personal data must be based on a legal basis and be proportionate.[242] The protection of Article 8 extends to personal data including electronic data and biometric data.[243] Blanket and indiscriminate retention of biometric data may pose a specific risk in connection with AI use and therefore for the right to respect for private life.[244] Biometric data is considered as sensitive data[245] and may reveal additional personal characteristics, such as ethnicity, health conditions, or disabilities. As a result, special protection is necessary to prevent misuse which could lead to discrimination. AI system-based identification and verification systems relying on fingerprints, iris scans, and facial recognition pose risks particularly when biometric data is collected, stored, used or shared without sufficient safeguards.

135. AI systems may generate errors, particularly when screening traveller data for security purposes such as to detect suspected terrorists or criminals. They may also overlook persons in vulnerable situations, such as victims of human trafficking, undocumented migrants in need of protection, or individuals fleeing persecution. These systems often process vast datasets from multiple sources (police, intelligence, border and asylum authorities) and are interoperable. Individuals often do not know the extent to which their data may be included.[246] Under such circumstances, oversight and the possibility to challenge wrongful inclusion and request rectification could be hampered. Depending on the specific measures triggered by an alert from a watchlist (e.g., a travel ban, denial of entry or stay, questioning, surveillance, arrest, or removal) it may, in turn, impact a broad range of rights, including freedom of movement, privacy, the right to liberty, the right to a fair trial. It can also directly or indirectly affect a spectrum of civil, political, economic, social and cultural rights of family members, including children, and associates of those listed. To avoid wrongful identification of travellers as suspects or persons posing terrorism-related threats, the relevance of individual results of automatic assessments should be carefully examined by a person in a non-automated manner.[247]

136. The creation and maintenance of AI systems used for such purposes and the procedure for their operation must provide for effective safeguards against abuse,[248] including time limits for data retention and particular protection of sensitive data such as information on someone's political views,[249] and the real possibility of requesting deletion of data[250] and rectification of false data.[251]

---

[242] *Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants*, UNHCR, 2020 A/HRC/45/9; UNGA, Report 'Contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2020) UN Doc A/75/590.
[243] See *S. and Marper v the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, §68; *Gaughran v. the United Kingdom*, No. 45245/15, 13 February 2020, §68; *Brunet v. France*, Application No. 21010/10, 18 September 2014, §39.
[244] *S. and Marper v the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, § 125.
[245] Convention 108+, Article 8.
[246] OSCE Policy Brief, Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021). p. 27.
[247] *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, Consultative Committee of Convention 108 (T-PD), Council of Europe, 2016, p. 8.
[248] *Shimovolos v. Russia*, No. 30194/09, 21 June 2011, concerning the registration of a human rights activist in a "surveillance database" that tracked his movements by train and air travel.
[249] *Catt v. the United Kingdom*, No. 43514/15, 24 January 2019, concerning the collection and retention of data on a lifelong activist in a police database for "domestic extremists."
[250] *Brunet v. France*, Application No. 21010/10, 18 September 2014, §43.
[251] *Khelili v. Switzerland*, No. 16188/07, 18 October 2011.

Non-discrimination

137. Decisions based on information from AI systems may result in discrimination, including indirect and intersectional discrimination, due to embedded bias. In addition, technologies such as facial recognition systems that use biometric data have been described as inherently fallible since they inevitably rely on statistical probabilities and are prone to inaccuracy and errors.[252] While this issue is not exclusively related to immigration, the consequences for migrants and refugees can be significant. If AI based facial recognition technologies are used for identification and identity verification at pre-departure or on arrival at borders, some individuals may be more exposed to inaccuracies and misidentification due to their protected characteristics. A combination of personal information about a person, as is used in visa and travel authorization systems, may also reveal protected characteristics. AI-assisted decision-making tools that analyse face, speech, dialect recognition, name transliteration, or mobile phone data in visa and travel authorization systems could inadvertently reveal protected characteristics, increasing the risk of biased assessments, unequal treatment and profiling. If such bias and errors are not mitigated, misidentified or discriminated individuals may be denied entry or removed to countries where they might face risks incompatible with the ECHR, including Article 3.[253]

Right to an effective remedy

138. The black box nature of AI systems can reduce transparency and explainability, leaving individuals unaware of how AI influenced decisions affecting them, such as visa denials, refugee status assessments, or removal orders. Automation bias compounds these issues. For example, the existence of an automated classification or risk score could significantly affect case workers' decisions regarding visa and residency permits or asylum applications.[254]

139. While decisions on immigration and related matters, such as entry, residence, and removal of aliens, fall outside the scope of Article 6 ECHR (right to a fair trial) as they do not engage "civil rights and obligations"[255], Article 13 ECHR (the right to an effective remedy) is applicable when other substantive ECHR rights are engaged. For instance, case law regarding removals under Article 13, when considered together with Article 3 (Prohibition of torture) of the ECHR, establishes that individuals subject to a removal measure should receive sufficient information to ensure adequate access to relevant procedures and available legal aid as well as information that could support them in substantiating their complaints.[256] Transparency and accountability in the context of AI system-based immigration and border control is thus necessary to enable individuals to exercise their right to an effective remedy.

Further reading

---

[252] The levels of inaccuracy in biometric face recognition algorithms depend heavily on gender, skin colour and age. Studies have shown that existing face recognition algorithms had more difficulties to recognise female faces and produced more false rejections and false acceptances for female faces, in particular darker female faces. See Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 5 October 2021.
[253] See e.g. *Saadi v. Italy* [GC], No. 37201/06, 29 February 2008, § 125ff.
[254] See Automating Decision-making in Migration Policy: A Navigation Guide, German Marshall Fund of the United States, 2021.
[255] *Maaouia v. France*, No. 39652/98, 5 October 2000, § 40; *Mamatkulov and Askarov v. Turkey* [GC], Nos. 46827/99 and 46951/99, 4 February 2005, §§ 82-83; *M.N. and Others v. Belgium* (dec.), No. 3599/18, 5 March 2020, § 137.
[256] *D. v. Bulgaria*, No. 29447/17, 20 July 2021, § 116; *Hirsi Jamaa and Others v. Italy* [GC], No. 27765/09, 23 February 2012, § 204; *M.S.S. v. Belgium and Greece* [GC], No. 30696/09, 21 January 2011, §§ 304-309.

- Council of Europe, *Protecting migrants under the European Convention on Human Rights and the European Social Charter*, 2013
- OSCE, *Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context*, 2021
- European Court of Human Rights, *Caselaw Guide – Immigration*
- EU Fundamental Rights Agency, *Handbook on European law relating to asylum, borders and immigration - Edition 2020,* 2020
- European Parliament, Artificial Intelligence at EU Borders, Overview of applications and key issues, 2021
- FRONTEX, Artificial Intelligence-Based Capabilities for the European Border and Coast Guard, Final Report, 2021
- EMN-OECD Inform*, The Use of Digitilisation and Artificial Intelligence in Migration Management*, 2022
- UNHRC, Report 'Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants', UN Doc A/HRC/45/9, 2020
- UNHRC, Report 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', UN Doc A/HRC/44/24, 2020
- Amnesty International, The Digital Border: Migration, Technology and Inequality, 2023
- OHCHR, Digital Border Governance: a Human Rights Based Approach
- ETIAS Fundamental Rights Guidance Board, *Guidance Note on right to an effective remedy and fair trial*
- ETIAS Fundamental Rights Guidance Board, *Guidance Note on risk for discrimination in the context of the ETIAS screening rules*
- European Union Agency for Fundamental Rights, *Guide on preventing unlawful profiling*

4.4. Democratic Processes

140. This sector includes activities relating to the organisation and administration of electoral processes and referendums, including the registration and verification of voters, management of electoral rolls, candidate registration, polling operations, vote casting and counting, tabulation and reporting of results, as well as oversight and monitoring mechanisms. It also covers the design and delivery of public information campaigns, voter education, dissemination of electoral information, and measures to ensure accessibility and integrity of the electoral process, including the use of translation or interpretation services where relevant. This section may also be relevant to other formal participatory mechanisms.

Key AI use cases

141. AI systems are used amongst other things to support, influence, inform, or automate various stages of electoral cycles, referendums, and other formal participatory democracy tools.

Use cases include:

- *AI-powered voter assistance*: chatbots and virtual assistants providing information on candidates, polling procedures locations and voter registration processes and on draft laws subject to confirmation by referendum.
- *AI-assisted electoral accessibility*: voice recognition systems enabling visually impaired individuals to access electoral information; automatic translation into sign language; adaptive interfaces for people with reduced mobility; and the automatic conversion of electoral documents into accessible formats, including digital braille, audio, or simplified language.
- *Generative AI in political campaigning*: use of synthetic text, audio, or video (such as deepfakes) for political advertising, which may influence public perception or mimic authentic communication, as well as AI-driven systems for microtargeted advertising that segment voters and automatically generate tailored political messages on digital platforms.
- *Sentiment analysis and opinion mining:* tools that scan social media, news, and online forums to gauge public sentiment on candidates, policies, or referenda questions and provide insight on emerging trends.
- *Election integrity and security*: encompasses AI-based tools for ballot scanning, counting, and verification, as well as systems for detecting cyber threats, foreign interference, and coordinated disinformation campaigns. AI tools may also be used to flag false or misleading content, deepfakes, or coordinated disinformation campaigns targeting voters.
- *AI-enabled monitoring and oversight*: tools that analyse media coverage, social media discourse, and campaign finance data to identify potential legal breaches or undue influence and support real-time fact-checking.
- *Voter data analysis and prediction*: tools that analyse historical voting patterns, demographic data, and social trends to predict voter turnout, identify areas where engagement efforts may be needed and help candidates allocate resources more effectively.
- *Data analysis in formal consultations:* AI-based systems used for content moderation, analysis of feedback to formal public consultations and consensus building.

Relevant human rights and principles[257]

142. Key ECHR rights in this sector are the right to free elections (Article 3 of Protocol No. 1 to the ECHR) and freedom of expression, including freedom to form an opinion (Article 10 ECHR). The use of AI systems in this sector may also impact privacy and data protection (Article 8 ECHR), freedom of assembly and association (Article 11), non-discrimination (Article 14 and Protocol No. 12 to the ECHR), and the right to an effective remedy (Article 13 ECHR).

143. The right to free elections is an essential principle in any democratic society and an individual right on which every enfranchised individual can rely, one that most effectively promotes "true democracy".[258] It incorporates the right to vote and the right to stand for election,[259] as well as

[257] In the context of this sector, it may be noted that the Court has given particular weight to the European Commission for Democracy through Law's (Venice Commission) *Code of Good Practice in Electoral Matters* and its accompanying Explanatory Report: see for example *Namat Aliyev v. Azerbaijan*, no. 18705/06, 8 July 2010; *Riza and others v. Bulgaria*, nos. 48555/10 and 48377/10, 13 October 2015; and *Cernea v. Romania*, no. 43609/10, 27 February 2018, *Caamaño Valle v. Spain*, no. 43564/17, 11 May 2021; *Toplak v. Slovenia*; *Myslihaka and others v. Albania*, nos. 68958/17 and 5 others, 24 January 2024.
[258] See *Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights – Right to free elections*, European Court of Human Rights.
[259] *Mathieu-Mohin and Clerfayt v. Belgium*, No. 9267/81, 2 March 1987, §§ 48-51; *Ždanoka v. Latvia* [GC], No. 58278/00, 16 March 2006, §102.

the right to political participation.[260] . Article 3 of Protocol No. 1 also requires the existence of a domestic system for the effective examination of individual complaints and appeals in matters concerning electoral rights.[261]

144. Article 3 of Protocol 1 is limited to the choice of the legislature. This can, however, include more than just the national parliament, depending on the country's constitutional structure.[262] It generally does not cover local elections at municipal or regional level,[263] unless the relevant authority exercises legislative powers such that it can considered part of the "legislature".[264] Article 3 Protocol 1 does not usually cover presidential elections, unless the president has real powers to make or block laws.[265] In principle, referendums are also not covered .[266] The limits on the scope of Article 3 Protocol 1 do not exclude the application of other relevant human rights and democratic processes to processes that fall outside its scope.

145. The right to free elections and freedom of expression are inter-related and operate to reinforce each other, together forming "the bedrock of any democratic system".[267] This entails a positive obligation on the member States to ensure the existence of conditions under which people can freely form and express their opinions and choose their representatives. The right to free elections extends beyond the moment of voting to include also aspects of the election campaign. Thus in the periods preceding and during an election, opinions and information of all kinds should in principle be permitted to circulate freely. In certain circumstances the right to free elections and freedom of expression may come into conflict and it may be considered necessary, in the period preceding or during an election, to place certain restrictions, of a type which would not usually be acceptable, on freedom of expression, in order to secure the "free expression of the opinion of the people in the choice of the legislature".[268] The right to freedom of assembly and association also plays an essential role in ensuring public debate, pluralism and the proper functioning of democracy.[269]

146. Member States are required to create a favourable environment for participation in public debate by all persons concerned, enabling them to express their opinions and ideas without fear. Under Articles 10 and 11 ECHR, the State must not only refrain from any interference in the individual's freedoms of expression, assembly and association but is also under a positive obligation to protect their right to freedom of expression against attack, including by private individuals.[270]

---

[260] *Aziz v.* Cyprus, no. 69949/01, judgment of 22 June 2004, § 28. See also UN Convention on the Rights of Persons with Disabilities, Article 29 – Participation in political and public life.
[261] *Davydov and Others v. Russia*, No. 75947/11, 30 May 2017, § 274
[262] *Timke v. Germany*, No. 27311/95, Commission decision of 11 September 1995.
[263] Xuereb *v. Malta*, No. 17056/99, decision of 30 May 2000; *Salleras Llinares v. Spain*, no. 51882/99, decision of 29 June 2000.
[264] *Repetto Visentini v. Italy* (dec.), No. 42081/10, 19 March 2021; *Miniscalco v. Italy* (dec.), no. 55093/13, 17 June 2021.
[265] *Boškoski v. the former Yugoslav Republic of Macedonia* (dec.), No. 11676/04, 3 June 2004*; Brito Da Silva Guerra and Sousa Magno v. Portugal* (dec.)*,* Nos. 26712/06 & 26720/06, 17 June 2008.
[266] *Cumhuriyet Halk Partisi v. Turkey* (dec.), No. 19920/13, 26 April 2017, §§ 33 and 38; *Moohan and Gillon v. the United Kingdom* (dec.), No. 22962/15, 13 June 2017, § 40. However, the Court takes account of the diversity of electoral systems and has not excluded the possibility that a democratic process described as a "referendum" by a Contracting State could potentially fall within the ambit of Article 3 of Protocol No. 1 (*Moohan and Gillon*, § 42).
[267] *Bowman v. the United Kingdom*, No. 24839/94, 19 February 1998, § 42.
[268] *Bowman v. the United Kingdom*, No. 24839/94, 19 February 1998, § 43; *Orlovskaya Iskra v. Russia*, No. 42911/08, 21 February 2017, § 110.
[269] See *Gorzelink & Otrs v. Poland* [GC], No. 44158/98, 17 February 2004, § 88; *Kudrevicius & Otrs v. Lithuania* [GC], No. 37553/05, 15 October 2015, § 142.
[270] *Dink v. Turkey*, Application Nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, 14 September 2010, § 106.

147. In certain circumstances, there may be tension between freedom of expression (Article 10 ECHR), freedom of assembly and association (Article 11 ECHR) and the right to free elections (Article 3 of Protocol No. 1 ECHR). In this respect, it should be recalled that Articles 10 and 11 permit restriction in certain circumstances and subject to certain conditions. To protect fair voting, in election periods, some restrictions may be considered necessary "in order to secure the free expression of the opinion of the people in the choice of the legislature".[271] However, any limitation must be proportionate to the legitimate aim pursued and necessary in a democratic society. Limits can apply to paid political advertisements if they risk giving unfair advantages to powerful groups and harming open, balanced debate, which states must protect.[272]

148. Article 5.2 of the Framework Convention states that "[e]ach Party shall adopt or maintain measures that seek to protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals' fair access to and participation in public debate, as well as their ability to freely form opinions". The voter's freedom to form an educated opinion may be affected by, for example, online information disorders, including the distribution of false information about election campaigns of political opponents.[273] AI systems can generate false information and exacerbate manipulative content curation.[274] AI tools could enable users, including malicious actors, to disseminate disinformation and misinformation that could undermine information integrity, including through the use of AI-generated content or AI-enabled manipulation of authentic content.[275] Political "deep fakes", namely the distribution of deceptive AI-generated content in the form of audio, images or video to influence an election, to infringe on voters' freedom to make informed decisions or to spread hatred and prejudice should be prohibited and sanctioned.[276] Whenever AI systems or in any other formal participatory mechanisms are being used in elections or referendums or in any other formal participatory mechanisms, voters should be informed that they are interacting with such systems rather than with a human.

149. While recognising the risks of AI systems in this context, individuals should not be subject to a decision that entails any restriction on lawful content. AI systems can help moderate harmful content on digital platforms. There is, however, also a risk that automated monitoring can result in restriction of lawful content.[277] States should ensure that AI systems used for moderation or ranking do not block lawful content or amplify disinformation in ways that harm pluralistic debate.

150. While new technologies, including AI-powered social media platforms, have enabled political parties to disseminate information directly to the electorate, they have also made it possible for hostile actors to spread disinformation and manipulate information, posing a significant threat to democracy.[278] According to the Venice Commission, "a new era of information disorder" has "distorted the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their

---

[271] *Bowman v the United Kingdom*, No. 24839/94, 19 February 1998, § 43*; Orlovskaya Iskra v. Russia*, No. 42911/08, 21 February 2017*,* § 111.
[272] *Animal Defenders International v. the United Kingdom,* No. 48876/08, 22 April 2013.
[273] *Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence*, CDL-AD(2024)044-e, Venice Commission, 2024.
[274] Explanatory Report Framework Convention, § 44.
[275] Ibid. § 43. See also the *Guidance note on countering the spread of online mis- and disinformation through factchecking and platform design solutions in a human rights compliant manner*, Council of Europe Steering Committee for Media and Information Society, 2023.
[276] CDL-AD(2024)044-e, § 8.
[277] CDL-AD(2024)044-e, § 38.
[278] *Bradshaw and others v. the United Kingdom*, no. 15653/22, 22 July 2025, §§ 134-135

votes",[279] even if it is difficult to assess accurately the impact that disinformation and "influence campaigns" may have on individual voters and, by extension, on the outcome of a given election.[280]

151. The fact that it is difficult to assess the impact of disinformation should not prevent States from taking measures to defend democratic values. However, while there is agreement among the international community that election interference through the weaponization of disinformation poses a serious threat to democracy, at present there is no clear consensus as to what specific actions States would need to take to protect their democratic processes against such risks, especially taking into account the importance of the freedom of expression.[281]

152. In order to be permissible, restrictions generally should be content-specific.[282] In principle, general bans on the operation of certain sites and systems may not be compatible with European electoral standards. Similarly, a site or an information-dissemination system should not be prohibited from publishing material solely on the basis that it may be critical of the government, or the political social system espoused by the government. However, in case an AI system has on many occasions disseminated false information aimed at influencing the election results, a general ban could be acceptable, provided that it is proportionate to the legitimate aim pursued and strictly necessary in a democratic society. In order to guarantee the stability and effectiveness of a democratic system, the State may be required to take specific measures to protect itself.[283] Sanctions should be imposed by an impartial body and subject to an effective system of appeal.[284]

153. States may also be responsible for preventing inequality in media coverage during elections.[285] Candidates and parties must be granted fair and equitable access to online media, and regulations should be implemented to ensure that AI systems used by internet intermediaries do not favour certain parties or candidates over others.[286] In this context, due regard should be had to the general standards set out in Committee of Ministers Recommendation CM/Rec(2022)12 on electoral communication and media coverage of election campaigns.

154. AI technologies are also increasingly being explored in the context of electronic voting (e-voting), including for improving system security, facilitating accessibility, notably for persons with disabilities, detecting irregularities, or supporting real-time technical troubleshooting. The Council of Europe has set standards in the field of e-voting.[287] They provide an enabling communication context for the enjoyment of the right to free elections and reflect positive obligations of the State to ensure that citizens receive necessary and truthful information on political parties to support their democratic choice to elect their representatives. These should be applied in the context of AI systems-based e-voting.

---

[279] Venice Commission, The impact of the information disorder (disinformation) on elections, CDL-LA(2018)02, para. 21
[280] *Bradshaw and others v. the United Kingdom*, no. 15653/22, 22 July 2025, § 158. See also Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09, pp. 13-14
[281] See *Bradshaw,* §§ 159-160. Also §§136-138
[282] CDL-AD(2024)044-e, § 60.
[283] *Bradshaw and others v. the United Kingdom*, No. 15653/22, 22 July 2025, § 114
[284] Explanatory Report Framework Convention, § 61.
[285] *Communist Party of Russia and Others v Russia*, No. 29400/05, 19 June 2012, §§ 125 - 128.
[286] *Urgent report on the cancellation of election results by constitutional courts*, CDL-AD(2025)003, Venice Commission, 2025. Committee of Ministers Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries describes internet intermediaries as entities that facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services (Preamble, § 4).
[287] See Committee of Ministers Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting and Recommendation CM/Rec(2017)5 on standards for e-voting.

155. While the use of digital technologies may make democratic processes more accessible to all citizens, it may also bring about obstacles and challenges to the exercise and development of electoral democracy. This is also true of AI systems. AI-driven electoral tools should be inclusive by design and guarantee accessibility to enable members of all groups, including persons with disabilities and older persons, to vote independently. In any case, accessible alternatives to AI-based systems should be guaranteed (e.g., non-digital voting options).

Non-discrimination and equality

156. States must ensure that AI systems used in elections and referendums do not lead to unequal and discriminatory outcomes. Article 14 ECHR specifically prohibits discrimination on grounds of "political or other opinions." States should address the capability of AI to generate false information or lead to the exclusion of individuals or those who may be underrepresented or in a vulnerable situation from the democratic processes. States must also ensure that AI systems do not indirectly restrict or discourage the participation of specific groups from engaging in democratic processes.

157. Given the documented risks of algorithmic bias which may also include political affiliation, strong safeguards should be applied to ensure that such systems do not exclude, disadvantage or otherwise discriminate against particular groups thereby jeopardising the principles of impartiality and neutrality in the administration of the electoral process.[288] Accordingly, through the lifecycle of AI systems in electoral contexts, proactive measures, such as the use of inclusive and representative datasets when training AI systems, to identify and mitigate discriminatory outcomes should be implemented, ensuring that political affiliation or other protected characteristics do not affect enjoyment of the right to free elections or otherwise distort the democratic process.

Transparency and Accountability

158. The existence of a domestic system for the effective examination of individual complaints and appeals in matters concerning electoral rights is one of the essential guarantees of free and fair elections. Such a system ensures the effective exercise of individual rights to vote and to stand for election, maintains general confidence in the State's administration of the electoral process, and constitutes an important device for the State to fulfil its positive duty under Article 3 of Protocol No. 1 to the Convention to hold democratic elections.[289]

159. When AI systems are used in democratic processes, it may be particularly challenging to ensure transparency and accountability. The complexity of AI systems, resulting in issues concerning explainability, and the potentially numerous upstream actors in the supply chain make it hard for individuals to detect rights violations, trace decisions and identify the accountable actors. These difficulties are compounded by evidentiary challenges. Proving that a particular AI system enabled interference had a concrete impact on the individual's right to vote or stand for election can be difficult. In practice, rights holders may find it hard to demonstrate how such interference affected their decision-making or the overall integrity of the election. Establishing a causal link between the use of AI and the distortion of democratic outcomes may require counterfactual analysis that domestic courts may not be equipped to undertake, especially where harms are diffuse and collective.

---

[288] *Sejdić and Finci v. Bosnia and Herzegovina* [GC], No. 27996/06, 22 December 2009, § 44.
[289] *Davydov and Others v. Russia*, No. 75947/11, 30 May 2017, § 274.

160. States should adopt or maintain measures to ensure the availability of accessible and effective remedies for human rights violations in the context of democratic processes resulting from the activities within the lifecycle of artificial intelligence systems. In the specific case of digital election technologies, Committee of Ministers Recommendation CM/Rec(2017)5 on standards for e-voting outlines accountability requirements for Member States, including: developing and updating technical, evaluation, and certification standards to reflect legal and democratic principles; ensuring independent evaluations of e-voting systems before introduction and after significant changes; issuing clear certificates that identify evaluation subjects and include safeguards against modifications; and maintaining an open, comprehensive audit system for e-voting to actively report potential issues.[290] These should equally apply when such systems are AI systems based.

Right to Privacy and Data Protection

161. AI systems used in electoral processes and referendums often rely on the large-scale collection, analysis, and prediction of personal data, including sensitive data. This creates heightened risks for data protection and privacy, particularly where sensitive information—such as political opinions or affiliations—is involved.

162. To address these risks, the processing of personal data in these contexts must comply with data protection standards[291] and the right to respect for private life under Article 8 ECHR. Personal data concerning i.a. political opinions, trade-union membership, and religious or other beliefs are considered as a special category of data (Art. 6 para 1 Convention 108+) and is therefore subject to heightened protection against the risks that the processing of such data may present for the rights and fundamental freedoms of the affected person. States should consider the implementation of privacy by design techniques. The collection of personal data on voters' opinions and preferences should be limited to what is necessary for those defined purposes and must not result in a disproportionate interference with the voter's interests, rights, and freedoms.[292]

Business and Human Rights

163. In the context of AI and democratic processes, private actors—particularly technology companies and internet intermediaries, including social media platforms —should consider measures to support democratic standards and human rights.[293] These include increased self-assessment and internal monitoring during electoral periods, cooperation with electoral management bodies, and ensuring basic access for all political candidates and parties to digital platforms and AI tools. Maintaining balance in the visibility of electoral content, responsible content moderation, and transparent labelling of AI-generated material and dissemination techniques used in political messaging have also been suggested. Further, platforms could provide clear information on the political nature of content and disclose its sponsors.[294]

Further reading:

---

[290] Committee of Ministers Recommendation CM/Rec(2017)5 on standards for e-voting accountability requirements for Member States, § 36-39.
[291] See in particular Article 5 of Convention 108(+).
[292] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, Consultative Committee of Convention 108 (T-PD), 2021.
[293] *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, CDL(2020)037, Venice Commission, 2020; *Interpretative Declaration of the Code of Good Practice in Electoral Matters as concerns Digital Technologies and Artificial Intelligence*, CDL-AD(2024)044, Venice Commission, 2024 .
[294] Idem.

- European Court of Human Rights, *Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights – Right to free elections*
- Venice Commission, CDL-AD(2024)044-e - *Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence*, 2024
- Venice Commission, CDL-AD(2025)003, *Urgent report on the cancellation of election results by constitutional courts,* 2025
- Venice Commission, CDL-AD(2019)016-e, *Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI) on Digital Technologies and Elections*, Venice Commission (2019)
- Venice Commission, CDL(2020)037 - *Venice Commission Principles for a Fundamental Rights-Compliant use of Digital Technologies in Electoral Processes*
- Consultative Committee of Convention 108 (T-PD), Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data for the purposes of voter registration and authentication*, 2024
- Council of Europe, *Conclusions of the 19th European Conference of Electoral Management Bodies (EMBs)*, 2022
- Council of Europe, *Disinformation and Electoral Campaigns*, 2019
- OHCHR, *Human Rights and Elections. A Handbook on International Human Rights Standards on Elections*, 2021
- OECD, *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, 2024
- European Commission, *Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065*, 2024
- Carnegie Endowment for International Peace, *Countering Disinformation Effectively: An Evidence-Based Policy Guide*, 2024
- European Partnership for Democracy *The EU's Artificial Intelligence Act and its Impact on Electoral Processes: a Human Rights-Based Approach*, 2024
- International IDEA, *Artificial Intelligence for Electoral Management*, 2024

4.5. Healthcare

164. Healthcare involves the provision of medical services aimed at maintaining or improving physical and mental well-being, including prevention, diagnosis, treatment, and rehabilitation, delivered by professionals like doctors and nurses across settings such as hospitals, clinics, primary care facilities and home care.

Key AI use cases

165. 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,[295] encompassing ancillary applications, such as the automation of routine administrative tasks, but also applications of significant impact on the provision of quality health services and a patient's treatment, that could be regulated as medical devices at national level, such as in radiology imaging.

[295] For an overview of AI applications in healthcare, see *Report on the Application of Artificial Intelligence in Healthcare and its impact on the "Patient-Doctor" Relationship*, Steering Committee for Human Rights in the field of Biomedicine and Health (CDBIO), September 2024, pp. 9-11. See also *Ethics and Governance of Artificial Intelligence for Health*, World Health Organization, 2021, pp. 6-16.

166. Key AI use cases include:

- *Medical diagnostics:* AI systems that can analyse medical images (X-rays, MRIs, CT scans etc.), laboratory testing (genome analysis, slide, imaging) and assess symptoms in order to help identify disease and diagnose health conditions.
- *Predictive analytics*: AI systems used to predict patient outcomes, such as risk of disease and potential complications, by data analysis.
- *Personalised medicine*: AI systems that help tailor treatment plans to individual patients, optimizing drug therapies and medical interventions by analysing genetic information and other health data.
- *Virtual health assistants*: AI-powered chatbots and virtual assistants that provide patient support, including mental health support, by answering questions, scheduling appointments, and offering medication reminders.
- *Remote monitoring and telemedicine*: AI-powered wearable devices and telehealth platforms enabling patient monitoring outside of traditional settings.
- *Robotic surgery*: AI-powered robotic systems enhancing surgical precision and control.
- *Process management*: AI systems used to manage access to treatment, distribute patients within the healthcare system or allocate resources, for example according to urgency or necessity.
- *Medical device development*: AI systems used in the design, testing, and optimisation of medical devices.
- *Mental health support*: AI tools used for digital therapies, early detection of mental health risks through behavioural data (e.g. digital phenotyping), and personalised mental health interventions including AI-powered chatbots simulating therapeutic interactions.

Relevant human rights and principles

167. Under Article 8 ECHR, States are under both a negative obligation not to directly interfere with the health of an individual (unless in a manner justified under the ECHR) and a positive obligation to take measures to safeguard the health of those within their jurisdiction, as required and appropriate in the specific circumstances. Although matters of healthcare policy fall in principle within States' margin of appreciation,[296] positive obligations require States to legislate or implement practical measures to protect individuals' health and lives and ensure they are informed of health risks,[297] establish regulations compelling hospitals to safeguard patients' lives,[298] and uphold high professional standards among healthcare providers,[299] including those in the private sector. The Court has interpreted Article 8 as covering the right to the protection of one's physical, moral and psychological integrity, as well as the right to exercise one's personal autonomy and self-determination in making choices about one's body, including by refusing medical treatment or requesting a particular form of medical treatment.[300] Other Articles through which the Court

[296] *Vavricka and others v. the Czech Republic* [GC], No. 47621/13 and 5 others, 8 April 2021, §§ 274, 285.
[297] *Brincat and others v. Malta*, No. 60908/11 and 4 others,24 July 2014, § 101; *Guerra and others v. Italy,* No. 116/1996/735/932, 19 February1998, §§ 57-60; *Roche v. the United Kingdom* [GC], No. 32555/96, 19 October 2005.
[298] *Calvelli and Ciglio v. Italy* [GC], No. 32967/96, 17 January 2002, § 49; *Mehmet Ulusoy and Others v. Turkey*, No. 54969/09, 25 June 2019, § 90.
[299] *Lopes de Sousa Fernandes v. Portugal* [GC], No. 56080/13, 19 December 2017, §§ 186-190.
[300] *Niemietz v. Germany*, No. 13710/88, 16 December 1992, § 29; *Glass v. the United Kingdom*, No. 61827/00, 9 March 2004, §§ 74-83; *Tysiąc v. Poland*, No. 5410/03, 20 March 2007, § 107; *Pindo Mulla v. Spain* [GC], No. 12345/19, 15 April 2024, § 98; *Pretty v. the United Kingdom*, No. 2346/02, 29 April 2002, § 63; *Taganrog LRO and Others v. Russia*, Nos. 32401/10 and 19 others, 7 November 2019, § 162.

approaches health issues are Article 2 (Right to life),[301] Article 3 (Prohibition of torture)[302] and Article 14 (Prohibition of discrimination).[303] In its case-law concerning health, the Court often refers to Convention 108,[304] the Oviedo Convention,[305] as well as other relevant instruments within the framework of the Council of Europe or beyond.[306]

168. The ESC explicitly guarantees the right to protection of health (Article 11) and the right to social and medical assistance (Article 13). Access to healthcare is a prerequisite for preserving human dignity.[307] States must ensure that healthcare services are accessible, effective, and inclusive by allocating sufficient resources, implementing robust operational procedures, and addressing the specific needs of vulnerable groups.[308] Integrating trustworthy AI systems into healthcare delivery can support states in achieving these aims. Article 11 imposes three key obligations on States, either directly or in collaboration with public or private organisations: to take appropriate measures (i) to eliminate, as far as possible, the causes of ill health, (ii) to provide advisory and educational facilities that promote health and encourage individual responsibility; and (iii) to prevent, as far as possible, epidemic, endemic, and other diseases, as well as accidents. States are further required to protect vulnerable groups,[309] such as the homeless, older persons, persons with disabilities, and those with irregular migration status, ensuring their right to health remains uncompromised, even under restrictive conditions. Additionally, foreigners who are nationals of other Parties lawfully residing or working in a Party's territory are entitled to health protection under the ESC.

Right to Privacy and Data Protection

169. As noted in the section on core human rights issues across public governance sectors, Article 8 ECHR protects health-related personal data,[310] which constitute a key element of private life. Article 10 of the Oviedo Convention states that everyone a) has the right to respect for private life in relation to information about his or her health and b) is entitled to know any information collected about her or his health. Health-related personal data is explicitly considered sensitive under Convention 108 (Article 6) as well as under regional and domestic regulatory frameworks.[311] The Committee of Ministers of the Council of Europe has issued specific guidelines on the protection of health-related data, by its Recommendation CM/Rec(2019)2, which seeks to ensure

[301] *Center of Legal Resources on behalf of Valentin Campeanu v. Romania* [GC], No. 47848/08, 17 July 2014, §§ 145-147; *Oyal v. Turkey*, No. 4864/05, 23 March 2010, § 72
[302] *Paposhvili v. Belgium* [GC], No. 41738/10, 13 December 2016, §§ 183-193; *D. v. the United Kingdom*, No. 30240/96, 2 May 1997, § 54; *Aswat v. the United Kingdom*, No. 17299/12, 16 April 2013, §§ 55-57.
[303] *Kiyutin v. Russia*, No. 2700/10, 10 March 2011, §§56-58, 74
[304] See e.g. *S. and Marper v. the United Kingdom* [GC], 2008, §§ 41 and 103.
[305] *Glass v. the United Kingdom*, 2004, § 58. "Oviedo Convention" refers to the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4 April 1997 (ETS no 164). The Oviedo Convention is complemented by four Additional Protocols. See https://www.coe.int/en/web/human-rights-and-biomedicine/oviedo-convention
[306] See e.g. the reference in *Biriuk v. Lithuania* (No. 23373/03, 25 November 2008, § 21) to Recommendation No. R (89) 14 of the Committee of Ministers of the Council of Europe on the ethical issues of HIV infection in the health care and social settings (1989) or the reference in *Pindo Mulla v. Spain* [GC], No. 15541/20, 17 September 2024, § 77, to the Universal Declaration on Bioethics and Human Rights adopted by UNESCO in 2005.
[307] *International Federation of Human Rights Leagues (FIDH) v. France*, Complaint No. 14/2003, decision on the merits of 3 November 2004, §31.
[308] Statement of Interpretation on the right to protection of health in times of pandemic, 21 April 2020.
[309] *International Commission of Jurists (ICJ) and European Council for Refugees and Exiles (ECRE) v. Greece*, Complaint No. 173/2018, decision on the merits of 26 January 2021, § 218.
[310] *Surikov v. Ukraine*, No. 42788/06, 26 January 2017, §§ 70 and 89.
[311] For instance, see Articles 4 and 9 and Recitals 35 and 53 of the GDPR, with definitions of the terms "health data", "genetic data", "biometric data".

the principles of Convention 108, including its modernised version, are fully applied to the exchange and sharing of health-related data.

170. AI systems in healthcare may rely heavily on sensitive patient data, including medical records and biometric information, for both training, testing and validation and when being used in relation to decision-making and prediction. Data security, confidentiality, and potential misuse, such as breaches or unauthorised sharing are among the concerns.[312] Moreover, individuals may face challenges in exercising control over their data, particularly when it is included in AI training datasets. The disclosure of health data can profoundly impact private and family life, as well as social and employment situations, risking stigma and exclusion. Therefore, domestic laws must provide safeguards to prevent unauthorised sharing or disclosure, ensuring compliance with Article 8 guarantees.[313]

Non-Discrimination and Equitable Access to Health Care

171. As noted in the section on core human rights issues across public governance sectors, the ECHR and the ESC prohibit discrimination.[314] Under Article 3 of the Oviedo Convention, State Parties are required to take appropriate measures with a view to providing, within their jurisdiction, equitable access to health care of appropriate quality.[315]

172. Unwanted biases in the data used to develop AI systems may skew the assessment of health needs and treatments for patients and thereby perpetuate or exacerbate existing biases. It is notable that AI models trained predominantly on data from specific populations may misdiagnose conditions or underestimate illness severity in underrepresented groups such as women and girls, persons belonging to ethnic minorities, indigenous populations, the elderly or persons with disabilities.[316] Examples include prioritisation systems for kidney transplants, where biased historical data skewed outcomes against some patients.[317] Similarly, inadequate representation in training datasets has led to misdiagnoses of skin conditions.[318] In addition, there is concern that access to the benefits offered by AI in healthcare may not be equally available to all. The deployment of such care may be geographically uneven across a given country, or dependent on the financial means of the patients.[319] A lack of accessible design of AI applications may exclude

[312] See also the CDBIO *Report on the role of health professionals and healthcare providers in collecting, generating and enriching* (CDBIO Report), as well as safeguarding health data, pp. 21-23, referring to a 2017 ruling by UK's Information Commissioner's Office (ICO) finding a breach of the applicable data protection law and the right to privacy with respect to a healthcare institution granting to a private company access to over 1 million pseudonymized patient data files in order to test an AI system under development.
[313] *Z. v. Finland*, No. 22009/93, 25 February 1997, § 95
[314] See the Preamble to the 1961 ESC and Part V-Article E of the RESC.
[315] See also Articles 15 §1(b) and 2§2 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) on the right of everyone to enjoy the benefits of scientific progress and its applications, without discrimination of any kind.
[316] See, e.g., CDBIO Report p. 26; see also WHO, Ethics and governance of artificial intelligence for health (2021), pp. 54-57. Further on the underrepresentation and low quality of data of women, as well as gender diverse persons in scientific research, the GEC/CDADI Study, p. 25. Also (p. 26) on the structural discrimination embedded in AI systems with respect to systematically disadvantaged patients with ethnic minority backgrounds. Furthermore, see WHO, *Ageism in artificial intelligence for health* (2022), showing that algorithmic systems used in the healthcare sector are trained on the data of predominantly younger populations, leading to disproportionately lower performance of these systems for older patients, including incorrect diagnosis www.who.int/publications/i/item/9789240040793.
[317] See, e.g., www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients; https://algorithmwatch.org/en/racial-health-bias-switzerland.
[318] See, e.g., www.theguardian.com/society/2021/nov/09/ai-skin-cancer-diagnoses-risk-being-less-accurate-for-dark-skin-study.
[319] CDBIO Report, p. 26. On the discussion on the possibility that the existing digital divide (including with respect to AI) and inequalities (within and between countries, as well as societal groups) will exacerbate the unequal distribution of

older persons or persons with disabilities. States should adopt measures to ensure AI systems are developed and deployed equitably.

Informed Consent, Autonomy and Decision-Making

173. Informed consent and autonomy in decision-making of the patient[320] is guaranteed under Article 8 ECHR[321] and Article 11 ESC.[322] Article 5 of the Oviedo Convention requires free and informed consent for health interventions, with prior information on purpose, risks, and consequences. Consent can be withdrawn at any time. Special consideration is given to emergency situations, and to individuals unable to consent.[323]

174. Individuals must be able freely to give or refuse their consent to any intervention, comprising all medical acts including those performed for the purpose of preventive care, diagnosis, treatment, rehabilitation or research. Their consent is considered to be free and informed when it is given on the basis of objective and full information from the responsible health care professional which includes adequately answering to requests for additional information. The provision of information should be detailed enough for the patient to understand the scope, areas and stages of the use of AI tools. The "black box" nature of many AI systems which render probabilistic results makes it difficult to sufficiently understand and weigh up the necessity or usefulness of the intervention. Adequate transparency and oversight requirements for AI systems and their developers as well as education and training of doctors using them might mitigate this. Concerns about the "de-skilling" of health professionals and the de-personalisation of the patient-doctor relationship require attention. [324]

Further reading

- Recommendation CM/Rec (2019)2 of the Committee of Ministers to Member States on the protection of health-related data
- Recommendation 2185 (2020) of the Parliamentary Assembly of the Council of Europe, *Artificial intelligence in healthcare: medical, legal and ethical challenges ahead*
- Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), *Report on the Application of Artificial Intelligence in Healthcare and its impact on the "Patient-Doctor" Relationship*, 2024
- Brent Mittelstadt, Senior Research Fellow and Director of Research at the Oxford Internet Institute, University of Oxford, United Kingdom, Report by consultant expert on the impact of artificial intelligence on the doctor-patient relationship

healthcare and problems of effective access to healthcare, see PACE Recommendation 2185 (2020), *Artificial intelligence in healthcare: medical, legal and ethical challenges ahead*. An additional concern could be linked to the use of AI for resource allocation and case prioritisation.

[320] Autonomy goes beyond informed consent and engenders a more active role for the patient in shared decision-making, encompassing, for example, the choice to take preventive measures, to ask for a second opinion or to introduce his or her own values, preferences and perspectives in patient-doctor communications, see CDBIO Report p. 13.

[321] *Trocellier v. France* (dec.), No. 75725/01, 13 April 2023, § 4; *Mayboroda v. Ukraine*, No. 14709/07, § 52.

[322] *Transgender Europe and ILGA Europe v. Czech Republic*, Complaint No. 117/2015, 15 May 2018, §81.

[323] Articles 6-8. See also the Explanatory Report to the Oviedo Convention, paragraphs 35-36.

[324] In accordance with Article 4 of the Oviedo Convention, any intervention in the health field must be carried out in accordance with relevant professional obligations and standards. This is interpreted as an obligation of health professionals to pay careful attention to the special needs of each patient. See paragraphs 32 and 33 of the Explanatory Report to the Oviedo Convention.

- Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), *Strategic Action Plan on Human Rights and Technologies in Biomedicine (2020-2025)*, 2019
- Ivana Bartoletti and Raphaële Xenidis, Council of Europe, *Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination*, 2023
- World Health Organisation, *Ethics and governance of artificial intelligence for health*, 2021
- World Health Organisation, *Ageism in artificial intelligence for health*, 2022
- World Health Organisation, *Regulatory considerations on artificial intelligence for health*, 2023
- World Health Organisation, *Ethics and governance of artificial intelligence for health, Guidance on large multi-modal models*, 2024
- UN Environment Progralle, *Navigating New Horizons, A global foresight report on planetary health and human well-being*, 2024
- Study on Artificial Intelligence in mental healthcare, Mental Health Europe, 2025
- OECD, *AI in Health: Huge Potential, Huge Risks*, 2024

4.6. Social services and welfare

175. Social services involve a broad range of programs and services intended to ensure a minimum standard of living and designed to promote human and societal well-being. In addition to fundamental public services such as health care and education, addressed specifically in parts 4.5 and 4.7. respectively of this Handbook, social services and welfare systems provide both financial and non-financial benefits. These include social security programs that offer financial support for older persons, persons with disabilities and survivors; sickness and accident benefits; unemployment benefits; maternity and paternity benefits, family benefits/allowances, housing assistance (subsidies or social housing), and support for the homeless or those at risk of homelessness; guaranteed minimum income or in-kind benefits, such as food assistance for low-income families; child and family services including child care subsidies, programs and tools aimed at combatting domestic violence, and child welfare services; old age and disability support.

Key AI use cases

176. AI is increasingly integrated into social services, ranging from automating routine tasks such as notetaking and case management to more complex applications with significant impact. Key AI-driven functions include:

- *Predictive analytics:* AI systems that can analyse large datasets using algorithmic processes, including machine learning, to identify individuals or groups most at risk of requiring social services. This enables agencies to proactively allocate support and resources, for example, identifying children at risk who may need additional assistance.
- *Resource allocation:* AI-driven models optimize the distribution of usually limited resources, ensuring more efficient and equitable service delivery.
- *Screening and error/fraud detection*: AI systems used to assist in screening applicants, verifying applicant information, flagging inconsistencies, and identifying patterns indicative of error, fraud or misuse of welfare services, enhancing accountability and efficiency.
- *AI-driven chatbots and virtual assistants*: these systems handle routine inquiries, can improve accessibility for people with disabilities through speech recognition or automated transcription, and monitor individuals' physical and mental health, issuing alerts to ensure timely interventions.

- *Overview and evaluation:* AI analyses social service outcomes to assess effectiveness, providing data-driven insights that help agencies refine policies and improve service delivery over time.

Relevant human rights and principles

177. The provision of social services may directly interfere with an individual's enjoyment of his or her rights, such as the right to private and family life within the meaning of Article 8 ECHR,[325] the right to liberty within the meaning of Article 5,[326] or the right to property within the meaning of Article 1 of Protocol No.1.[327] In addition, effective social services contribute to the fulfilment of the State's positive obligations for the prevention of ill-treatment administered by private persons (Article 3).[328]

178. States have a margin of appreciation in spheres involving the application of social or economic policies.[329] The Court will also generally respect domestic policy choices unless they are "manifestly without reasonable foundation".[330] This is particularly so in the context of the allocation of limited State resources.[331] The Court has thus found it legitimate for States to put in place criteria according to which a benefit can be allocated, when there is insufficient supply available to satisfy demand, so long as such criteria are not arbitrary or discriminatory.[332] This means that where a State decides to provide such benefits, it must do so in a non-discriminatory manner. The State's margin of appreciation is considerably reduced where the distinction in treatment is based on an inherent or immutable personal characteristic such as race, sex, nationality or disability, and "very weighty reasons" would be required to justify the difference of treatment at issue.[333]

---

[325] For instance, with respect to decisions on the removal of children, placement and adoption, determination of custody and visiting rights, see *B. v. the United Kingdom,* 8 July 1987, No. 9840/82, §§ 60-65; *Saviny v. Ukraine,* 18 December 2008, 39948/06, §§57-42; *A.K. and L. v. Croatia*, 8 January 2013, No. 37956/11, §§ 58-60. Also see for obligations of national authorities to facilitate family visits and, in exceptional cases, to secure shelter for particularly individuals in a situation of vulnerability *A and Others v. Italy*, 7 December 2003, No.17791/22, §§ 93-104.

[326] For instance, with respect to the compulsory confinement of persons of "unsound mind". See, among others, *Ilnseher v. Germany* [GC]*,* 4 December 2018, No.10211/12 and 27505/14, §§ 126-134.

[327] For a comprehensive synopsis of the Court's case-law relating to social security/welfare benefits see *Béláné Nagy v. Hungary* [GC], No. 53080/13, 13 December 2016, §§ 80-89; *Yavaş and Others v. Turkey*, No. 36366/06, 5 March 2019, 36366/06, §§ 39-43.

[328] See, among others, *Z. and Others v. the United Kingdom,* No. 29392/95, 10 May 2001, §121, concerning the failure of the respondent State's social services to take adequate protective measures with regard to a child abuse case; as well, *V.C. v. Italy,* 1 February 2018, No. 54227/14, §89. Also, with respect to the failure to protect victims of domestic violence, see *Opuz v. Turkey,* No. 33401/02, 9 June 2009, §159; *Talpis v. Italy,* No. 41237/14, 2 March 2017, § 141, also in conjunction with Article 14 and the State's failure to guarantee the right of women to equal protection before the law.

[329] For instance, regarding housing, see, among others, *Hudorovič and Others v. Slovenia*, 10 March 2020, Nos 24816/14 and 25140/14 and *European Roma and Travellers Forum (ERTF) v. France*, Complaint No. 64/2011, 24 January 2012, §95; regarding old-age pensions, *Fábián v. Hungary*, No. 78117/13, 5 September 2017, § 67; regarding survivors' pensions, *Muñoz Díaz v. Spain*, No. 49151/07, 8 December 2009, §§ 48-49, etc; regarding employment policies, see, *General Federation of employees of the national electric power corporation (GENOP-DEI) / Confederation of Greek Civil Servants Trade Unions (ADEDY) v. Greece*, Complaint No. 66/2011, 23 May 2012, §20.

[330] *Stec and Others v. the United Kingdom* [GC], 12 April 2006, No. 65731/01 and 65900/01, § 52.

[331] *Šaltinytė v. Lithuania*, No. 32934/19, 26 October 2021, §§ 64 and 77.

[332] *Bah v. the United Kingdom*, No. 56328/07, 27 December 2011, § 52.

[333] *Savickis and Others v. Latvia* [GC], No. 49270/11, 9 June 2022, § 183; *J.D. and A. v. the United Kingdom*, No.32949/17, No.34614/17, §§ 88-89, 97 and 104, 24 October 2019; *Ribać v. Slovenia*, No.57101/10, 5 March 2018, § 53.

179. Under the ESC, States Parties have the obligation to ensure non-discriminatory access to social security,[334] social and medical assistance,[335] and social welfare services.[336] It requires that a social security system guarantees effective access to benefits provided under each branch of the respective system.[337] Equal treatment must be ensured for nationals of other States Parties lawfully resident or working regularly within the territory of the State Party concerned, as well as refugees and stateless persons.[338]

Right to Privacy and Data Protection

180. The use of AI in social services involves processing sensitive personal data, raising serious privacy concerns under Article 8 ECHR. The aggregation of sensitive data, such as health records, financial and employment history, and other personal details, that enables the State to acquire a detailed profile of the most intimate aspects of citizens' lives, may result in particularly invasive interference with private life.[339] For example, concerns related to compliance with Article 8 ECHR were raised in the "SyRi" case, where the Hague District Court found that an algorithm used for the purpose of identifying potential social welfare fraud (the "Systeem Risico Indicatie" or "SyRi") and the relevant legislation did not meet the requirements for necessity and proportionality as required by Article 8(2) ECHR.[340]

181. An additional risk is the misuse of personal data collected in social services, including unauthorised surveillance, profiling without consent, or accidental breaches. Concerns also arise from businesses involvement in developing or maintaining AI systems or outsourcing social services to private companies. Considering that AI systems store vast amounts of sensitive data, particular importance should also be placed on data security, including when a particular AI system is developed and maintained by third-party (private) vendors.

Non-discrimination and equality

182. The use of AI in social services can perpetuate discrimination (including indirect and intersectional) due to biases embedded in societal data, such as racial, gender, or socioeconomic biases.[341] This may lead to unfair denial of services or benefits, disproportionately affecting marginalised groups and undermining equal access to these services. Predictive analytics, error or fraud detection and resource allocation systems are more likely to be affected by bias, as they rely on historical data and are prone to exacerbating structural discrimination and stereotypes. For instance, a fraud detector system trained on data that disproportionately reflects the experiences of certain groups is likely to develop risk profiles and create links based on bias, such as lower socio-economic status or an immigration background. This may lead to biased recommendations

---

[334] ESC, Article 12; see also Digest of Case Law of the European Committee of Social Rights, December 2022, p. 119 ff.
[335] ESC, Article 13.
[336] ESC, Article 14.
[337] Digest of Case Law of the European Committee of Social Rights, December 2022, p. 120.
[338] ESC Article 12(4); Paragraph 1 of the Appendix of the ESC.
[339] *Szabó and Vissy v. Hungary*, No. 37138/146, 12 January 2016, § 70.
[340] The Hague District Court, *NCJM* et al. *and FNV v The State of the Netherlands*, 6 March 2020, available in English at uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 (ECLI:NL:RBDHA:2020:865). The system concerned was the "Systeem Risico Indicatie" or "SyRi". See also the *amicus curiae* brief submitted by the United Nations Special Rapporteur on Extreme Poverty and Human Rights stressing in particular the discriminatory and stigmatizing effect of SyRi".
https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf
[341] See *The Netherlands – Opinion on the Legal Protection of Citizens*, CDL-AD(2021)031, Venice Commission, 2021, §§ 96-98 https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2021)031-e

and eventually the violation of the right to not be discriminated against of not just individuals but whole populations perceived by the system as homogeneous. Safeguards are required, including human oversight, ensuring the critical evaluation of AI outputs and thus neutralising the risk of discriminatory effects.[342]

183. Where discrimination is alleged, state authorities should take all reasonable measures to determine whether the outcome was discriminatory. This should include an effective and independent investigation.[343]

Transparency and Accountability

184. As already observed, AI decision-making processes can be opaque, making it difficult to understand how and why a decision was made. This lack of transparency can undermine accountability in the delivery of social services, especially when individuals are denied benefits or services based on AI decisions. If a person is disadvantaged by an AI decision (e.g., being wrongly denied welfare benefits), it may be challenging for them to appeal or challenge the decision due to the "black-box" nature of many AI systems, whether it is intentional (i.e., for intellectual property considerations) or intrinsic (i.e., too complicated for anyone without particularly advanced digital skills).

185. The lack of transparency and accountability around the use of AI systems can lead to depriving the subjects of AI decision-making from an explanation or the opportunity to appeal against decisions that in some cases may be of vital importance to them and thus interferes with their right to an effective remedy. In cases where the events in issue lie wholly, or in large part, within the exclusive knowledge of the authorities, as would arguably be the case when AI systems are involved, or when it would be extremely difficult in practice for the applicant to prove discrimination, the Court/ESCR has shifted the burden of proof on the authorities.[344]

Accessibility and Quality of Care

186. Persons in a situation of vulnerability, such as older persons, people with disabilities, or those with limited digital literacy or access to modern technology, may be ill-equipped to interact with AI systems. These groups may face difficulties in accessing AI-based services, from simple application platforms online to chatbots and virtual assistants. This could result in exclusion from social services and consequently exacerbate existing inequalities.

187. On the other end of social services delivery, reliance on AI systems raises quality-related questions. Such systems are, in most cases, designed to support decisions by human professionals and should not replace human judgment. Nevertheless, as evident from domestic caselaw, there may be cases where professionals lack the time, the resources or are simply prone to automation bias and reluctant to use their professional expertise to reach a different decision

---

[342] It must however be noted that human involvement is not enough by itself in neutralising discrimination risks; in the Dutch childcare benefits scandal, for example, civil servants were responsible for manually reviewing the highest risk score applications. Without being given any information as to why the system had given a particular application a high-risk score to a specific application, .civil servants have been observed to be prone to apply generalisations to the behaviour of individuals of the same race or ethnicity perceiving them stereotypically as fraudulent or deviant.
[343] *Basu v. Germany*, No. 215/19, 18 October 2022, § 38.
[344] *Salman v. Turkey* [GC], No. 21986/93, 27 June 2000, § 100; *Anguelova v. Bulgaria*, no 38361/97, 13 June 2002, § 111; *Cînţa v. Romania*, No. 3891/19, 18 February 2020, 3891/19, §79; *Mental Disability Advocacy Centre (MDAC) v. Bulgaria*, Complaint No. 41/2007, decision on the merits of 3 June 2008, § 52.

than the one recommended by the system. AI systems are however not error-proof,[345] and errors in welfare can be fatal for some of the most vulnerable members of the society. In addition, there is concern that "digital-by-design" social services and over-relying on AI would lead to the erosion of social workers' skills, thus undermining the quality of service, especially in complex, sensitive cases.

Further reading

- Recommendation CM/Rec(2011)12 of the Committee of Ministers to member states on children's rights and social services friendly to children and families
- Declaration by the Committee of Ministers on the risk of computer-assisted or artificial intelligence enabled decision-making in the field of the social safety net, 2021
- Council of Europe, *Children rights and social services, Report on the implementation of the Council of Europe Recommendation on children's rights and social services friendly to children and families*, 2016
- Ivana Bartoletti and Raphaële Xenidis, Council of Europe, *Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination,* GEC/CDADI Study, 2023
- *The Netherlands – Opinion on the legal protection of citizens,* CDL-AD(2021)031, 2021
- Council of Europe, *Social Security as a human right,* Human Rights Files No. 23, 2007
- OECD Artificial Intelligence Papers, *AI and the future of social protection in OECD countries,* No. 42, 2025
- Special Rapporteur on extreme poverty and human rights*, Report on the privatization of public services*, A/73/396, 26 September 2018
- Special Rapporteur on extreme poverty and human rights*, Report on the "digital welfare state",* A/74/493, 11 October 2019
- Amnesty International, *Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal*, 2021

4.7. Education

188. This sector includes activities related to teaching, access to learning, student assessments, vocational guidance and training, life-long learning, and educational outcomes.

Key AI use cases[346]

[345] For instance, in the United Kingdom, the *Johnson and others v SSWP* judgment (EWCA Civ 778, Judgement, Secretary of State for Work and Pensions v Johnson *et al.*, *Case Nos: CO/1643/2018 CO/1552/2018*, https://www.judiciary.uk/wp-content/uploads/2019/01/johnson-and-others-judgment-final.pdf) raised important issues arising from the implementation of an AI system making benefit and welfare decisions for the then newly introduced system of Universal Credit (a single welfare payment comprising a basing personal amount also reflecting childcare, housing, and other prescribed needs). The claimants argued that the automated assessment system used to calculate the amount of universal credit payable to each claimant was unlawful and could create income insecurity, whereas the State acknowledged that the method was "unfortunate" and "arbitrary" but redesigning the system "from scratch" to accommodate adjustments would be too onerous. This defence was rejected and the challenge succeeded, on the ground that the effects, in these instances, were judged to run counter to the policy and objectives of the UC's underlying regulations and thus "irrational".

[346] Council of Europe, Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022), pp.15-23; see also UNESCO, Artificial Intelligence and Education: Guidance for Policy Makers (2021) , pp. 13-19.

189. In education, AI systems are used to enhance learning, support administrative functions, and assist teachers through AI-driven analytics and automation. Use cases include:

- *Learner support*: AI-driven tutoring systems provide personalised instruction, adaptive learning tools adjust to individual progress, and chatbots offer 24/7 student assistance, including in life-long learning.
- *Assessment and feedback*: AI automates writing evaluation, generates real-time performance analytics, utilizes open learner models to help students track their progress and helps to detect plagiarism in student work by scanning databases for similarities to existing content. AI based proctoring assesses a test-taking individual's behaviour, environment and movement.
- *Educational administration*: AI optimises admissions processes, automates timetabling, and manages learning systems to streamline institutional operations.
- *Teacher support*: AI curates learning materials from online sources and create adaptive learning content and dynamic textbooks, provides real-time classroom analytics through dashboards to analyze data from students' performance, attendance, participation, and engagement, and assists with course planning and time management.
- *Learning analytics and resource allocation*: AI analyses student engagement, predicts learning outcomes, and informs resource distribution to improve educational efficiency.
- *Speech recognition and language processing***:** AI-based speech recognition and language processing tools can assist students with disabilities, by converting speech to text or providing real-time translation and transcription.

Relevant human rights and principles

190. Article 2 of Protocol No. 1 to the ECHR guarantees a right to education, which is indispensable to the furtherance of human rights in a democratic society.[347] It applies to mandatory pre-school education,[348] primary and secondary education, and higher education institutions set up by the State.[349] The right to education may give rise to implicitly accepted limitations, bearing in mind that the right to access to education "by its very nature calls for regulation by the State."[350] Consequently, the domestic authorities enjoy a certain margin of appreciation, but restrictions must not impair the essence of the right or render it ineffective; they must be foreseeable for those concerned and pursue a legitimate aim.[351] While there is no exhaustive list of "legitimate aims" that may be pursued when limiting enjoyment of the right to education,[352] any limitation must maintain a proportionate balance between the means employed and the aim sought to be achieved.[353] The State has responsibilities concerning both public and private schools.[354]

191. Article 2 of Protocol No. 1 must be interpreted in harmony with other rules of international law of which the ECHR forms part, including the UNCRC, the International Covenant on Economic, Social and Cultural Rights, the International Convention on the Elimination of All Forms of Racial

---

[347] *Timishev v. Russia,* Nos 55762/2000 and 55974/00, 13 December 2005, § 64
[348] *Djeri and Others v. Latvia*, Nos. 50942/20 & 2022/21, 18 July 2024, §§ 118 & 122.
[349] *Leyla Şahin v. Turkey* [GC], No. 44774/98, 10 November 2005, §§ 137 & 141.
[350] *Case "Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium" (Merits)*, Nos. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63, 2126/64,23 July 1968, § 5 of "The Law" part I.A (the "Belgian linguistics" case).
[351] *Leyla Şahin v. Turkey* [GC], No. 44774/98, 10 November 2005, § 154.
[352] Unlike ECHR Articles 8,9,10 and 11.
[353] *Leyla Şahin v. Turkey* [GC], No. 44774/98, 10 November 2005, § 154 et seq.
[354] *Kjeldsen, Busk Madsen and Pedersen v. Denmark*, Nos. 5095/71, 5920/72, and 5926/72, 7 December 1976.; see also *O'Keefe v. Ireland [GC],* No 35810/09, 28 January 2014, §§ 144-152

Discrimination, the UNESCO Convention against Discrimination in Education[355], the UN Convention on the Rights of Persons with Disabilities[356] and the ESC.[357] States should respect and fulfil the obligations and commitments within existing Council of Europe and United Nations standards on the rights of the child.

192. As to the (Revised) ESC, States Parties are, under Part II, Article 17§2, required – either directly or in partnership with public and private organisations – to implement measures that provide a free primary and secondary education for all individuals under 18 (unless majority is attained earlier under the law applicable the child).[358] Article 17 requires States Parties to establish and maintain an education system that is both accessible and effective.[359] While private actors may contribute, their involvement must not detract from the quality or accessibility of public education.[360] States Parties must ensure effective vocational training by promoting technical and vocational programmes for all.[361] Under Article 17, equal educational opportunities must be guaranteed for all children, especially for groups at risk.[362]

Right to Privacy and Data Protection

193. The use of AI systems for educational purposes may lead to the processing of personal data of, for example, children, university students, persons with disabilities, persons in vocational training, lifelong learners, educators, or parents by a variety of actors, including national governments, public and private educational establishments, business enterprises such as providers of products or services, software developers and individuals such as teachers, legal guardians and peers. Processing a child's personal data in educational settings has particular complexity due to the non-consensual setting, which may affect the freely given nature of consent, also considering that, as a general rule, children cannot enter into contracts.[363] The use of AI systems in the educational context therefore attracts consideration under Article 8 ECHR.

194. CM/Rec(2018)7, which provides "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", acknowledges that personal data can be processed to the benefit of children, but highlights that States should take measures to ensure that children's personal data is processed fairly, lawfully, accurately and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents, carer or legal representative, or in accordance with another legitimate basis laid down by law. The data minimisation principle should be respected, meaning that the personal data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed.[364]

---

[355] *Catan and Others v. the Republic of Moldova and Russia* [GC], Nos 43370/04, 8252/05 and 18454/06), 19 October 2012, § 136
[356] *Çam v. Turkey*, No. 51500/08, 23 February 2016, § 53
[357] See *Ponomaryovi v. Bulgaria*, No. 5335/05, 21 June 2011, §§ 34-35, referring to the Revised European Social Charter.
[358] Without prejudice to other specific provisions set out in the ESC, notably Article 7. See Appendix to the European Social Charter (Revised) – European Treaty Series – No. 163.
[359] *Conclusions 2003, Bulgaria*, European Committee on Social Rights.
[360] *Conclusions 2019, Statement of Interpretation on Article 17§2 - Private sector involvement in education*, European Committee on Social Rights.
[361] *Conclusions I (1969), Statement of Interpretation on Article 10§1*, European Committee on Social Rights.
[362] *Mental Disability Advocacy Center (MDAC) v. Bulgaria*, Complaint No. 41/2007, decision on the merits of 3 June 2008, §34, citing Conclusions 2003, Bulgaria.
[363] Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022), Council of Europe, p. 71.
[364] Guidelines on children's data protection in an education setting, Consultative Committee of Convention 108 (T-PD)

195. States should ensure that the processing of special categories of data which are considered sensitive, should in all instances only be allowed where appropriate safeguards are enshrined in law. Profiling of children, which is any form of automated processing of personal data which consists of applying a "profile" to a child, particularly to take decisions concerning the child or to analyse or predict their personal preferences, behaviour and attitudes, should be prohibited by law. In exceptional circumstances, States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law. Profiling must also be excluded with respect to young people and adults in educational contexts. AI system-based educational tools, such as real-time classroom analytics and student engagement tracking or proctoring AI that monitors students through facial recognition and behavioural tracking may interfere with the right to privacy. This concern extends not only to children but also to adult students and to educational staff subject to monitoring or performance assessment through similar technologies. Individuals should not be subjected to arbitrary or unlawful interference with their privacy. Any interference should be in accordance with the law, pursue a legitimate aim, be necessary in a democratic society and be proportionate to the legitimate aim pursued. Surveillance or interception measures may in particular heighten the risk of interference with the right to privacy and should be subject to effective, independent and impartial oversight.[365]

Non-discrimination and equality

196. The right to education under Article 2 of Protocol No. 1 to the ECHR, taken in conjunction with Article 14 ECHR, require that States address risks related to non-discrimination and equality for all individuals in educational contexts.[366] In the context of AI systems, it entails ensuring that AI systems do not reinforce biases which may lead to discriminatory outcomes or create barriers to access to education, or inequalities in the standard and quality of education. Children, in particular, due to their stage of development, have specific needs and rights that distinguish them from adults. As such, there is a need for child-focused approach in the procurement and use of educational technology, including AI systems.[367] In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.[368]

197. Given the increasing importance of new technologies, a number of Council of Europe documents have been adopted in this area, which invite states to ensure that children have access to the digital environment in a way that is non-discriminatory and inclusive and takes into account children's developing capacities and the particular circumstances of children in vulnerable situations.[369] This should apply also in situations where AI systems are involved. Whereas efforts should be undertaken to respect, protect and fulfil the rights of each and every child in an education

[365] Committee of Ministers Recommendation CM/Rec(2018)7 on guidelines to respect, protect and fulfil the rights of the child in the digital environment.
[366] Several international treaties prohibit discrimination in education, including the 1960 UNESCO Convention against Discrimination in Education, the 1966 International Covenant on Economic, Social and Cultural Rights (article 13), the 1989 UN Convention on the Rights of the Child (article 28) and the Convention on the Rights of Persons with Disabilities (article 24).
[367] Preparatory study for the development of a legal instrument on regulating the use of artificial intelligence systems in education, Revised draft (March 2024), Digital Transformation Unit of the Education Department, Council of Europe.
[368] United Nations Convention on the Rights of the Child (1989), Article 3. On the "best interests of the child", see *Neulinger and Shuruk* [GC], No. 41615/07, 6 July 2010, §§ 49-56. The Court also places first "the child's best interests", which may override, depending on their nature and seriousness, those of the parents (ibid, §134).
[369] Committee of Ministers Recommendation CM/Rec(2018)7 on guidelines to respect, protect and fulfil the rights of the child in the digital environment, 4 July 2018.

setting, targeted measures may be needed to address specific needs, recognising that AI systems have the potential both to increase children's vulnerability and to empower, protect and support them.[370]

198. In the context of Article 14 ECHR, positive obligations of States could include measures of 'reasonable accommodation' to correct "factual inequalities".[371] Positive action, or temporary special measures, may involve measures to prevent or compensate for disadvantage suffered by groups exposed to discrimination and intolerance and to facilitate their full participation in all fields of life.[372] Member States should therefore ensure that education institutions use AI systems in a way that is inclusive.[373] States should also make efforts to enhance the use of information and communication technology by closing the gender digital divide and to promote the equality of opportunities and outcomes for all children.[374] In addition, systems such as facial recognition, used as part of a proctoring AI system designed to monitor student behaviour during online exams, can exhibit biases and lead to intersectional discrimination, including on grounds of race and gender.[375] Under the ECHR, any difference in treatment must pursue a legitimate aim and be proportionate.[376] Thus, particular attention should be given to the use of AI systems in selection and exam procedures, in the interest of avoiding discriminatory outcomes.

199. In addition, limited access to AI systems and tools can prevent individuals or groups from experiencing their benefits and advantages, resulting in disadvantages in various sectors including education. AI literacy, which might be considered an extension or specialisation of digital literacy, should be included in the basic education curriculum from the earliest years, taking into account children's developing capacities.[377] This includes technical competencies, content creation skills, and critical understanding of online risks and opportunities. Efforts should focus on schools, child-focused organisations, and parents or guardians, ensuring a safe and inclusive digital environment. Digital education policies should not disadvantage children who lack resources at home or live in institutions. Special support should be provided to children with limited or no digital access, including those from socio-economically disadvantaged backgrounds and children with disabilities. States should also work to bridge the digital divide and the gender gap in technology, ensuring equal opportunities for all children, regardless of their background, and with a special focus on girls, in accessing and benefiting from digital tools, including AI systems.[378]

---

[370] Council of Europe Guidelines on Children's Data Protection in an Education Setting (2020), Consultative Committee of Convention 108 (T-PD), T-PD(2019)06BISrev5, para 5.4.
[371] *Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol 12*, European Court of Human Rights, p. 14.
[372] See also ECRI General Policy Recommendation No. 2 revised on Equality Bodies to combat racism and intolerance at national level, European Commission against Racism and Intolerance (ECRI), paragraph 60, and General Policy Recommendation No. 7 revised on National legislation to combat racism and racial discrimination, ECRI, paragraph 5.
[373] Committee of Ministers Recommendation CM/Rec(2019)1 on preventing and combating sexism, in particular II.G. 'Education institutions'.
[374] Committee of Ministers CM/Rec(2018)7 on guidelines to respect, protect and fulfil the rights of the child in the digital environment, 4 July 2018, para. 46
[375] GEC/CDADI Study (2023), p. 24.
[376] For example, changes to a university access system that led to differential treatment amounted to a violation of Article 14, in conjunction with Article 2 of Protocol No. 1, despite being intended to rapidly improve the quality of higher education. The unforeseeable application of the new system, coupled with the absence of corrective measures, rendered its implementation disproportionate to that aim – see *Altınay v. Turkey*, No. 37222/04, 9 July 2013, § 60.
[377] Recommendation CM/Rec(2019)10 on developing and promoting digital citizenship education, 21 November 2019; Recommendation CM/Rec(2016)2 on the Internet of citizens, 10 February 2016.
[378] Recommendation CM/Rec(2018)7 on guidelines to respect, protect and fulfil the rights of the child in the digital environment, 4 July 2018, §§ 41-46.

Transparency and Accountability

200. The lack of transparency, explainability and interpretability in AI systems ("black box problem") presents risks in the context of education. If an AI system makes recommendations on a child's learning pathway or provides recommendations, which may have long-term consequences for the child's development, then teachers and parents must be able to understand the reasoning behind its decisions, including the parameters used, and have the ability to evaluate and override them if necessary. Likewise, AI systems used in admissions or examinations could have significant implications for rights holders' educational opportunities and future prospects. The opacity of AI can also make it difficult to provide genuinely informed consent or to contest its decisions and outcomes.[379] Consent must unambiguously be freely given and able to be refused without detriment.[380] Sufficient levels of transparency should be ensured. The same apply with respect to adult learners.

201. Member States should also ensure the effective implementation of their obligations under Article 13 ECHR to fulfil the right of children and adult learners to an effective remedy when their human rights and fundamental freedoms have been infringed using AI systems in the educational context.

202. In particular for children, this entails the provision of available, known, accessible, affordable, and child-friendly avenues through which children, as well as their parents or legal representatives, may submit complaints and seek remedies. Effective remedies can include, depending on the violation in question, inquiry, explanation, reply, correction, proceedings, immediate removal of unlawful content, apology, reinstatement, reconnection and compensation.[381] States should also ensure that in all cases, access to courts or judicial review of administrative remedies and other procedures are available, in line with the principles set out in the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice (2010).

Business and Human Rights

203. The private sector's role in education is expanding, whether through private schools or the procurement of AI-driven teaching and school management systems from private business enterprises for use in public schools. States should ensure that business enterprises and other key partners meet their human rights responsibilities and are held accountable in case of abuses. Business enterprises have a responsibility to respect human rights, including the rights of the child, as affirmed in the UN Guiding Principles on Business and Human Rights and Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business.[382] Under the ECHR, States cannot absolve themselves from responsibility by delegating their obligations to private bodies or individuals. This includes provision of education by private schools and their staff, whose acts may engage the responsibility of the State.[383]

204. Committee of Ministers Recommendation CM/Rec(2018)7 recommends that States should require business enterprises and other relevant stakeholders to meet their responsibility to respect

---

[379] Ibid., p. 52.
[380] Guidelines on Children's Data Protection in an Education Setting (2020), Council of Europe Committee on Convention 108, T-PD(2019)06BISrev5.
[381] CM/Rec(2018)7, § 67.
[382] See section VI.
[383] *Costello-Roberts v. the United Kingdom*, No. 13134/87, 25 March 1993, § 27.

the rights of the child in the digital environment and encourage them to support and promote these rights. States should promote and provide incentives to business enterprises to implement safety by design, privacy by design and privacy by default as guiding principles for products and services' features and functionalities addressed to or used by children.

205. States should take appropriate steps to protect children against human rights abuses within the digital environment by business enterprises and to ensure that children have access to an effective remedy. This includes implementing policies and measures to encourage business enterprises to establish their own remedial and grievance mechanisms, in line with the effectiveness criteria set out in the UNGPs, while ensuring that these mechanisms do not impede the child's access to the State-based judicial or non-judicial mechanisms. States should also encourage business enterprises to provide information that is accessible, age-appropriate, and available in the language of the child about how to introduce complaints and seek redress through remedial and grievance mechanisms. Additionally, business enterprises should be required to make available, on their platform or within their service, easily accessible ways for any person, and in particular children, to report any material or activity which causes them concern, ensuring that reports received are dealt with efficiently and within reasonable timescales.[384] There should be accessible and effective ways to report biases, errors, or concerns also about AI-driven educational systems that could impact rights holders.

Further reading:

- European Court of Human Rights, *Guide on Article 2 of Protocol No. 1 - Right to education*
- Council of Europe, *Regulating the use of Artificial Intelligence systems in education - Preparatory study on the development of a legal instrument*, 2024
- Council of Europe, *The state of artificial intelligence and education across Europe – Results of a survey of Council of Europe member states*, 2024
- Council of Europe, *1st Working Conference "Artificial Intelligence and education: A critical view through the lens of human rights, democracy and the rule of law" - Conference highlights*, 2022
- Council of Europe, *Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law*, 2022
- Council of Europe, *2nd Working Conference "Artificial Intelligence and education: Regulating the use of AI in education" - Conference Report*, 2024
- The Alan Turing Institute (approved by the Council of Europe Steering Committee for the Rights of the Child), *Mapping Study on the Rights of the Child and Artificial Intelligence – Legal Frameworks that Address AI in the Context of Children's Rights*, 2024
- Ilkka Tuomi, *Regulating artificial intelligence in the education domain: a general approach*, 2024
- Beth Havinga, *Towards a European review framework for AI EdTech systems*, 2024
- UNESCO, *Beijing Consensus on Artificial Intelligence and Education*, 2019
- UNESCO, *Artificial Intelligence and Education: Guidance for Policy Makers*, 2021
- UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*,
- OECD, Recommendation of the Council on Children in the Digital Environment

[384] CM/Rec(2018)7, § 71.

4.8. Labour and Employment

206. This sector includes activities related to employment, human resources and labour management, including but not limited to issues such as recruitment, access to employment, performance management and worker policies.

Key AI use cases

207. In the workplace, AI systems are used to automate or assist human resources decisions on candidate recruitment and evaluation, automate tasks traditionally performed by workers and to support managerial functions through AI-driven analytics and algorithms — commonly known as "algorithmic management". These include:

- *Recruitment and hiring*: AI is used for the creation of optimised job description and their dissemination through social networks and job platforms and for matching between jobs and job seekers, automates CV screening, candidate scoring, and predictive assessments, as well as conducting initial interviews via chatbots or automated video tools.
- *Task automation and productivity*: AI systems used by workers to automate routine tasks such as data entry or data search, and non-routine tasks, such as creating text, pictures or videos.
- *Algorithmic management*: AI optimises scheduling, monitors productivity, and enhances workflow automation; AI systems used to track and analyse employee performance, using data to identify strengths, weaknesses, and potential areas for improvement.
- *Employee well-being*: AI-powered tools analyse workplace sentiment, employee satisfaction and commitment, detect burnout risks, and personalise employee support programs.

Relevant human rights and principles

208. The ECHR has been interpreted, through the right to respect for private life (Article 8 ECHR), non-discrimination (Article 14 and Protocol No. 12 ECHR), freedom of expression (Article 10 ECHR) and freedom of association (Article 11 ECHR), to encompass certain labour and employment related rights such as the right to collective bargaining[385] or the right to strike[386] and to recognise the particular value of certain rights at work such as workplace privacy[387] or occupational health.[388] The ESC includes a large set of labour rights, both individual and collective.[389]

209. The use of AI systems may have far-reaching implications for labour and employment, spanning numerous categories of occupations (including those relatively sheltered from previous waves of automation), employers, and workers. The use of AI systems could hinder access to

[385] *Demir and Baykara v. Turkey*, No. 34503/97, 12 November 2008.
[386] *Ognevenko v. Russia*, No. 44873/09, 20 November 2018, § 73.
[387] *López Ribalda and Others v. Spain* [GC], Nos. 1874/13 and 8567/13, 17 November 2019.
[388] *Meier v. Switzerland*, No. 10109/14, 9 February 2016.
[389] The right to work, just conditions of work, safe and healthy working conditions, fair remuneration, the right to equal opportunities and equal treatment in matters of employment and occupation without discrimination on the grounds of sex, protection in cases of termination of employment and protection of workers' claims in the event of the insolvency of their employer, dignity at work, right of workers with family responsibilities to equal opportunities and equal treatment; and collective: the right to organise and to bargain collectively, the right to information and consultation – also in collective redundancy procedures – and to take part in the determination and improvement of the working conditions and working environment, protection of workers' representatives in the undertaking and facilities to be accorded to them.

work, increase work intensity, reinforce or exacerbate power imbalances between employers and workers, reduce human involvement in decisions on hiring, evaluation and dismissal, and undermine fundamental principles and rights at work. AI-related challenges are particularly prevalent in new forms of employment such as platform or "gig" work.[390]

Right to Privacy and Data Protection

210. Article 8 protects the right to respect for private life at the workplace, encompassing privacy of correspondence,[391] email use,[392] data protection,[393] access to data,[394] professional reputation,[395] and provides grounds for protection in cases of unfair dismissals.[396]

211. States may also be obliged to adopt measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves, having regard to the fair balance that has to be struck between competing interests.[397] Taking into account that labour law leaves room for negotiations between the parties to a contract of employment to regulate the content of their relations, States have a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace.[398] However, the domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse.[399] In light of the rapid developments in this area, relevant factors have been identified for proportionality, as well as procedural guarantees against arbitrariness.[400] The domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body.[401]

212. Concerning lawfulness, employer policies may be sufficient in cases where labour market issues are, according to the State's legal framework, mainly regulated by the parties on the labour market and allow for the employer's right to manage and organise the work. [402] For this to be so, in cases concerning the positive obligations of the State under Article 8, the individual's right to privacy should be effectively protected and correctly balanced with the employer's rights by national courts. This includes cases of dismissal of employees for non-compliance with their duties revealed

---

[390] Platform work is a form of employment in which organisations or individuals use an online platform to access other organisations or individuals to solve specific problems, or to provide specific services in exchange for payment.
[391] *Bărbulescu v. Romania* [GC], No. 61496/08, 5 September 2017.
[392] *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.
[393] *Surikov v. Ukraine*, No. 42788/06, 26 January 2017.
[394] *Yonchev v. Bulgaria*, No. 12504/09, 7 December 2017.
[395] *S.W. v. the United Kingdom*, No. 87/18, 22 June 2021
[396] *Ülya Ebru Demirel v. Turkey*, No. 30733/08, 19 June 2018; *Denisov v. Ukraine* [GC], No. 76639/11, 25 September 2018.
[397] *Köpke v. Germany (dec.)*, No. 420/07, 5 October 2010, with further references.
[398] *Barbulescu v Romania* [GC], §§ 118-119.
[399] Ibid. § 120.
[400] Ibid. § 121. The relevant factors are: (i) whether the employee was clearly notified in advance about monitoring; (ii) the extent and intrusiveness of the monitoring; (iii) whether the employer had legitimate reasons for monitoring communications, especially for accessing their content; (iv) whether less intrusive alternatives were available; (v) the consequences for the employee and how the monitoring results were used; and (vi) whether adequate safeguards were in place to protect employee privacy.
[401] Ibid., § 122.
[402] *Wretlund v. Sweden,* No. 46210/99, decision of 9 March 2004 (inadmissible).

through video surveillance,[403] monitoring of private messages sent from a corporate messenger account[404], and employer access to employee files on a computer.[405]

213. For the ESC, the right to work freely includes protection from unwarranted privacy intrusions (Article 1§2).[406] Privacy interference can take various forms, including employer data collection (through video surveillance[407] or checking employees' emails[408]), storage, sharing, and use for employment decisions. Employees must be safeguarded against such interference, particularly when occurring through electronic communication and data processing.[409] Articles 1§2 and 26 (harassment protection) broadly protect against unnecessary workplace intrusion, but violations of employee privacy may also breach Article 3 (worker health, including mental health), Article 5 (trade union membership), Article 6 (collective bargaining), Article 11 (mental health), Article 20 (sex discrimination), and Article 24 (unjust dismissal).[410] The question of privacy at work can also be regulated by collective agreements.[411] In addition, Article 3 (the right to a safe and healthy workplace) applies across the public and private sectors, covering both employees and the self-employed.[412] In relation to the application of this right, the introduction of new technologies can generate, increase and shift factors of risk to the workers' health and safety. In particular, new technology, organisational constraints and psychological demands favour the development of psychosocial factors of risk, leading to work-related stress, aggression, violence and harassment.[413] States Parties to the ESC (or Revised European Social Charter) should review occupational risk prevention at both national and company levels in consultation with social partners (Article 3§1).[414] Under Article 3§2, they should adopt health and safety regulations aligned with scientific and international standards,[415] ensuring clear employer responsibilities and worker rights and duties.

Non-discrimination and equality

214. Article 14 and Protocol No. 12 ECHR prohibit discrimination in employment-related matters on a wide range of grounds. Gender-based discrimination in employment-related matters in particular is a recurrent problem: "where a difference of treatment is based on sex, the margin of appreciation afforded to the State is narrow and in such situations the principle of proportionality does not merely require that the measure chosen should in general be suited to the fulfilment of the aim pursued, but it must also be shown that it was necessary in the circumstances".[416] The advancement of gender equality is today a major goal in the member States of the Council of

---

[403] *Köpke v. Germany*, No. 420/07, decision of 5 October 2010 (inadmissible); *López Ribalda and Others v. Spain* [GC], Nos. 1874/13 and 8567/13, 17 October 2019.
[404] *Barbulescu v Romania* [GC].
[405] *Libert v. France, No. 588/13, 22 February 2018.*
[406] Conclusions 2012, Statement of Interpretation on Article 1§2.
[407] Conclusions 2020, Georgia.
[408] Conclusions XXI-1, Iceland.
[409] Conclusions 2012, Statement of Interpretation on Article 1§2.
[410] Conclusions 2012, Statement of Interpretation on Article 1§2.
[411] Conclusions 2016, Belgium.
[412] Conclusions II (1971), Statement of Interpretation on Article 3; Conclusions 2013, Statement of Interpretation on Article 3§3.
[413] Conclusions 2013, Statement of Interpretation on Article 3.
[414] Conclusions 2003, Statement of Interpretation on Article 3§1; see in particular Conclusions 2003, Bulgaria; Statement on Covid-19 and social rights adopted on 24 March 2021.
[415] *Marangopoulos Foundation for Human Rights (MFHR) v. Greece*, Complaint No. 30/2005, decision on the merits of 6 December 2006, §224.
[416] *Emel Boyraz v. Turkey,* No. 61960/08, 2 December 2014, § 51.

Europe and very weighty reasons would have to be put forward before such a difference of treatment could be regarded as compatible with the ECHR.[417]

215. As regards the ESC, to comply fully with the rights to access employment (Article 1§2),[418] to equal pay between women and men (Article 4§3),[419] and to equal opportunities in matters of employment (Article 20)[420], States Parties must implement legal measures to ensure the effective enforcement of the prohibition of discrimination. Should claims of discrimination arise, effective remedies include judicial and administrative procedures, ensuring access to reinstatement, compensation, and enforceable penalties, with labour inspections playing a key role in enforcement.[421] These remedies must be adequate, proportionate, and dissuasive to ensure meaningful protection against discrimination.[422]

216. AI systems are increasingly being used in recruitment processes,[423] which may be negatively affected, for example in cases where reliance on machine learning in the identification of candidates led to discriminatory outcomes, or where AI-based facial recognition and emotion analysis systems have resulted in racial discrimination.[424] As such, AI systems used for recruitment and selection of candidates should be objective, neutral and free from bias, including gender bias. In a broader context, States should ensure that the use of AI systems in the workplace does not reproduce or amplify existing patterns of inequality and promotes equality including gender equality, diversity and inclusion. In particular, this could consist of regular auditing of the outcomes of the use of AI systems in recruitment, promotion and other procedures; the involvement of employees and their representative organisations in policies or choices regarding the use of AI in decision-making in the workplace; monitoring of the impact of the introduction of AI systems in the workplace on gender equality and diversity in the workforce; and training and awareness-raising for the workforce on data bias, stereotypes and risks of discrimination in using AI systems.

217. The use of AI in employment also harbours the risk that inequalities will persist and worsen if, for example, older persons, persons with disabilities or persons with limited digital skills lack the required abilities to use them. For these people, the chances of participating in the labour market may deteriorate. In addition, limited access to AI systems and tools can prevent individuals from experiencing the benefits and advantages which they may offer. Policymakers should ensure that AI systems are accessible, and promote together with employers the development and diffusion of AI systems that contribute to better participation in employment, such as assistance systems.

Transparency and Accountability

218. The use of AI in labour and employment presents challenges regarding transparency and accountability, particularly in the context of hiring, wage determination, workplace surveillance, and decision-making processes. For example, due to AI systems' black box problem, wage-setting and task allocation in platform and gig work may leave workers without explanations for pay fluctuations or job availability. Accountability mechanisms are equally vital to prevent the use of AI in the

[417] Ibid.
[418] Conclusions XVI-1 (2003), Iceland.
[419] *University Women of Europe (UWE) v. Belgium*, Complaint No. 124/2016, decision on the merits of 6 December 2019, §115.
[420] Conclusions 2020, Albania.
[421] Conclusions 2020, Cyprus.
[422] Conclusions XVIII-I (2006), Austria.
[423] Resolution 2343 (2020) 'Preventing discrimination caused by the use of artificial intelligence', paragraph 1. See also Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems, paragraph 8.
[424] CDADI/GEC Study (2023), pp. 19-21.

workplace from undermining labour rights. Employers and policymakers should implement clear regulations, ensuring that AI systems align with fairness, non-discrimination, and worker protection standards. Effective remedies should be available to rights holders.

Freedom of Expression; Freedom of Assembly and Association

219. Article 10 ECHR (freedom of expression) applies in the context of labour relations, including where these are governed by private law; the State has a positive obligation to protect the right to freedom of expression even in the sphere of relations between individuals.[425] Article 11 ECHR (freedom of assembly and association) protects both workers and trade unions. An employee or worker should be free to join or not join a trade union without being sanctioned or subject to disincentives.[426] In view of the sensitive character of the social and political issues involved in achieving a proper balance between the respective interests of labour and management, and given the high degree of divergence between the domestic systems in this field, States enjoy a wide margin of appreciation as to how trade union freedom and protection of the occupational interests of union members may be secured.[427]

220. The ESC protects freedom of association as the right to organise under Article 5, guaranteeing workers the right to form and join trade unions and employers' organisations without prior authorisation.[428] Article 28 ESC complements these protections by safeguarding trade union independence and ensuring protection for workers' representatives,[429] including protection from dismissal or any retaliatory treatment[430] such as denial of benefits, training, promotions, or discriminatory layoffs.[431]

221. AI-driven workplace surveillance may have adverse consequences for free expression and unionisation. The misuse of AI system-based surveillance can present threats to employees' freedom of expression and their freedom of association by potentially having a chilling effect on their rights to hold opinions, receive and impart information and ideas and organise, set up workers' meetings, and communicate confidentially. Monitoring communications, interactions, and movements can help employers suppress trade union activities by hindering meetings or discouraging employees from speaking out. A lack of protection for employees from discrimination by the employer on the grounds of their trade union activities could have discourage other persons from joining that trade union, which could in turn lead to its disappearance.[432]

222. To prevent the adverse impacts of AI system-driven workplace surveillance, States should enforce strict safeguards ensuring transparency, accountability, and compliance with Articles 10 and 11 ECHR and Articles 5 and 28 ESC. Employers must justify surveillance measures as necessary and proportionate, with clear limits to prevent anti-union misuse.

---

[425] *Herbai v. Hungary*, No. 11608/15, 5 November 2019, § 37; *Fuentes Bobo v. Spain*, No. 39293/98, 2000 February 29, § 38.
[426] *Associated Society of Locomotive Engineers and Firemen (ASLEF) v. the United Kingdom,* No. 11002/05, 27 February 2007, § 39.
[427] *Sindicatul "Păstorul cel Bun" v. Romania* [GC], No. 2330/09, 9 July 2013, § 133.
[428] Conclusions 2010, Georgia; Conclusions I (1969), Statement of interpretation on Article 5.
[429] Conclusions 2003, Bulgaria.
[430] Conclusions 2018, Russian Federation.
[431] Conclusions 2018, Azerbaijan.
[432] *Danilenkov and Others v. Russia*, No. 67336/01, 30 July 2009, § 135; and *Trade Union of the Police in the Slovak Republic and Others v. Slovakia*, 25 September 2012, No. 11828/08, §§ 60-61.

Further reading

- European Court of Human Rights, *Factsheet – Surveillance at workplace*,
- European Court of Human Rights, *Factsheet – Trade union rights*
- European Court of Human Rights, *Factsheet – Work related rights*
- OECD, *Employment Outlook 2023, Artificial Intelligence and the Labour Market*, 2023
- OECD, *Using AI to Support People with Disability in the Labour Market: Opportunities and Challenges*, 2023
- OECD, *Using AI in the Workplace: Opportunities, Risks and Policy Responses*, 2024
- International Labour Organisation, *Generative AI and Jobs: A global analysis of potential effects on job quantity and quality*
- International Labour Organisation, *Digital transformation in employment policies*
- International Labour Organisation, *The Algorithmic Management of work and its implications in different contexts*, 2022
- McKinsey Global Institute, *A new future of work: The race to deploy AI and raise skills in Europe and beyond*, 2024