EUROPEAN CONVENTION ON HUMAN RIGHTS
CONVENTION EUROPÉENNE DES DROITS DE L'HOMME
1950 · 2025 75

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CDDH-IA(2025)01
17/01/2024

STEERING COMMITTEE FOR HUMAN RIGHTS

(CDDH)

DRAFTING GROUP ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

(CDDH-IA)

[DRAFT] Handbook on human rights and artificial intelligence

Chapters I and III

Table of Contents

1. INTRODUCTION

1. Artificial intelligence (AI) is increasingly influencing various aspects of society, unlocking new opportunities for innovation and progress. This includes the potential to advance human rights, for example, by expediting judicial proceedings, enhancing healthcare through predictive diagnostics, and personalising education to meet individual learning needs. Yet alongside these opportunities come significant risks that have been recognised by the international community.

2. AI's potential to threaten human rights has driven global efforts to regulate this set of technologies. The Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law is the first international treaty on AI and human rights.[1] 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.[2] Implementation of the Framework Convention will be facilitated by the HUDERIA Methodology, a structured tool designed to assess and mitigate risks posed by AI systems to human rights, democracy, and the rule of law. The Council of Europe [has also developed] specific instruments on the implications of generative artificial intelligence for freedom of expression and AI's impact on equality and non-discrimination, including gender equality.[3] Another important development regionally is the "AI Act" of the European Union.[4] As the first comprehensive horizontal legal framework for AI regulation in the EU, it aims to ensure that AI systems operating in the EU are safe and adhere to fundamental rights and EU values, incorporating measures for risk assessment, accountability, and oversight. The EU AI Act complements existing EU laws, such as the General Data Protection Regulation (GDPR).

3. The OECD adopted the first "Recommendation on Artificial Intelligence" in 2019. UNESCO's "Recommendation on the Ethics of Artificial Intelligence", adopted in 2021 provides voluntary guidelines for ethical AI governance, encouraging stakeholder collaboration for implementation. The United Nations General Assembly has also adopted two resolutions on AI which emphasise international cooperation for safety and development.[5]

4. Existing human rights instrument such as the European Convention on Human Rights and its Protocols (ECHR) and the European Social Charter (ESC), remain fully applicable in the context of AI. These instruments, interpreted by the European Court of Human Rights (ECtHR or the Court) and the European Committee on Social Rights (ECSR) respectively, establish basic standards for the protection of human rights for Council of Europe member States. While neither the Court nor the ESCR has yet addressed AI's impact on human rights, States must align their legal frameworks on AI with the requirements of the ECHR and ESC.

5. 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

[1] Status signatures and ratifications as of 16/01/2025 - https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225

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

[3] Appendix [x] of the Handbook provides further information on concluded, ongoing, or forthcoming initiatives [to be completed].

[4] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.

[5] Resolution A/RES/78/265 "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development" (21 March 2024) emphasises respect, protection, and promotion of human rights in the design, development, deployment, and use of AI, and calls on stakeholders to "refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights" and reinforces the need for "regulatory and governance approaches and frameworks related to safe, secure and trustworthy use of AI"; and Resolution A/RES/78/311 on "Enhancing International Cooperation on Capacity-building of Artificial Intelligence" (1 July 2024).

States in applying ECHR and ESC standards to AI-related challenges. 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, 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 assess AI's human rights impacts considering ECHR and ESC standards, without predicting specific outcomes of future cases.[6]

6. Chapter 2 of the Handbook introduces key technical concepts linking AI's technological aspects to human rights implications. Chapter 3 outlines general human rights principles under the ECHR and ESC relevant to AI across public sectors. It addresses first cross-cutting issues relevant to all sectors. Then it provides a sectoral analysis of AI use cases in public governance, examining human rights impacts, relevant legal principles, and good practices from Council of Europe member States. The Handbook also considers the role of businesses in AI governance and explores how policymakers can address public-private intersections using the standards of the ECHR and the ESC, as well as other international norms. It concludes in Chapter IV with reflections on emerging challenges in AI governance, ensuring a dynamic and forward-looking approach.

[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.

3. HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

3.1 General Issues

7. This section introduces the ECHR, the ESC, and the Framework Convention. It outlines the general principles of the ECHR and the ESC that guide the protection of rights in the context of AI and refers to the Framework Convention where its principles may provide useful guidance in the context of the ECHR and the ESC. Recurring human rights challenges are also examined.

3.1.1 The European Convention on Human Rights (ECHR)

8. 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 (ECtHR or the Court) monitors the implementation of the ECHR. Individuals, groups, companies, and non-governmental organizations (NGOs) can bring complaints of alleged human rights violations before the Court once all domestic remedies have been exhausted. The rights and freedoms protected in the ECHR are listed in appendix [x].

3.1.2 The European Social Charter (ESC)

9. The European Social Charter guarantees fundamental social and economic rights as a counterpart to 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.[7] 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.[8] While its decisions and conclusions are not directly enforceable, they establish binding legal interpretations that States must respect. The rights protected in the ESC are listed in appendix [x].

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

10. The Framework Convention complements existing international standards (such as the ECHR and the ESC). It adopts a technology-neutral approach, focusing on principles rather than regulating specific technologies. It applies to AI systems used by public authorities (including private actors acting on their behalf) but it does not automatically apply to private actors. Instead, State Parties may choose to extend its rules and principles to private entities or implement “other appropriate measures”.[9] In addition, three areas are exempted from the scope of the treaty: (i) activities related to “national security”[10]; (ii) research and development activities[11]; and (iii) activities related to “national defence”.[12]

11. Activities within the lifecycle of AI systems must comply with the following principles.[13]

- Human dignity and individual autonomy

[7] Liechtenstein, Monaco, San Marino and Switzerland have not ratified either of these treaties.

[8] 16 of the 42 Parties to the ESC have ratified this additional protocol.

[9] Article 3 subparagraph 1 (b).

[10] Article 3.2

[11] Article 3 subparagraph (3).

[12] Article 3.4

[13] Chapter III (Articles 6-13)

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

12. Key requirements include the provision of remedies[14], conducting risk and impact assessments[15] on human rights, democracy, and the rule of law; ensuring procedural safeguards for affected persons, including providing notice when interacting with AI systems;[16] and enabling the possibility of bans or moratoria on high-risk AI applications.[17] It also provides for follow-up mechanisms and cooperation and introduces an obligatory monitoring mechanism.[18]

3.1.4 ECHR and ESC General Principles in the Context of AI

13. Neither the Court nor the ESCR has yet addressed AI's impact on rights under the ECHR and ESC. Established principles under the ECHR and the ESC provide guidance on how these treaties may apply to AI-related human rights challenges. While some principles are shared, others are unique to each treaty.[19]

Effective Protection of Rights

14. The ECHR and the ESC are intended to guarantee rights that are not theoretical or illusory but practical and effective.[20] National authorities must ensure rights holders can effectively enjoy their rights, which involves not only adopting legislation but also ensuring its effective application, providing adequate resources, and establishing appropriate operational procedures. Thus, States should ensure the effective protection of human rights against harms related to activities within the lifecycle of AI systems not only by implementing laws but also by providing resources, and establishing, for example, oversight mechanisms.

Subsidiarity and the margin of appreciation

15. Subsidiarity means that the States bear the primary responsibility to secure to everyone within their jurisdiction the rights and freedoms defined in the ECHR. The Court authoritatively interprets the ECHR and acts as a safeguard for individuals whose rights and freedoms are not secured at the national level.[21]

16. 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.

[14] Chapter IV (Article 14).

[15] Chapter V (Article 16).

[16] Article 15.

[17] Article 16 (4).

[18] Chapter VII (Articles 23-26).

[19] 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*, 9 October 1979, 6289/73, § 24; see also Digest of Case Law of the European Committee of Social Rights, December 2022, p. 33.

[20] *Airey v Ireland*, 9 October 1979, 6289/73, § 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.

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

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.[22]

17. The extent of the margin of appreciation enjoyed by national authorities depends on the nature of the right involved and the severity of the threat that the act or omission in question would pose to that right.

Evolutive Interpretation and the 'Living Instrument' Doctrine

18. The ECHR and the ESC are "living instruments," interpreted dynamically in the light of present-day conditions to address evolving societal and technological issues. The Court's past rulings on topics like data interception[23], biometric data[24], the internet and digital tools[25] highlight its ability to adapt rights to modern challenges. Through application of this doctrine, the Court is expected to apply the ECHR to AI-related cases in the future.

Human Dignity

19. Upholding human dignity implies respecting the inherent value and worth of each individual, regardless of their background, characteristics, or circumstances and refers in particular to the manner in which all human beings should be treated.[26]

20. In the ECHR system, human dignity is invoked by the Court to affirm individuals' intrinsic worth and equality.[27] The Court has held that "[r]espect for human dignity forms part of the very essence of the Convention".[28] The ESC system recognises human dignity as central for the effective realisation of economic and social rights and as a core principle that may not be derogated from.[29]

21. The Framework Convention also features human dignity among the principles that must govern artificial intelligence.[30] 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.[31]

Personal Autonomy and Self-Determination

22. The notion of personal autonomy is an important principle underlying the interpretation of ECHR guarantees.[32] 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.[33]

[22] Idem.

[23] *Big Brother Watch and Others v. United Kingdom* [GC], no. 58170/13, 2021.

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

[25] *Ahmet Yıldırım v. Turkey*, no. 3111/10, 2012; *Magyar Helsinki Bizottság v. Hungary* [GC], no. 18030/11, 2016.

[26] Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Explanatory Report), §54.

[27] *Lăcătuş v Switzerland*, application, no. 14065/15, Merits and Just Satisfaction, 19 January 2021.

[28] *Magyar Helsinki Bizottság v Hungary* [GC], no. 18030/11, Merits and Just Satisfaction, 8 November 2016 at para 155.

[29] International Federation of Human Rights (FIDH) v. France, complaint No. 14/ 2003, decision on the merits of 8 September 2004, §31.

[30] Framework Convention, Article 7.

[31] Explanatory Report, § 53.

[32] *Pretty v. United Kingdom*, no. 2346/02, § 61 and [GC] judgment of 11 January 2006, *Sorensen and Rasmussen v. Denmark*, nos. 52562/99 and 52620/99, § 54.

[33] Explanatory Report to the Framework Convention, §55.

Positive Obligations

23. States have a duty under 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). This applies even in cases where threats originate from private individuals or entities beyond direct state control as these instruments address both vertical relationships—between national authorities and individuals—and horizontal relationships[34], which involve interactions between individuals or entities. States must protect human rights in the sphere of the relations between individuals themselves (horizontal effect).

24. Positive obligations impose a duty of conduct, not result. States must act diligently and reasonably, taking appropriate measures within their resources and capacities. Positive obligations may require the State to impose sanctions for individuals or entities violating the ECHR, enact specific legal rules, and/or take operational steps to protect individuals from foreseeable risks to their rights.[35]

25. States' positive obligations require them proactively to assess whether AI systems might harm human rights and enact legislation; and/or implement measures to mitigate risks.

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

26. States Parties are allowed to restrict certain rights in the ECHR[36] and the ESC[37] but only if the interference can be justified. There are some general requirements which are relevant to almost all rights and freedoms. The interference must be (i) 'prescribed by law' or 'in accordance with the law' (requirement of lawfulness). 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. The interference must also be foreseeable, allowing people to anticipate how and when their rights might be restricted. Lastly, it must be free from arbitrariness and implemented with proper procedural safeguards to ensure fairness and due care. The interference with the right must (ii) pursue a legitimate aim and it must be (iii) necessary (in a democratic society) to achieve the legitimate aim pursued (requirement of 'necessity'; often framed as the requirement of 'proportionality' or the requirement of 'fair balance').

27. States will have to show that any restrictions on ECHR or ESC rights resulting from activities within the AI systems lifecycle that amount to interference are lawful, pursue legitimate aims, and are necessary in a democratic society. Restrictions must be proportionate, respond to pressing social needs, and use the least restrictive means.

[34] 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*, n 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.

[35] *Osman v. The United Kingdom* [GC], nos. 87/1997/871/1083, § 115

[36] There are absolute rights which cannot be subject to derogations, exceptions, or permissible interference, e.g., the prohibition of torture (Article 3 of the ECHR). Some rights may be subject to specific exceptions provided by the relevant legal provision, e.g. the right not to be arbitrarily deprived of liberty (Article 5 of the ECHR). In such cases, the Court has clearly established that the list of exceptions in a given provision is exhaustive and that only a narrow interpretation of those exceptions is consistent with the aim of that provision. Measures affecting such rights should respect the limits of the exceptions set in the relevant provisions.

[37] 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.

3.1.5 Core human rights issues across public governance sectors

28. AI impacts 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 in the ECHR and the ESC

29. The ECHR[38] and the ESC[39] prohibits discrimination but only in relation to the enjoyment of rights and freedoms set out in the ECHR/ESC, serving as a complement to their substantive provisions. Article 1 of Protocol No. 12 ECHR introduces a broader prohibition against discrimination covering "any right set forth by law".[40] The grounds for discrimination explicitly mentioned in these instruments are "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 and, for example, cover also disability[41] or age.[42] The prohibition of discrimination applies in vertical and horizontal relations. Discrimination can be direct or indirect.[43] Direct discrimination arises from "a difference in the treatment of persons in analogous, or relevantly similar, situations" [44] and where this difference is "based on an identifiable characteristic".[45] Indirect discrimination occurs when seemingly neutral legislation disproportionately and unjustifiably affects a particular group of persons.[46]

30. The Framework Convention's principle on equality and non-discrimination[47] 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"[48], and its provision on non-discrimination explicitly prohibits discrimination in its implementation.[49] It draws directly from established international norms, including the ECHR and the ESC.[50]

ii. Risks to Non-Discrimination and Equality

31. 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

[38] ECHR Article 14.
[39] RESC Article E.
[40] This Protocol has been ratified by 20 member States of the Council of Europe.
[41] *Glor v. Switzerland*, no. 13444/04, 30 April 2009, § 80.; *G.N. and Others v. Italy*, no. 43134/05, 1 December 2009, § 126.; *Kiyutin v. Russia*, no. 2700/10, 10 March 2011, § 57.; *Association internationale Autisme-Europe (AIAE) v. France*, Complaint No. 13/2000, decision on the merits of 4 November 2003, §51.
[42] *British Gurkha Welfare Society and Others v. the United Kingdom*, no. 44818/11, 15 September 2016, § 88; *Šaltinytė v. Lithuania,* no. 32934/19, 26 October 2021, § 63.
[43] *D.H. and Others v. The Czech Republic* [GC], no. 57325/00, § 184.
[44] *Burden v. the United Kingdom* [GC], no. 13378/05, 29 April 2008, § 60.
[45] *Biao v. Denmark* [GC], no. 38590/10, § 89.
[46] *D.H. and Others v. the Czech Republic* [GC], no. 57325/00, 13 November 2007.
[47] Framework Convention, Article 10.
[48] Explanatory Report, § 75.
[49] Framework Convention, Article 17.
[50] Explanatory Report, § 71.

characteristics or proxies and their intersections. These effects can be further compounded by information asymmetries and can be more severe for those in vulnerable situations and women, by among other things leading to an increase in online and offline violence against these groups. This is a cross-cutting issue as interconnectedness of public governance systems means that biased outcomes resulting from the use of AI systems in one sector can ripple into others; for example, biased predictive policing may affect criminal justice decisions, which in turn influence social service provisions.

32. AI systems may be prone to indirect discrimination, as seemingly neutral data points that indirectly correlate with protected characteristics can lead to discriminatory outcomes. For example, the use of proxies like postal codes or spending habits, which may seem neutral but indirectly reflect characteristics such as ethnicity or socio-economic status, may result in biased decisions. Another concern is AI systems capacity for intersectional discrimination where multiple grounds of discrimination intersect.[51] States should ensure that appropriate measures are in place to promote equality and prevent and combat discrimination in the context of AI systems.

The Right to Privacy and Personal Data Protection

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

33. Article 8 (the right to respect for private and family life), through the protection of private life, applies to the collection and processing of personal data.[52] Private life, among others, includes the one's image, identity, personal development, and relationships, and extends also to professional or business activities. Personal data covers information such as names, addresses, dynamic IP addresses, and sensitive data like health and racial information. The Court also addressed under this right the interception of communications, such as emails and phone calls. It held that such measures constitute an interference with privacy rights and must be lawful, pursue a legitimate aim, be necessary and proportional.

34. Council of Europe Convention No. 108 and its amending Protocol (the ‘modernised’ Convention 108(+)[53] protects individuals with regard to automatic processing of personal information relating to them.[54] Convention No. 108 defines personal data as "any information relating to an identified or identifiable individual".[55] Key principles of personal data processing include lawfulness, fairness, purpose limitation, data minimization, accuracy, 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. Consent, which must be free, specific, and informed, plays a central role in legitimising data processing.[56] The Court has referred to the standards of Convention No. 108 in its judgments concerning data protection.

[51] 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”.

[52] 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.

[53] CETS No. 223.

[54] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108.)

[55] Article 2.

[56] The updated Convention 108(+) enhances these protections by addressing emerging digital challenges and emphasising accountability for data controllers and processors.

35. The Framework Convention obliges Parties to adopt measures ensuring the protection of privacy and personal data throughout the lifecycle of AI systems.[57] This includes compliance with applicable domestic and international laws, such as the ECHR and Convention No. 108.[58]

ii. Privacy and Data Protection Risks

36. Data protection and the right to privacy are cross-cutting issues in the context of AI because these systems rely heavily on collecting, processing, and analysing vast amounts of data that may include personal data. The risks include unauthorised data use, inadequate safeguards, and decisions to process personal data made without individuals' knowledge or consent, threatening privacy and personal data protection. Furthermore, AI systems may be used for mass surveillance (including biometric surveillance), or profiling.

37. Effective safeguards are necessary to address risks like unauthorised data collection, misuse, and harm to individuals' dignity.[59] There should be independent supervisory authorities and adherence to international best practices to ensure privacy protection in both public and private sector AI applications.[60] The 2019 Guidelines on Artificial Intelligence and Data Protection, developed by the Convention No. 108 Consultative Committee (T-PD), provide further guidance for policymakers and AI developers, emphasising privacy-by-design, transparency, and the prevention of discrimination to uphold democratic values and foster public trust. Key points include ensuring risk assessments, supporting supervisory authorities, fostering collaboration between regulatory bodies, preserving human decision-making autonomy, and promoting digital literacy.

Effective remedies

i. The right to an effective remedy

38. 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 and capable of addressing the substance of the alleged violation and providing appropriate redress.[61] Effective remedies must be practical in both law and practice, accessible, affordable, and capable of providing appropriate redress.[62] They can include judicial mechanisms or a quasi-judicial body such as an ombudsman[63], an administrative authority such as a government minister[64], or a political authority such as a parliamentary commission.[65] These should be independent and procedural safeguards should be afforded to the applicant.[66] However, the Court may find a remedy before a judicial authority to be essential.[67] Additionally, States are required to

[57] Article 11.
[58] Explanatory Report, §§ 80-82.
[59] Recommendation CM/Rec(2021)8 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.
[60] Explanatory Report, §§ 79-83.
[61] *Boyle and Rice v. the United Kingdom*, 1988, § 52; *Powell and Rayner v. the United Kingdom*, 1990, § 31; M.S.S. *v. Belgium and Greece* [GC], 2011, § 288; *De Souza Ribeiro v. France* [GC], 2012, § 78; *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], 2014, § 148.
[62] *Paulino Tomás v. Portugal*, (dec)., no. 58698/00.
[63] *Leander v. Sweden*, 26 March 1987, no. 9248/81.
[64] *Boyle and Rice v. the United Kingdom*, 27 April 1988, Nos. 9659/82 and 9658/82.
[65] *Klass and Others v. Germany*, 6 September 1978, No. 5029/71, § 67
[66] *Khan v. the United Kingdom*, 12 May 2000, No. 35394/97, §§ 44-47.
[67] *Ramirez Sanchez v. France* [GC], 2006, §§ 165-166.

ensure that individuals have access to judicial or non-judicial mechanisms to address human rights violations by private actors, such as businesses.[68]

ii. Risks to the Right to an Effective Remedy

39. Exercise of the right to an effective remedy may be hindered in relation to alleged violations caused by AI systems due to their technical complexity, opacity, and reliance on vast datasets. Individuals may lack the knowledge or access to information necessary to identify violations. Individuals may remain unaware of the extent of interference with their rights or struggle to understand the underlying decision-making processes. Consequently, remedies should be accessible - available and comprehensible to individuals - and effective, meaning they can adequately address and rectify the harm caused by AI systems.

40. Parties to the Framework Convention are required to provide mechanisms that ensure access to effective remedies for human rights violations arising from AI activities.[69] This includes documenting and making relevant information available to affected individuals, enabling them to understand and exercise their rights. The relevant content in the information-related measures should be context-appropriate, sufficiently clear and meaningful, and critically, provide a person concerned with an effective ability to use the information in question to exercise their rights in the proceedings in respect of the relevant decisions affecting their human rights.[70]

3.2 Business and Human Rights

41. 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

42. States can be held accountable for failing to regulate and control acts of businesses that violate human rights.[71] The concrete scope and content of State obligations to prevent and redress corporate-related human rights violations depends to some extent on the human right in question and the factual circumstances. For example, States may need to criminalise harmful actions by private actors, adopt laws or policies, or take operational measures to prevent third-party abuses. Positive obligations may arise in a wide range of situations, such as media businesses interfering with freedom of expression[72]; abuses in private hospitals[73] and schools[74]; workplace dress restrictions affecting the right to manifest religion[75];

[68] *Z and Others v. the United Kingdom* [GC], No. 29392/95, 2001, § 109; *Keenan v. the United Kingdom*, No. 27229/95, 2001, § 129; *Paul and Audrey Edwards v. the United Kingdom*, No. 46477/99, 2002, § 97.

[69] Framework Convention, Article 9.

[70] Explanatory Report, § 99

[71] *Ilaşcu and Others v. Moldova and Russia* [GC], no. 48787/99, 8 July 2004, § 318. "The acquiescence or connivance of the authorities of a Contracting State in acts of private individuals which violate the Convention rights of other individuals within its jurisdiction may engage the State's responsibility under the Convention".

[72] *Axel Springer AG v. Germany* [GC] 7 February 2012 and *Von Hannover v. Germany* [No. 2]
[GC], 7 February 2012.

[73] *Storck v. Germany*, no. 61603/00, 16 June 2005.

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

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

providing workers with information to assess occupational health and safety risks[76]; or environment-related human rights harms caused by business activities.[77]

43. The Court's caselaw highlights positive obligations (i) to regulate and control business operations; (ii) to provide essential information and enable public participation and informed decision making and (iii) to provide effective remedies for business-related human rights violations.

Obligations to regulate and control business operations[78]

44. States should reasonably ensure that businesses involved in the AI lifecycle are subject to adequate oversight, and compliance mechanisms[79]. The Court's focus on 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 biases" or opaque AI decision-making processes.

Obligations to provide essential information and procedural obligations[80] to enable public participation and informed decision making

45. States should provide essential information to the public about risks involved in the business activity.[81] This obligation is prospective and precautionary, as 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.[82]

State decisions in relation to business activities – such as granting a licence - may also impact on human rights. To afford due respect for the interest safeguarded 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".[83]

46. In the Framework Convention, the principles of transparency and oversight[84] 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".[85]

Obligations relating to the provision of effective remedies

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

[77] *Lopez Ostra v. Spain,* no. 16798/90, 9 December 1994; *Guerra and Others v. Italy* [GC], No. 14967/89, 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.

[78] Including for example the licensing, setting up and supervision of dangerous activities and the provision of information about such activities to the general public.

[79] *Fadeyeva v. Russia*, no. 55723/00, 9 June 2005, § 89.

[80] Procedural obligations call for domestic procedures to ensure better protection of rights holders.

[81] *Öneryıldız v. Turkey* [GC], no. 48939/99, § 90.

[82] *Vilnes and Others v. Norway*, nos. 52806/09 and 22703/10, 24 March 2014, § 235.

[83] *Taskin and Others v. Turkey*, § 118.

[84] See Framework Convention Article 8.

[85] Explanatory Report, para 57.

47. States should also provide effectively remedies for business-related human rights violations. This may include amending laws if the legal framework is inadequate.[86] Of relevance here is the right to an effective remedy (Article 13 ECHR).

Margin of appreciation in the context of positive obligations

48. It is important to note that States generally enjoy a wide margin of appreciation in deciding how to regulate and control 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",[87] as well as in cases of severe threats to human rights. Thus, while States have a margin of appreciation in regulating AI technologies in the context of businesses activities, their discretion could be significantly limited when AI systems pose severe threats to human rights.

3.2.2 Balancing Competing Human Rights in the Context of AI Governance

49. Transparency and explainability requirements in relation to, for example, bias mitigation raise questions around the intersection of privacy and intellectual property and trade secret laws. A business' own AI system may be covered by intellectual property and trade secrets legislation. Businesses are entitled to the protection of rights, such as property rights (e.g., intellectual property)[88] or freedom of expression (Article 10 ECHR).[89] Their rights must be balanced against, and can sometimes outweigh, the rights of individual applicants.

50. If rights holders claim that AI systems violate 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 under the ECHR). Domestic courts or regulators should carefully weigh these interests to ensure a fair and proportional outcome. In this context, the Council of Europe Recommendation 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.[90]

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

Relevant non-binding instruments

51. The ECHR and ESC do not address human rights obligations to businesses directly (see however vertical and horizontal effect). While individuals cannot directly raise complaints against businesses before the Court or the ECSR, they may bring claims against states for failing to prevent or address violations resulting from business-related activities. Some international non-binding instruments in the field of business and human rights, however, provide further detail on states and businesses responsibilities.

52. 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,

[86] *Fadeyeva v. Russia*, §§89 and 92; see also *Powell and Rayner v. the United Kingdom*, no. 93101/81, 21 February 1990.
[87] *Hatton & Others v United Kingdom* [GC], 7 August 2003, § 102.
[88] *Anheuser-Busch Inc. v. Portugal* [GC], no. 73049/01, 11 January 2007, § 72.
[89] *Axel Springer AG v. Germany* [GC], no. 39954/08, judgment of 7 February 2012.
[90] CM/Rec(2020)1, § 5.2

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.

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

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

55. For Council of Europe member States, the duty to protect against business-related human rights abuses; and to provide effective remedies are best exemplified by the jurisprudence of the Court and the practice of the ECSR as detailed above.

56. The following section therefore will focus on businesses responsibilities to protect human rights in the context of AI through the framework of the UNGPs.

Corporate Responsibility to Respect Human Rights

57. Experience has shown that companies in almost any industry can impact—positively or negatively—almost any human right. Businesses (usually) do not directly violate human rights but may breach labour or environmental regulations, which are tied to the state's duty to protect human rights. For instance, States must regulate workplace safety to uphold the right to life, while businesses are obligated to comply with these rules and may be subject to criminal or administrative proceedings for failure to do so.

58. 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.[91] 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).

59. To date, no AI-specific guidance on corporate responsibility for human rights has been developed. The UNGPs, however, 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.

[91] UNGPs, Principle 15-24.

60. In line with Recommendation CM/Rec(2016)3 on human rights and business, States should 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.[92] 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.[93]

3.3 Public Governance Sectoral Analysis

61. This chapter 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 is advanced or is reasonably in prospect.

3.3.1 Administration of Justice

62. 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 and correctional facilities.

Key AI use cases

63. 118 AI-integrated systems have been documented as being used or piloted within justice systems across Europe.[94] While AI systems designed for ancillary administrative tasks pose minimal risk,[95] 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.

64. Key high-risk 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 / automated decision-making*: 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.

[92] CM/Rec(2016)3, para 20.
[93] Idem, para 20.
[94] https://www.coe.int/en/web/cepej/resource-centre-on-cyberjustice-and-ai
[95] Such as anonymisation or pseudoanonymisation of judicial decisions, documents or data, communication between personnel and the automation of other administrative tasks.

- *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.

65. 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

66. The principles identified in the Framework Convention[96] and the non-binding European Ethical Charter on the Use of Artificial Intelligence[97] 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(+). These principles include respect for human rights; non-discrimination; quality and security of AI[98]; transparency, impartiality and fairness; and the principle of "under user control".[99]

67. The human right primarily impacted in this sector is the right to a fair trial, guaranteed by Article 6 ECHR.[100]

The right to a fair trial

68. The key principle governing Article 6 is fairness.[101] 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.[102] Certain subsidiary principles of fairness are particularly relevant in the AI context:

(i) Independence and impartiality

69. Article 6 guarantees in the determination of civil rights and obligations or of any criminal charge a hearing by an independent and impartial tribunal established by law.[103] The tribunal should be independent both from other branches of government, such as the executive and legislature, and from the parties

[96] Framework Convention (Articles 4 to 13).

[97] The European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" ("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 (albeit non-binding) 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

[98] With regard to the processing of judicial decisions and data, using certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment.

[99] Precluding a prescriptive approach and ensuring that users are informed actors and in control of their choices.

[100] 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.

[101] *Vacher v. France*, no. 20368/92, 17 December 1996.

[102] *Ibrahim and Others v. the United Kingdom* [GC], 2016, § 250

[103] See *Deweer v. Belgium*, 27 February 1980, § 49, Series A no. 35; *Kart v. Turkey* [GC], 3 December 2009, no. 8917/2005, § 67.

involved in a case.[104] 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.[105]

70. Bias in AI systems may not be easily discernable by the judge due to the generalised perception of algorithmic/mathematic "neutrality" and judges' own technology bias. This could lead to discriminatory outcomes and interfere with the impartiality of the judge. 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, or in which their personal liability (disciplinary, civil or even criminal) is likely to be incurred.[106]

(ii) Presumption of innocence

71. 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.[107]

72. As a result of algorithmic bias, the potential inclusion in AI systems of variables such as criminal history and family background means that the fate of an individual 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[108], in other jurisdictions there are real-life examples of the negative effects.[109]

(iii) Equality of arms and adversarial proceedings

73. Equality of arms 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.[110] The right to adversarial proceedings 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.[111] 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.[112] The right to adversarial proceedings may not be disregarded to save time and expedite the proceedings.[113]

[104] *Beaumartin v. France*, no. 15287/89, 24 November 1994, § 38; Sramek v. Austria, no. 8790/79, 22 October 1984, § 42.
[105] *Findlay v. the United Kingdom*, no. 22107/93, 25 February 1997, § 73.; *Micallef v. Malta* [GC], no. 17056/06, 2009 § 93
[106] CEPEJ, *Ethical Charter*, § 140.
[107] *Barberà, Messegué and Jabardo v. Spain*, 6 December1988, Application no 10590/83, § 77
[108] Ethical Charter, para 124.
[109] Idem, paras 128-131.
[110] *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.
[111] *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.
[112] *Natunen v. Finland,* 31 March 2009, Application no. 21022/04, §43.
[113] *Nideröst-Huber v. Switzerland*, no. 18990/91, 18 February 1997, § 30.

74. Concerns may arise if a party is denied sufficient access to AI-analysed data used as evidence.[114] The same could apply with respect to denying a request by the defendant to use the same AI system in the preparation of his or her defence. The right to adversarial proceedings likely requires access to, understanding of, and the ability to challenge an AI system's scientific validity, biases, and potential errors. However, intellectual property rights and trade secret laws may restrict this access. 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.

(iv) Access to court

75. Everyone has the right to have any claim relating to his "civil rights and obligations" brought before a court or tribunal.[115] An individual must "have a clear, practical opportunity to challenge an act that is an interference with his rights".[116] The practical and effective nature of this right may be impaired by, for instance, excessive formalistic interpretation of procedural rules.

76. Within that context, it can be argued that resorting to AI systems, such as ODR tools, should not hinder the right of access to a court within the meaning of Article 6[117] nor challenge human oversight over decision-making.[118] Access to court should also not be hindered by technical hurdles related to a specific AI system. In that respect, the Court has found that 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 had taken a formalistic approach that was excessive and conducive to a violation of Article 6§1.[119]

[Related rights]

77. Linked to the right to a fair trial are concerns relating to the right to liberty and security (Articles 5).

Right to liberty and security (Article 5 ECHR)

78. The key purpose of Article 5 is to prevent unlawful, arbitrary or unjustified deprivations of liberty.[120] In order to meet the requirement of lawfulness, detention must be "in accordance with a procedure prescribed by law" and based on a court order or a conviction decision. While flaws in a detention order do not automatically render detention unlawful, issues like insufficient reasoning are considered under Article

[114] 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.

[115] *Golder v. the United Kingdom*, no. 4451/70, 21 February 1975, § 36.

[116] *Bellet v. France*, no. 23805/94, 4 December 1995, § 38,

[117] See Resolution 2081 (2015) of the Parliamentary Assembly of the Council of Europe (PACE), "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), https://rm.coe.int/cepej-2023-19final-en-guidelines-online-alternative-dispute-resolution/1680adce33

[118] The right to human oversight is set out also in Article 9(1)(a) of Convention 108+.

[119] 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.

[120] *Selahattin Demirtaş v. Turkey* (no. 2) [GC], no. 14305/17, 22 December 2020, § 311.

5 § 1.[121] Deprivation of liberty is also unlawful if the conviction is the result of proceedings which amount to a “flagrant denial of justice”[122] by being “manifestly contrary to the provisions of Article 6 or the principles embodied therein”.[123] A trial that is summary in nature, which does not allow for a thorough and objective assessment of the case could thus amount to a violation of not only the right to a fair trial (Article 6), but also Article 5.[124]

79. 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

80. Courts and authorities involved in the administration of justice handle and retain personal data, including sensitive data whose misuse could lead to privacy breaches and discrimination. [125] Article 8 is violated when sensitive data is retained without adequate safeguards such as time-limits or a real possibility of review by the data subject.[126] To strike a fair balance between the need to make judicial decisions public and respect for the fundamental rights of parties or witnesses, information on their identity should not appear in published decisions.[127]

81. The general concerns on the risk of AI systems for privacy and data protection apply. Anonymisation or pseudoanonymisation 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, it has been suggested that these tools are not completely efficient.[128] The general concerns on the risk of AI systems for privacy and data protection apply.

Further reading

- CEPEJ, *European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment* (2018), https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c
- Resource Centre on Cyberjustice and AI, https://www.coe.int/en/web/cepej/resource-centre-on-cyberjustice-and-ai Detailed information on the deployment and usage of digital tools in administration of justice can be found in the individual country profiles
- Glossary on Cyberjustice and AI: https://www.coe.int/en/web/cepej/glossary-2
- On AI systems geared towards the private sector: *First Global Report on the State of Artificial Intelligence in Legal Practice*, 2023 https://globalailawreport.com/wp-content/uploads/2024/04/E-Book-First-Global-Report-on-AI-in-Legal-Practice.pdf

[121] *S., V. and A. v. Denmark* [GC], no. 35553/12, 36678/12, and 36711/12, 22 October 2018, § 92.
[122] *Othman (Abu Qatada) v. the United Kingdom*, no. 8139/09, 17 January 2012, § 260.
[123] *Willcox and Hurford v. the United Kingdom* (dec.), 2013, § 95; *Othman (Abu Qatada) v. the United Kingdom*, 2012, § 259; *Stoichkov v. Bulgaria*, 2005, §§ 51, 56-58.
[124] *Vorontsov and Others v. Ukraine*, 2021, §§ 42-49.
[125] Convention 108(+), Article 6.
[126] *S. and Marper v. the United Kingdom* [GC], 4 December 2008, nos. 30562 and 30566/2004, §103; *M.M. v. the United Kingdom*, 13 November 2012, no 24029/2007, §195
[127] 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*, 2013, § 45; *Z v. Finland*, 1997, § 97
[128] *Ethical Charter,* 2.3.1, §40: The volume and variety of information contained in court decisions, combined with the growing ease of cross-referencing with other databases, makes it impossible, in practice, to guarantee that the person concerned cannot be re-identified. In the absence of such a guarantee, these data cannot be qualified as anonymous and must therefore be subject to personal data protection rules.

- CEPEJ *Guidelines on electronic court filing (e-filing) and digitalization of courts* (2021), https://rm.coe.int/cepej-2021-15-en-e-filing-guidelines-digitalisation-courts/1680a4cf87
- CEPEJ *Guidelines on online alternative dispute resolution* (2023), https://rm.coe.int/cepej-2023-19final-en-guidelines-online-alternative-dispute-resolution/1680adce33, including good practices related to the Guidelines.
- CEPEJ *Information Note on the use of Generative AI by judicial professionals in a work-related context* (2024) https://rm.coe.int/cepej-gt-cyberjust-2023-5final-en-note-on-generative-ai/1680ae8e01
- PACE Resolution 2081 (2015) on *Access to Justice and the Internet: potential and challenges, https://pace.coe.int/en/files/22283/html*
- PACE Resolution 2342(2020) on *Justice by Algorithm – The Role of Artificial Intelligence in policing and criminal justice system* https://pace.coe.int/en/files/28805/html
- European Committee on Legal Cooperation, *Artificial Intelligence and Administrative Law,* Comparative Study (2022), https://www.coe.int/documents/22298481/0/CDCJ%282022%2931E+-+FINAL+6.pdf/4cb20e4b-3da9-d4d4-2da0-65c11cd16116?t=1670943260563

3.3.2 Healthcare

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

In healthcare these include a variety of applications[129] 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.

Key AI use cases include:

- *Medical imaging and diagnostics:* AI systems that can analyze medical images (X-rays, MRIs, CT scans…) to help diagnose health conditions.
- *Predictive Analytics*: AI systems used to predict patient outcomes, such as risk of disease and potential complications, by data analysis.
- *Personalized medicine*: AI systems that help tailor treatment plans to individual patients, optimizing drug therapies and medical interventions by analyzing 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.

Relevant human rights and principles

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

82. 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 under Article 8 ECHR 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[130], positive obligations require States to legislate or implement practical measures to protect individuals' health and lives and ensure they are informed of health risks[131], establish regulations compelling hospitals to safeguard patients' lives[132], and uphold high professional standards among healthcare providers.[133] 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.[134] Other Articles through which the Court approaches health issues are Article 2 (Right to life),[135] Article 3 (Prohibition of torture)[136] and Article 14 (Prohibition of discrimination).[137] In its case-law concerning health, the Court often refers to Convention 108,[138] the Oviedo Convention,[139] as well as other relevant instruments within the framework of the Council of Europe or beyond.[140]

83. The ESC explicitly guarantees the right to health (Article 11) and social and medical assistance (Article 13). Healthcare, and access to it, is a prerequisite for the preservation of human dignity.[141] States must provide accessible and effective healthcare by allocating resources, implementing operational procedures, and addressing vulnerable groups' specific needs.[142] Article 11 outlines three key obligations for States, either directly or in collaboration with public or private organisations (i) to take appropriate measures designed, *inter alia*, to remove as far as possible the causes of ill health, (ii) to provide advisory and educational facilities for the promotion of health and the encouragement of individual responsibility in matters of health; and (iii) to take appropriate measures to prevent as far as possible epidemic, endemic and other diseases, as well as accidents. States must protect vulnerable groups[143], such as the homeless, elderly, disabled, and those with irregular migration status, ensuring their right to health is not impeded, even under restrictions. Foreigners lawfully residing or working in a Party's territory are also covered under the ESC.

[130] *Vavricka and others v. the Czech Republic* [GC], 2021, §§ 274, 285

[131] *Brincat and others v. Malta*, 2014, § 101; *Guerra and others v. Italy* 1998, §§ 57-60; *Roche v. the United Kingdom* (GC), 2005, §§ 157-169; Mc Ginley and Egan v. the United Kingdom, 1998, §§98-104

[132] *Calvelli and Ciglio v. Italy* [GC], 2002, § 49; *Mehmet Ulusoy and Others v. Turkey*, 2019, § 90

[133] *Lopes de Sousa Fernandes v. Portugal* [GC], no. 56080/13, 19 December 2017, §§ 186-190.

[134] *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.

[135] *Center of Legal Resources on behalf of Valentin Campeanu v. Romania* [GC], 2014, §§ 145-147; Oyal v. Turkey, 2010, § 72

[136] *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.

[137] *Kiyutin v. Russia*, 2011, §§56-58, 74

[138] For instance, *S. and Marper v. the United Kingdom* [GC], 2008, §§ 41 and 103.

[139] *Glass v. the United Kingdom*, 2004, § 58.

[140] For instance, see 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) 2024, § 77, to the Universal Declaration on Bioethics and Human Rights adopted by UNESCO in 2005.

[141] International Federation of Human Rights Leagues (FIDH) v. France, Complaint No. 14/2003, decision on the merits of 3 November 2004, §31.

[142] Statement of Interpretation on the right to protection of health in times of pandemic, 21 April 2020.

[143] 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.

Right to Privacy and Data Protection

84. Article 8 ECHR protects health-related personal data.[144] 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.[145] 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. It seeks to ensure the principles of Convention 108, including its modernised version, are fully applied to the exchange and sharing of health-related data.

85. AI systems in healthcare may rely heavily on sensitive patient data, including medical records and biometric information, for decisions-making, predictions, training, testing and validation. Data security, confidentiality, and potential misuse, such as breaches or unauthorised sharing are among the concerns.[146] 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.[147]

Non-Discrimination and Equitable Access to Health Care

86. The ECHR and the ESC prohibit discrimination.[148] Under Article 3 of the Oviedo Convention, equitable access to health care of appropriate quality should be provided by the State.

87. Biased AI systems used to determine health needs and treatments may deprive a person of the necessary health care by underperforming for specific demographic groups due to the lack of sufficient representative data in their development. AI models trained predominantly on data from specific populations may misdiagnose conditions or underestimate illness severity in underrepresented groups.[149] An example includes prioritisation systems for kidney transplants, where biased historical data skewed outcomes against some patients.[150] Similarly, inadequate representation in training datasets has led to misdiagnoses of skin conditions.[151] 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

[144] *Surikov v. Ukraine*, no. 42788/06, 26 January 2017, §§ 70 and 89.

[145] As an example of a regional framework (that is also the domestic framework of the thirty Member States of the Council of Europe that apply it), see Articles 4 and 9 and Recitals 35 and 53 of the GDPR, with definitions of the terms “health data”, “genetic data”, “biometric data”.

[146] See also the CDBIO Report on the role of health professionals and healthcare providers in collecting, generating and enriching, 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.

[147] *Z. v. Finland*, no. 22009/93, 25 February 1997, § 95

[148] See the Preamble to the 1961 of the ESC and Part V-Article E of the RESC.

[149] See e.g., CDBIO Report p. 26; see also WHO, Ethics and governance of artificial intelligence for health (2021), pp. 54-57 www.technologyreview.com/2019/10/25/132184/a-biased-medical-algorithm-favored-white-people-for-healthcare-programs; www.weforum.org/stories/2024/02/racial-bias-equity-future-of-healthcare-clinical-trial.

[150] See, e.g., www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients; https://algorithmwatch.org/en/racial-health-bias-switzerland.

[151] See, e.g., www.theguardian.com/society/2021/nov/09/ai-skin-cancer-diagnoses-risk-being-less-accurate-for-dark-skin-study.

given country, or dependent on the financial means of the patients.[152] States should adopt measures to ensure AI systems are developed and deployed equitably, with representative training data and safeguards against bias.

Informed Consent, Autonomy and Decision-Making

88. Informed consent and autonomy in decision-making of the patient[153] is guaranteed under Article 8 ECHR.[154] 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.[155]

89. Informed consent and patient autonomy call for information, explanation, and transparency, which may not be readily provided, considering AI's "black box" problem, relevant not only for the patient but for the health professional as well.[156] Arguably, the right to decision-making would include being able to opt for care by a human doctor over an AI-enabled chatbot or being able to opt for diagnostic tools not involving AI, especially in view of the therapeutic nature of the 'patient-doctor' relationship which is inherently human.[157] Should AI becomes integral to medical practice, patient autonomy may be compromised if non-AI alternatives are unavailable or if health professionals lose the ability to provide care independently due to reliance on AI systems and subsequent de-skilling caused by handing over responsibility for such functions to AI.[158]. In addition to undermining the patient's autonomy, over-reliance on AI systems and the ensuing automation bias may result in the loss of the patient-doctor relationship, de-personalisation of health care[159] and, consequently, in interference with the patient's right to quality health care and his or her right to physical, moral and psychological integrity.

Further reading

- CDBIO, *Report on the Application of Artificial Intelligence in Healthcare and its impact on the "Patient-Doctor" Relationship* (2024), https://www.coe.int/en/web/bioethics/-/report-on-the-application-of-ai-in-healthcare
- *Strategic Action Plan on Human Rights and Technologies in Biomedicine (2020-2025),* 2019, https://rm.coe.int/strategic-action-plan-final-e/1680a2c5d2

[152] 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 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.

[153] 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 (CDBIO Report p. 13).

[154] *Trocellier v. France* (dec.), no. 75725/01, § 4; *Mayboroda v. Ukraine*, no. 14709/07, § 52.

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

[156] On trustworthiness in the professional standards which scrutinize the safety, quality and efficacy of AI systems, human oversight and the explainability of AI outputs, see CDBIO Report p. 28

[157] AI systems (e.g. health checker apps) are unlikely to discern a patient's symptoms where underlying (hidden, unquantifiable) causes are at play (e.g. psychological, social, cultural) which require a greater understanding and trust building process for them to manifest. See CDBIO Report p. 25

[158] CDBIO Report p. 14

[159] 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.

- Recommendation CM/Rec (2019)2 of the Committee of Ministers to Member States on the "*Protection of health-related data*", https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html
- PACE Recommendation 2185 (2020), *Artificial intelligence in healthcare: medical, legal and ethical challenges ahead*, https://pace.coe.int/en/files/28813/html
- Gender Equality Commission and Steering Committee on Anti-discrimination, Diversity and Inclusion, *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) https://edoc.coe.int/en/artificial-intelligence/11649-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.html
- WHO, *Ethics and governance of artificial intelligence for health* (2021) https://www.who.int/publications/i/item/9789240029200
- WHO *Ageism in artificial intelligence for health* (2022) www.who.int/publications/i/item/9789240040793.
- WHO, *Ethics and governance of artificial intelligence for health, Guidance on large multi-modal models* (2024) https://www.who.int/publications/i/item/9789240084759
- UNEP, *Navigating New Horizons, A global foresight report on planetary health and human well-being* (2024), https://www.unep.org/resources/global-foresight-report

3.3.3 Social services and welfare

90. Social services encompass a broad range of programs and services designed to promote human and societal well-being. Along with basic public services such as access to education and health care, discussed in the respective chapters of this Handbook, social services and welfare include pecuniary and non-pecuniary assistance in the form of social security (programs that provide financial support for the elderly, the disabled and survivors based on workers' contributions); unemployment benefits; housing assistance (subsidies or social housing), and support for the homeless or those at risk of homelessness; 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

91. This sector includes various AI applications, from automating routine tasks like notetaking and case management to those with significant impacts, such as:

- *Predictive analytics:* AI systems that can analyse large datasets and use algorithmic processes, including machine learning, to predict which individuals or groups are most at risk of needing social services, allowing agencies to proactively provide support and resources; for instance, systems that aim to identify children at risk and in need of additional help.
- *Resource allocation:* AI systems that use machine learning to optimize the distribution of the usually limited resources.
- *Screening and fraud detection*: AI systems designed to assist social workers in screening applicants, verifying information, flagging potential issues and identifying patterns suggestive of fraud or misuse of welfare services.
- *AI-driven chatbots and virtual assistants*: Systems that provide a wide range of services, from handling routine inquiries and providing information, to enhancing accessibility for people with disabilities through speech recognition or automated transcription services, to monitoring an individual's physical and mental condition, providing alerts and ensuring timely interventions.
- *Overview and Evaluation:* AI systems that are used to evaluate the effectiveness of social services by analysing data on outcomes, with a view to assisting agencies refine and improve their performance over time.

Relevant human rights and principles

92. The provision of social services may directly interfere with an individual's enjoyment of his or her rights, such as the right to family life within the meaning of Article 8 of the ECHR,[160] the right to liberty within the meaning of Article 5,[161] or the right to property within the meaning of Article 1 of Protocol no. 1.[162] In

[160] 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, 37956/11, §§ 58-60. Also see for obligations of national authorities to facilitate family visits and, in exceptional cases, to secure shelter for particularly vulnerable individuals *A and Others v. Italy*, 7 December 2003, 17791/22, §§ 93-104.

[161] For instance, with respect to the compulsory confinement of persons of "unsound mind". See, among others, *Ilnseher v. Germany* [GC], 4 December 2018, 10211/12 and 27505/14, §§ 126-134.

[162] For a comprehensive synopsis of the Court's case-law relating to social security/welfare benefits see *Béláné Nagy v. Hungary* [GC], 13 December 2016, 53080/13, §§ 80-89; *Yavaş and Others v. Turkey*, 5 March 2019, 36366/06, §§ 39-43.

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).[163]

93. States have a margin of appreciation in spheres involving the application of social or economic policies.[164] The Court will also generally respect domestic policy choices unless they are "manifestly without reasonable foundation".[165] This is particularly so in the context of the allocation of limited State resources.[166] 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.[167] This means that where a State decides to provide such benefits, it must do so in a non-discriminatory manner (Article 14). 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, gender, nationality or disability, and "very weighty reasons" would be required to justify the difference of treatment at issue.[168]

94. The ESC obligates States Parties to ensure non-discriminatory access to social security,[169] social and medical assistance,[170] and social welfare services[171]. It requires that a social security system guarantees effective access to benefits provided under each branch.[172] 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.[173]

Right to Privacy and Data Protection

95. 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.[174] For example, concerns related to compliance with Article 8 ECHR have been raised in the "SyRi" case, where the Hague District Court has 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.[175]

[163] See, among others, *Z. and Others v. the United Kingdom,* 10 May 2001, no. 29392/95, §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, 54227/14, §89. Also, with respect to the failure to protect victims of domestic violence, see *Opuz v. Turkey,* 9 June 2009, 33401/02, §159; *Talpis v. Italy,* 2 March 2017, 41237/14, § 141, also in conjunction with Article 14 and the State's failure to guarantee the right of women to equal protection before the law.

[164] For instance, regarding housing, see, among others, *Hudorovič and Others v. Slovenia*, 10 March 2020, 24816/14 and 25140/14; regarding old-age pensions, *Fábián v. Hungary*, 5 September 2017, 78117/13, § 67; regarding survivors' pensions, *Muñoz Díaz v. Spain*, 8 December 2009, 49151/07, §§ 48-49, etc.

[165] *Stec and Others v. the United Kingdom* [GC], 12 April 2006, 65731/01 and 65900/01, § 52.

[166] *Šaltinytė v. Lithuania*, 26 October 2021, 32934/19, §§ 64 and 77.

[167] *Bah v. the United Kingdom*, 27 December 2011, 56328/07, § 52.

[168] *Savickis v. Latvia* [GC], 9 June 2022, 49270/11, § 83; *J.D. and A. v. the United Kingdom*, 24 October 2019, 32949/17, 34614/17, §§ 88-89, 97 and 104; *Andrejeva v. Latvia* [GC], 18 February 2009, 55707/00, § 87; *Ribać v. Slovenia*, 5 March 2018, 57101/10, § 53.

[169] ESC, Article 12; see also Digest of Case Law of the European Committee of Social Rights, December 2022, p. 119 ff.

[170] ESC, Article 13.

[171] ESC, Article 14.

[172] Digest of Case Law of the European Committee of Social Rights, December 2022, p. 120.

[173] ESC Article 12(4); Paragraph 1 of the Appendix of the ESC.

[174] *Szabó and Vissy v. Hungary*, no. 37138/146, June 2016, § 70.

[175] 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". It is worth noting that the United Nations Special

96. 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

97. 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. This may lead to unfair denial of services or benefits, disproportionately affecting marginalised groups and undermining equal access to these services. Predictive analytics, fraud detection and resource allocation systems are especially vulnerable to 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 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, unless there are safeguards, including human oversight, ensuring the critical evaluation of AI outputs and thus neutralising the risk of discriminatory effects.[176]

98. The Court has found that State authorities are under a duty to take all reasonable measures to ascertain through an independent body whether certain treatment was influenced by a discriminatory attitude and carry out an effective investigation in this regard.[177]

Transparency and Accountability

99. 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).

100. 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. In cases where the events in issue lie wholly, or in large

Rapporteur on Extreme Poverty and Human Rights submitted an *amicus curiae* brief stressing in particular the discriminatory and stigmatizing effect of SyRi, that targeted mostly the poor and other vulnerable groups, or, as the State admitted in the hearings, “problem districts”. https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf

[176] 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, a civil servant was responsible for manually reviewing the highest risk score applications, though without being given any information as to why the system had given a particular application a high-risk score to a specific application. However, civil servants have been observed to be prone to apply generalizations to the behavior of individuals of the same race or ethnicity perceiving them stereotypically as fraudulent or deviant.

[177] *Basu v. Germany*, 215/19, 18 October 2022, §38.

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.[178]

Accessibility and Quality of Care

101. Vulnerable groups such as the elderly, 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.

102. 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 than the one recommended by the system. AI systems are however not error-proof,[179] and errors in welfare can be fatal for some of the most vulnerable members of our societies. 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

- Council of Europe, *Social Security as a human right,* Human Rights Files no. 23, 2007
- 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, https://rm.coe.int/168046ccea
- 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),https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680649301
- Report of the Special Rapporteur on extreme poverty and human rights on the "privatization of public services", United Nations General Assembly document A/73/396, 26 September 2018
- Report of the Special Rapporteur on extreme poverty and human rights on the "digital welfare state", United Nations General Assembly document A/74/493, 11 October 2019
- Amnesty International, Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal, 2021, https://www.amnesty.org/en/documents/eur35/4686/2021/en/
- GEC and CDADI, *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,*

[178] *Salman v. Turkey* [GC], 27 June 2000, 21986/93, § 100; *Anguelova v. Bulgaria*, 13 June 2002, 38361/97 § 111; *Cînţa v. Romania*, 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.

[179] 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".

Prepared by Ivana Bartoletti and Raphaële Xenidis, 2023, https://edoc.coe.int/en/artificial-intelligence/11649-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.html