CDDH-IA(2025)10
28/03/2025

STEERING COMMITTEE FOR HUMAN RIGHTS

COMITÉ DIRECTEUR POUR LES DROITS HUMAINS

(CDDH)

DRAFTING GROUP ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

GROUPE DE RÉDACTION SUR LES DROITS HUMAINS ET L'INTELLIGENCE ARTIFICIELLE

(CDDH-IA)

Compilation of comments received on the [DRAFT] Handbook on human rights and artificial intelligence

Chapters I, II and III

Compilation des commentaires reçus sur [EBAUCHE] Manuel sur les droits humains et l'intelligence artificielle

Chapitres I, II et III

TABLE OF CONTENTS / *TABLE DES MATIÈRES*

MEMBERS / *MEMBRES*

CZECHIA / *TCHEQUIE*

2.2 Further technical concepts relevant for AI and human rights

Commented [MK1]: Although we mention principle of „Accountability“ in multiple places in the document as one of the basic principles related to the use of AI systems, it seems we do not explain its content.

We suggest adding a brief explanation (here or somewhere else) that according to this principle „all AI actors should be accountable for proper functioning of AI systems and for the respect of other principles“.“(see OECD AI principles, available here: https://oecd.ai/en/dashboards/ai-principles/P9)

We could also recommend that regular audits of AI systems (for example their algorithms) and due process considerations are appropriate in this regard.

2.2.1 Transparency

18. Transparency refers to openness and clarity in the governance of activities within the lifecycle of AI systems. It means that the decision-making processes and general operation of AI systems should be understandable and accessible to appropriate AI actors and, where necessary and appropriate, relevant stakeholders.[1]

3.3.4 Law Enforcement and Public Security

131. This sector involves police,[2] intelligence and assimilated services[3], including such issues as identification of individuals for law enforcement purposes, crime prevention, crime investigation, programmes regarding protection of persons in danger (e.g. victims of domestic violence or protected witnesses), arrests and detentions, prison and probation crowd management during public events and maintenance of public order, counterterrorism, national security operations, measures entailing surveillance of communications, restrictions, bans, prohibitions, lockdowns, various forms of supervision including those affecting the freedom of movement.

Commented [MK2]: Although we correctly mention the freedom of movement (Art 2 P4 to the Convention), it is not part of relevant human rights and principles in § 132 (see below).

We suggesting adding the freedom of movement in §§ 132 and 134. The ECtHR´s approach is more or less the same as in case of Articles 8-11 (i.e. legitimate aims, necessity etc.).

Key AI use cases

- *Digital forensics*: Several tools and techniques for data recovery and analysis have been developed with AI components. These tools can recover deleted files, access data from damaged devices, restore fragmented pieces of information into coherent formats and investigate the digital footprint of criminals.
- *Surveillance systems*: technologies such as image classification, computer vision and biometrics including automated facial recognition, fingerprints or biometric categorisation.
- *Data analytics and predictive policing*: employing statistical methods to extract insights from vast datasets, for instance on crime records, events and environmental factors identified in criminological insights and also unstructured data originating from open-source intelligence and social media intelligence sources.
- *Natural language processing:* performing tasks through processing textual data, such as text classification and clustering, text summarization and machine translation.

Commented [MK3]: It seems there are also AI powered tools created for decrypting data. We suggest adding „decryption“ here. In Podchasov case, the ECtHR stated that the obligation to retain the applicant´s internet communications and related data, to allow the authorities access to that information upon request, **and to facilitate decryption**, constituted an interference with the applicant's rights under Article 8 of the Convention (see Podchasov v. Russia, no. 33696/19, judgment of the European Court of Human Rights of 13 February 2024)

Commented [MK4]: We suggest adding the word „voice“ recognition here.

Relevant human rights and principles

[1] See the Explanatory Report to the Framework Convention, § 57.

[2] Police refers to traditional police forces or services and other publicly authorised and/or controlled services granted responsibility by a State, in full adherence to the rule of law, for the delivery of policing services.

[3] Government departments or units that are considered equivalent to the intelligence services in terms of their function.

132. The use of AI systems in law enforcement and public security could present particular human rights risks. This is because of the strong human rights impact of decisions that might be taken based on AI systems output such as surveillance, search and seizure, or arrest and detention. The use of AI systems in this sector may interfere with Articles 5 (Right to liberty and security), 8 (Right to respect for private and family life), 10 (Freedom of expression), and 11 (Freedom of assembly and association) of the ECHR. States may justify interference with Articles 8, 10 and 11 ECHR by the legitimate aims listed in the texts of these articles which include national security, public safety, or the prevention of disorder or crime.

Commented [MK5]: We suggest adding the words „actions or" here. Just to be coherent - see the wording in § 133 below. Decisions may also imply outcome of the formal process while actions are less formal.

3.3.5. Immigration and Border Control

148. This sector includes activities relating to border control, conditions and modalities of entrance to and removal from the territory of the State, including issuance of visas, expulsion and deportation, asylum and refugee status and adjustments of status, translation/interpretation services, production of transcripts, collection and assessment of evidence.

Commented [MK6]: We suggest adding the words „residence permits" here.

152. The use of AI systems in immigration and border control may raise issues under Article 8 (Respect for private and family life), Article 14 (Non-discrimination), and Article 13 (Effective remedy) ECHR.

Commented [MK7]: We suggest adding the words „Article 1 Protocol no. 7 (Procedural safeguards relating to expulsion of aliens). This article specifically affects the rights of foreigners. Although the ECtHR has not yet addressed any case in connection with the use of AI systems, this probably cannot be ruled out in the future. We find it odd not mention this article here.

Right to Privacy and Data Protection

153. Member States are obliged to respect the rights under Article 8 of non-nationals who find themselves within the State's jurisdiction. Although the protection afforded by Article 8 is not absolute, any restriction must have a clear legal basis with appropriate safeguards; it must be necessary and proportionate to a legitimate aim; and must be non-discriminatory. While surveillance might be necessary to ensure national security and other legitimate aims, measures should not disproportionately infringe on individual rights.[4] Convention 108(+) too allows exceptions, such as for national security and public safety, but requires strict safeguards to ensure that any exceptions remain necessary and proportionate and are subject to independent and effective review and supervision under the domestic legislation of the respective Party.[5]

154. The use of AI systems for border management, such as AI-powered drones, facial recognition and predictive analytics using personal data, could result in excessive technology-enabled surveillance of individuals.[6] The protection of Article 8 extends to personal data including electronic data[7] and biometric data.[8] Blanket and indiscriminate retention of biometric data has been found to be incompatible with the right to respect for private life.[9] Biometric data is considered as sensitive data[10] and may reveal additional personal characteristics, such as ethnicity, health conditions, or disabilities. As a result, special protection is necessary to prevent misuse which could lead to discrimination. AI system-based identification and

Commented [MK8]: We suggest adding the word „sensors" here.

[4] *Glukhin v Russia*, § 90; UNHRC, Report 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020) UN Doc A/HRC/44/24; UNGA n(11) para 1.
[5] Ibid.
[6] UNHRC, Report 'Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants' (2020) UN Doc A/HRC/45/9; UNGA, Report 'Contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2020) UN Doc A/75/590;
[7] *S. and Marper v UK* App Nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008)
[8] See among many others *Van der Velden v. the Netherlands* (dec.), No. 29514/05, 7 December 2006; *Schmidt v. Germany* (dec.), No. 32352/02, 5 January 2006; *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008; *Canonne v. France* (dec.), No. 22037/13, 2 June 2015; *Gaughran v. the United Kingdom*, No. 45245/15, 13 February 2020; *Dragan Petrović v. Serbia*, No. 75229/10, 14 April 2020; *McVeigh, O'Neill and Evans v. the United Kingdom*, Nos. 8022/77, 8025/77, and 8027/77, Commission decision of 18 March 1981; *Allan v. the United Kingdom*, No. 48539/99, 5 November 2002; *Doerga v. the Netherlands*, No. 50210/99, 27 April 2004; *Vetter v. France*, No. 59842/00, 31 May 2005; *Wisse v. France*, No. 71611/01, 20 December 2005.
[9] *S. and Marper v the United Kingdom*, § 125.
[10] Convention 108+, Article 8.

verification systems relying on fingerprints, iris scans, and facial recognition pose risks particularly when biometric data is collected, stored, or used without sufficient safeguards.

155. AI systems may generate errors, particularly when screening ordinary traveller data for security purposes such as to detect suspected terrorists or criminals. These systems process vast datasets from multiple sources (police, intelligence, border authorities), often without individuals knowing they are included[11] and often include interoperable databases that share fingerprints and biometrics between police and border control agencies. Under such circumstances oversight and the possibility to challenge wrongful inclusion and request rectification could be hampered. Wrongful inclusion in terrorism watchlists has serious human rights implications for the individual concerned.[12] Depending on the specific measures triggered by an alert from a watchlist (e.g., a travel ban, denial of entry or stay, questioning, surveillance or even arrest) it may, in turn, impact a broad range of rights, including freedom of movement, privacy, the right to liberty, the right to a fair trial. It can also directly or indirectly affect a spectrum of civil, political, economic, social and cultural rights of family members, including children, and associates of those listed. To avoid wrongful identification of travellers as suspects or persons posing terrorism-related threats, the relevance of individual results of automatic assessments should be carefully examined by a person in a non-automated manner.[13] Officers conducting such examination should be adequately trained and sensitised to potential bias and the implications of erroneous risk identification for the people concerned.

Commented [MK9]: We could add a sentence here explaining that the AI systems may overlook persons in vulnerable situations (for examples victims of human trafficking, etc.).

3.3.7 Education

Commented [MK10]: There seems to be no mention of the risks of reduced human interaction. We could discuss whether it should be included here or not. The idea is that relying on modern technologies, including AI systems, may reduce the teacher-to-student interactions and relationships and take away from the social-emotional aspects of learning. If those interactions diminish, students´ social skills and interpersonal development may diminish as well. On the other hand, automating administration (for example lesson planning, grading, and maintaining records) may free up teachers´ time to spend more time building relationships with students and fostering their social growth.

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

GERMANY / *ALLEMAGNE*

133. This Handbook on Human Rights and Artificial Intelligence (‘Handbook’) has been designed as an accessible tool primarily to support government officials and policymakers in Council of Europe member States in applying ECHR, ESC and other relevant standards to AI-related challenges and opportunities. Given the diverse audience of policymakers and government officials working across various areas of public governance, this Handbook does not assume extensive prior knowledge of human rights law or AI-related issues. Nor does it aim to provide an exhaustive analysis of every topic addressed. As a practical resource, it provides insights into how these standards, along with instruments like the Framework Convention, may apply to activities in AI systems’ lifecycle. Focusing on key AI use cases in public governance, both current and reasonably foreseeable, it offers a framework to assess AI's human rights impacts considering ECHR and ESC standards, without predicting specific outcomes of future cases.[14]

Commented [PL11]: GER: We suggest to consider also the positive impact (see also further comments and suggestions in the sectoral analysis)

20. “Explainability” therefore refers to the capacity to provide, subject to technical feasibility and taking into account the generally acknowledged state of the art, sufficiently understandable explanations about

[11] OSCE Policy Brief, Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021). p. 27.
[12] *Nada v. Switzerland* [GC], No. 10593/08, ECHR 2012.
[13] Council of Europe Consultative Committee of Convention 108, “Opinion on the Data protection implications of the processing of Passenger Name Records”, Strasbourg, 19 August 2016, p. 8.
[14] 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.

why an AI system provides information, produces predictions, content, recommendations or decisions.[15] This seems to be of special importance for AI applications in the fields of medicine, where “explainability” together with reliability provides the ground for informed consent.

Commented [PL12]: GER: We suggest to add this aspect.

Key AI use cases

108. Major technological breakthroughs in AI systems, have the potential to advance biomedicine and benefit healthcare, yet uncertainty exists about their impact and direction of developments. AI systems are being developed for a variety of applications,[16] encompassing ancillary applications, such as the automation of routine administrative tasks, but also applications of significant impact on the provision of quality health services and a patient’s treatment, that are regulated as medical devices in most jurisdictions, such as in radiology imaging.

Commented [PL13]: GER: This should be clarified

109. Key AI use cases include:

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

Commented [PL14]: GER: We suggest to add this use case

111. The ESC explicitly guarantees the right to health (Article 11) and the right to social and medical assistance (Article 13). Access to healthcare is a prerequisite for preserving human dignity.[17] States must ensure that healthcare services are accessible, effective, and inclusive by allocating sufficient resources, implementing robust operational procedures, and addressing the specific needs of vulnerable groups.[18] Integrating trustworthy AI systems into healthcare delivery can support states in achieving these aims. Article 11 imposes three key obligations on States, either directly or in collaboration with public or private organisations: ~~(i)~~ to take appropriate measures to (i) eliminate, as far as possible, the causes of ill health, (ii) to provide advisory and educational facilities that promote health and encourage individual responsibility; and (iii) ~~to take implement measures~~ to prevent, as far as possible, epidemic, endemic, and other diseases, are further required to protect vulnerable groups,[19] such as the homeless, elderly, disabled, and those with

Commented [PL15]: GER: We suggest to also mention the opportunities of AI in this regard.

[15] Framework Convention Explanatory Report, § 60.

[16] 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.

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

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

[19] *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.

irregular migration status, ensuring their right to health remains uncompromised, even under restrictive conditions. Additionally, foreigners lawfully residing or working in a Party's territory are entitled to health protection under the ESC.

Non-Discrimination and Equitable Access to Health Care

115. Unwanted ~~B~~biases in the data used to develop ~~and train~~ AI systems may skew the assessment of health needs and treatments for patients and thereby perpetuate or exacerbate existing biases. It is notable that AI models trained predominantly on data from specific populations may misdiagnose conditions or underestimate illness severity in underrepresented groups such as women and girls, persons belonging to ethnic minorities, indigenous populations, the elderly or persons with disabilities.[20] Examples include prioritisation systems for kidney transplants, where biased historical data skewed outcomes against some patients.[21] Similarly, inadequate representation in training datasets has led to misdiagnoses of skin conditions.[22] In addition, there is concern that access to the benefits offered by AI in healthcare may not be equally available to all. The deployment of such care may be geographically uneven across a given country, or dependent on the financial means of the patients.[23] A lack of accessible design of AI applications may exclude elderly or disabled persons. States should adopt measures to ensure AI systems are developed and deployed equitably~~, with representative training data and safeguards against bias~~. The presence of adequate frameworks to use large and representative health datasets for secondary purposes, such as quality assurance, research and development, including AI training, is therefore imperative to detect existing biases in healthcare and mitigate potential biases when integrating AI into medical decision making. Furthermore, AI offers many ways to support making healthcare delivery and society as a whole more inclusive, including bridging language barriers or converting speech to text for persons with disabling hearing loss.

Commented [PL17]: GER: We suggest to add this aspect.

Commented [PL18]: GER: We suggest to add this aspect.

117. Individuals must be able freely to give or refuse their consent to any intervention, comprising all medical acts including those performed for the purpose of preventive care, diagnosis, treatment, rehabilitation or research. Their consent is considered to be free and informed when it is given on the basis of objective information from the responsible health care professional which includes adequately answering to requests for additional information. The "black box" nature of many AI systems which render probabilistic results makes it difficult to sufficiently understand and weigh up the necessity or usefulness of the intervention. ~~This is a challenge for individuals to make a decision on consent.~~ Thus, apart from transparency and explainability requirements, reliable data on and standards for the AI's actual behavior (safety and performance) is necessary for achieving informed consent. ~~This is also a challenge for doctors responsible for interpreting the results of AI systems~~. Currently, this presents a systemic hindrance for providing reliable information that is needed as a foundation for a truly informed consent, a challenge for

[20] See, e.g., CDBIO Report p. 26; see also WHO, Ethics and governance of artificial intelligence for health (2021), pp. 54-57. Further on the underrepresentation and low quality of data of women, as well as gender diverse persons in scientific research, the GEC/CDADI Study, p. 25. Also (p. 26) on the structural discrimination embedded in AI systems with respect to systematically disadvantaged patients with ethnic minority backgrounds. Furthermore, see WHO, *Ageism in artificial intelligence for health* (2022), showing that algorithmic systems used in the healthcare sector are trained on the data of predominantly younger populations, leading to disproportionately lower performance of these systems for older patients, including incorrect diagnosis www.who.int/publications/i/item/9789240040793.

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

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

[23] 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.

individuals to make a decision on consent and for doctors responsible for interpreting the results of AI systems[24] ~~Furthermore, without a~~Adequate transparency and oversight requirements for AI systems and their developers ~~and the~~ as well as education and training of doctors using them might mitigate this.~~,~~ ~~there are c~~Concerns about the ~~'de-skilling' of health professionals and the~~ de-personalisation of the patient-doctor relationship require attention. [25] At the same time, with its capability to translate and accommodate for a patient's prior knowledge and beliefs, generative AI tools have the potential to improve the processes to inform patients and thereby aid them in reaching an informed decision.

Commented [PL19]: GER: We suggest to add this positive aspect.

Key AI use cases

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

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

Commented [PL20]: GER: We suggest a more open wording.

135. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8[26] and the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned.[27] The fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, has no bearing on that finding.[28] A surveillance measure will generally involve an interference in private life.[29]

Commented [PL21]: GER: This could be understood to mean that risks of misuse or, conversely, measures for organizational and technical data security are irrelevant for the weighting of interventions. This not correct (cf. § 67 of the cited judgment)

141. As for the collection of (biometric) personal data with facial recognition technology, minimum safety measures regarding the duration, storage, usage and destruction of personal data are required to ensure appropriate safeguards. While the need to use modern technologies in states' efforts to fight against crime,

[24] 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

[25] 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.

[26] *Leander v. Sweden*, No. 9248/81, 26 March 1987, § 48.

[27] *S. and Marper v. UK*, § 103.

[28] *S. and Marper v. UK*, §§ 67 and 75.

[29] *Amann v. Switzerland* [GC], No. 27798/95, §§ 69-70, ECHR 2000-II; *Leander v. Sweden*, No. 9248/81, 26 March 1987, Series A No. 116.; *Kopp v. Switzerland*, 25 March 1998; *Rotaru v. Romania* [GC], No. 28341/95, §§ 43-44, ECHR 2000-V; *McGinley and Egan v. the United Kingdom*, 9 June 1998, § 101.

and in particular against organised crime and terrorism is beyond dispute,[30] in *Glukhin v Russia* the authorities' use of facial recognition technology to investigate the applicant violated his right to respect for private life (Article 8) and freedom of expression (Article 10). Although the police measures were based on domestic law, there were no adequate and effective guarantees against abuse. Moreover, the personal data processed contained information about the applicant's participation in a peaceful protest and therefore revealed his political opinions. Personal data revealing political opinions fall within the special category of sensitive data attracting a heightened level of protection.[31] In the context of implementing facial recognition technology, it is essential to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards is greater where there is use of live facial recognition technology.[32] In addition to the Article 8 concerns, the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect in relation to the rights to freedom of expression (Article 10 ECHR) and assembly (Article 11 ECHR).[33]

~~19.~~ The Guidelines on facial recognition of the Council of Europe[34] provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect human rights. It emphasises that the use of facial recognition, must have a lawful basis, as per Article 6 of Convention 108+. Special safeguards should be established in domestic law, ensuring that any use is proportionate to the legitimate aim pursued. The necessity and proportionality of facial recognition must be carefully assessed, and a legal framework should define its various applications. This includes criteria such as the purpose of use, algorithm reliability, data retention, auditability, traceability, and safeguards. The use of facial recognition to determine attributes like skin colour, religion, sex, ethnicity, or health should be prohibited unless appropriate legal safeguards exit to prevent discrimination. Specific rules should be set for law enforcement use, restricting biometric data processing in controlled and uncontrolled environments to strictly necessary and proportionate purposes.

142. AI systems driven **surveillance technologies**, including biometric monitoring and behaviour-tracking may be used also to enhance **prison security**. Placing a person under permanent video surveillance whilst in prison – which already entails a considerable limitation on a person's privacy – has to be regarded as a serious interference with the right to respect for privacy, as an element of the notion of "private life" (Article 8 ECHR).[35] Recommendation CM/Rec(2024)5 **regarding the ethical and organisational aspects of the use of AI and related digital technologies by prison and probation services** emphasises that the use of such systems for maintaining safety, security and good order should be strictly necessary, proportionate to the purpose and should avoid any negative effects on the privacy and well-being of offenders and staff. The use of AI systems in monitoring should be proportionate to the purpose and used only when strictly necessary. The human-centred approach should remain a key element in decision taking for offender management, risk assessment, rehabilitation and reintegration. Under no circumstances should the use of AI systems cause intentional physical or mental harm or suffering to a person.

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

[30] *Glukhin v. Russia*, No. 12317/16, 4 July 2023, § 85.
[31] Ibid, § 76 and 86.
[32] Ibid., § 82.
[33] Ibid., § 88.
[34] Adopted by the Consultative Committee of the Convention 108 in 2021.
[35] *Vasilică Mocanu v. Romania*, No. 43545/13, 6 December 2016.

opaque, biased, or be prone to errors. As such, ensuring compliance with Articles 8, 10, and 11 may require beyond traditional safeguards additional measures tailored to address issues of algorithmic bias, transparency, explainability and interpretability, and accountability. AI systems-based surveillance should be grounded in accessible and foreseeable legislation, pursue a legitimate aim, and include robust oversight, including judicial protection where appropriate, to protect the right to respect for private life (Article 8), freedom of expression (Article 10), and freedom of assembly and association (Article 11). Facial recognition technologies, especially real-time systems, require heightened safeguards against abuse and chilling effects on freedom of expression and assembly. Member States should provide clear rules, independent scrutiny, and effective remedies to prevent arbitrary or unlawful surveillance practices that risk violating human rights and the principles of human dignity and personal autonomy. ~~Where necessary, this~~

152. The use of AI systems for border management, such as AI-powered drones, facial recognition and predictive analytics using personal data must be based on a legal basis and be proportionate~~, could result in excessive technology-enabled surveillance of individuals~~.[37] The protection of Article 8 extends to personal data including electronic data[38] and biometric data.[39] Blanket and indiscriminate retention of biometric data has been found to be incompatible with the right to respect for private life.[40] Biometric data is considered as sensitive data[41] and may reveal additional personal characteristics, such as ethnicity, health conditions, or disabilities. As a result, special protection is necessary to prevent misuse which could lead to discrimination. AI system-based identification and verification systems relying on fingerprints, iris scans, and facial recognition pose risks particularly when biometric data is collected, stored, or used without sufficient safeguards.

153. AI systems may generate errors, particularly when screening ordinary traveller data for security purposes such as to detect suspected terrorists or criminals. These systems often process vast datasets from multiple sources (police, intelligence, border authorities)~~,~~ and are interoperable. Individuals often do not know ~~without individuals knowing~~ they are included[42] ~~and often include interoperable databases that share fingerprints and biometrics between police and border control agencies~~. Under such circumstances oversight and the possibility to challenge wrongful inclusion and request rectification could be hampered. Wrongful inclusion in terrorism watchlists has serious human rights implications for the individual concerned.[43] Depending on the specific measures triggered by an alert from a watchlist (e.g., a travel ban, denial of entry or stay, questioning, surveillance or even arrest) it may, in turn, impact a broad range of rights, including freedom of movement, privacy, the right to liberty, the right to a fair trial. It can also directly or indirectly affect a spectrum of civil, political, economic, social and cultural rights of family members, including children, and associates of those listed. To avoid wrongful identification of travellers as suspects or persons posing terrorism-related threats, the relevance of individual results of automatic assessments should be carefully examined by a person in a non-automated manner.[44] Officers conducting such examination should be adequately trained and sensitised to potential bias and the implications of erroneous risk identification for the people concerned.

155. Decisions based on information from AI systems may result in unlawful discrimination, including indirect and intersectional discrimination, due to bias in AI systems. In addition, technologies such as facial recognition systems that use biometric data have been described as inherently fallible since they inevitably rely on statistical probabilities and are prone to inaccuracy and errors.[45] While this issue is not exclusively related to migration, the consequences for migrants' and refugees' rights can be significant. If AI systems based facial recognition technologies are used for identification and identity verification at pre-departure or on arrival at borders, some individuals may be more exposed to inaccuracies and misidentification due to their protected characteristics. A combination of personal information about a person, as is used in visa and travel authorization systems, may also reveal protected characteristics AI-assisted decision-making tools that analyse face, speech, dialect recognition, name transliteration, or mobile phone data in visa and travel authorization systems could inadvertently reveal protected characteristics, increasing the risk of biased assessments and unequal treatment and their misuse could lead to discriminatory profiling. If such mistakes are not corrected, misidentified individuals may be denied entry, resulting in discriminatory decisions ~~potentially~~ that might have an impact on the right guaranteed by ~~impacting the right to liberty of movement (~~Article 2 Protocol 4 (Freedom of movement). Any measure restricting that~~e~~ right ~~to liberty of movement~~ must pursue one of the legitimate aims [46] referred to in paragraph 3 of Article 2 of Protocol No. 4 and strike a fair balance between the public interest and the individual's rights.[47]

Commented [PL23]: GER: Please change this language, as there does not exist a universal "right to liberty of movement" across borders. Protocol no 4 only provides for such rights (1) for movement within a country to persons which are rightfully staying in that country, and (2) for leaving countries.

Commented [PL24]: GER: see above

Key AI use cases

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

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

Commented [PL25]: GER: Large Language Models (e. g. ChatGPT) extend fields of applications.

Commented [PL26]: GER: In the public debate, the term algorithmic management is often used for such systems. The categories workplace management and performance management could be combined under this term.

Commented [PL27]: GER: see comment above.

Relevant human rights and principles

160. The ECHR has been interpreted through the right to respect for private life (Article 8 ECHR), non-discrimination (Article 14 and Protocol No. 12 ECHR), freedom of expression (Article 10 ECHR) and freedom of association (Article 11 ECHR) to encompass certain labour and employment related rights such

~~[36] EU AI Act, preamble (33).~~

[37] UNHRC, Report ‘Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants’ (2020) UN Doc A/HRC/45/9; UNGA, Report ‘Contemporary forms of racism, racial discrimination, xenophobia and related intolerance’ (2020) UN Doc A/75/590;

[38] *S. and Marper v UK* App Nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008)

[39] See among many others *Van der Velden v. the Netherlands* (dec.), No. 29514/05, 7 December 2006; *Schmidt v. Germany* (dec.), No. 32352/02, 5 January 2006; *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008; *Canonne v. France* (dec.), No. 22037/13, 2 June 2015; *Gaughran v. the United Kingdom*, No. 45245/15, 13 February 2020; *Dragan Petrović v. Serbia*, No. 75229/10, 14 April 2020; *McVeigh, O’Neill and Evans v. the United Kingdom*, Nos. 8022/77, 8025/77, and 8027/77, Commission decision of 18 March 1981; *Allan v. the United Kingdom*, No. 48539/99, 5 November 2002; *Doerga v. the Netherlands*, No. 50210/99, 27 April 2004; *Vetter v. France*, No. 59842/00, 31 May 2005; *Wisse v. France*, No. 71611/01, 20 December 2005.

[40] *S. and Marper v the United Kingdom*, § 125.

[41] Convention 108+, Article 8.

[42] OSCE Policy Brief, Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021). p. 27.

[43] *Nada v. Switzerland* [GC], No. 10593/08, ECHR 2012.

[44] Council of Europe Consultative Committee of Convention 108, “Opinion on the Data protection implications of the processing of Passenger Name Records”, Strasbourg, 19 August 2016, p. 8.

[45] The levels of inaccuracy in biometric face recognition algorithms depend heavily on gender, skin colour and age. Studies have shown that existing face recognition algorithms had more difficulties to recognise female faces and produced more false rejections and false acceptances for female faces produced more accurate results for lighter faces than dark ones and had the highest error rate on darker female faces. See Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 5 October 2021.

[46] These are: national security or public safety, for the maintenance of public order, for the prevention of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[47] *De Tommaso v. Italy* [GC], No. 43395/09, 23 February 2017, § 104; *Pagerie v. France*, No. 24203/16, 12 January 2023, § 171; *Battista v. Italy*, No. 43978/09, 2 December 2014, § 37; *Khlyustov v. Russia*, No. 28975/05, 11 July 2013, § 64; *Labita v. Italy* [GC], No. 26772/95, 6 April 2000, §§ 194-195.

as the right to collective bargaining[48] or the right to strike[49] and to recognise the particular value of certain rights at work such as workplace privacy[50] or occupational health.[51] The ESC includes a large set of labour rights, both individual and collective.[52]

161. The use of AI systems may have far-reaching implications for labour and employment, spanning numerous categories of occupations (including those relatively sheltered from previous waves of automation), employers, and workers. The use of AI systems could hinder access to work, increase work intensity, reinforce or exacerbate power imbalances between employers and workers, reduce human involvement in decisions on hiring, evaluation and dismissal, change or possibly decrease the importance of human abilities and skills, and undermine fundamental principles and rights at work. AI-related challenges are particularly prevalent in new forms of employment such as platform or "gig" work.[53]

Commented [PL28]: GER: This does not seem clear to us. What would be the mechanism behind AI system hindering access to work?

Commented [PL29]: GER: We suggest to add this possible consequence of task automation and productivity.

Right to Privacy and Data Protection

162. Article 8 protects the right to respect for private life at the workplace, encompassing privacy of correspondence,[54] email use,[55] data protection,[56] access to data,[57] professional reputation,[58] and provides grounds for protection in cases of unfair dismissals.[59]

163. Any interference with privacy ~~should~~ must be lawful, pursue a legitimate aim, and be necessary and proportional.[60] This applies to both the State's negative obligation not to interfere with employee's privacy rights (for example in cases brought by public servants) and its positive obligations to secure the right to privacy in relations between private parties.[61] States have a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace.[62] However, the domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse.[63] In light of the rapid developments in this area, relevant factors have been identified for proportionality, as well as procedural

[48] *Demir and Baykara v. Turkey*, No. 34503/97, 12 November 2008.
[49] *Ognevenko v. Russia*, No. 44873/09, 20 November 2018, § 73.
[50] *López Ribalda and Others v. Spain* [GC], Nos. 1874/13 and 8567/13, 17 November 2019.
[51] *Meier v. Switzerland*, No. 10109/14, 9 February 2016.
[52] The right to work, just conditions of work, safe and healthy working conditions, fair remuneration, the right to equal opportunities and equal treatment in matters of employment and occupation without discrimination on the grounds of sex, protection in cases of termination of employment and protection of workers' claims in the event of the insolvency of their employer, dignity at work, right of workers with family responsibilities to equal opportunities and equal treatment; and collective: the right to organise and to bargain collectively, the right to information and consultation – also in collective redundancy procedures – and to take part in the determination and improvement of the working conditions and working environment, protection of workers' representatives in the undertaking and facilities to be accorded to them.
[53] Platform work a form of employment in which organisations or individuals use an online platform to access other organisations or individuals **to solve specific problems**, or to provide **specific services in exchange for payment**. The digital platform economy (or "gig economy") has developed exponentially during and after the Covid-19 pandemic.
[54] ***Bărbulescu** v. Romania* [GC], No. 61496/08, 5 September 201
[55] *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.
[56] *Surikov v. Ukraine*, No. 42788/06, 26 January 2017.
[57] *Yonchev v. Bulgaria*, No. 12504/09, 7 December 2017.
[58] *S.W. v. the United Kingdom*, No. 87/18, 22 June 2021
[59] *Ülya Ebru Demirel v. Turkey*, No. 30733/08, 19 June 2018; *Denisov v. Ukraine* [GC], No. 76639/11, 25 September 2018.
[60] *Peev v. Bulgaria*, No. 64209/01, 26 July 2007; *Radu v. Moldova*, No. 50073/07, 15 April 2014.
[61]*Köpke v. Germany (dec.)*, No. 420/07, 5 October 2010 (inadmissible).; ***Bărbulescu** v. Romania* [GC] § 118 "From a regulatory perspective, labour law leaves room for negotiation between the parties to the contract of employment. Thus, it is generally for the parties themselves to regulate a significant part of the content of their relations. It also appears from the comparative-law material at the Court's disposal that there is no European consensus on this issue. Few member States have explicitly regulated the question of the exercise by employees of their right to respect for their private life and correspondence in the workplace".
[62] *Barbulescu v Romania* [GC], § 119.
[63] Ibid. § 120.

guarantees against arbitrariness.[64] The domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body.[65]

169. AI systems are increasingly being used in selection procedures to determine access to employment.[66] Recruitment processes have the potential of being negatively affected by the use of AI systems, for example in cases where reliance on machine learning in the identification of candidates led to discriminatory outcomes, or where AI-based facial recognition and emotion analysis systems have resulted in racial discrimination.[67] As such, AI systems used for recruitment and selection of candidates should be objective, neutral and free from bias, including gender bias. In a broader context, States should ensure that the use of AI systems in the workplace does not reproduce or amplify existing patterns of inequality and promotes equality including gender equality, diversity and inclusion. In particular, this could consist of regular auditing of the outcomes of the use of AI systems in recruitment, promotion and other procedures; the involvement of employees and their representative organisations in policies or choices regarding the use of AI in decision-making in the workplace; monitoring of the impact of the introduction of AI systems in the workplace on gender equality and diversity in the workforce; and training and awareness-raising for the workforce on data bias, stereotypes and risks of discrimination in using AI systems.

The use of AI in employment also harbours the risk that inequalities will persist and worsen if the usability and accessibility of AI applications is not given. Elderly people, people with disabilities or people with limited digital skills may lack the required abilities to use them. For these groups, the chances of participating in the labour market may deteriorate. In addition, limited access to AI systems and tools can prevent individuals or groups from experiencing the benefits and advantages which they may offer. Policymakers should ensure that AI systems are accessible, and promote together with employers the development and diffusion of AI systems that contribute to better participation in employment, such as assistance systems.

Commented [PL30]: GER: We suggest to add this aspect

Page 61:

Further reading:

Commented [PL31]: GER: We suggest to add the study: Mapping Study on the Rights of the Child and Artificial Intelligence – Legal Frameworks that Address AI in the Context of Children's Rights (Prepared by The Alan Turing Institute
and approved by the CDENF during its 9th plenary meeting, Strasbourg, 28-30 May 2024).
It could be considered to also add some conclusions of the Study to the text.

- ECHR, Guide on Article 2 of Protocol No. 1 - Right to education
- COE, Regulating the use of Artificial Intelligence systems in education - Preparatory study on the development of a legal instrument (2024)
- COE, The state of artificial intelligence and education across Europe – Results of a survey of Council of Europe member states (2024)
- COE, 1st Working Conference "Artificial Intelligence and education: A critical view through the lens of human rights, democracy and the rule of law" - Conference highlights (2022)
- COE, Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022)
- Regulating artificial intelligence in the education domain: a general approach (2024: Ilkka TUOMI)
- Towards a European review framework for AI EdTech systems (2024: Beth HAVINGA)
- UNESCO, Beijing Consensus on Artificial Intelligence and Education (2019)
- UNESCO, Artificial Intelligence and Education: Guidance for Policy Makers (2021)

[64] Ibid. § 121. The relevant factors are: (i) whether the employee was clearly notified in advance about monitoring; (ii) the extent and intrusiveness of the monitoring; (iii) whether the employer had legitimate reasons for monitoring communications, especially for accessing their content; (iv) whether less intrusive alternatives were available; (v) the consequences for the employee and how the monitoring results were used; and (vi) whether adequate safeguards were in place to protect employee privacy.
[65] Ibid., § 122.
[66] Resolution 2343 (2020) 'Preventing discrimination caused by the use of artificial intelligence', paragraph 1. See also Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems, paragraph 8.
[67] CDADI/GEC Study (2023), pp. 19-21.

- (UN) Committee on the Rights of the Child, General Comment No. 25 (2021) on children’s rights in relation to the digital environment (2021)

SWITZERLAND / *SUISSE*

134. Chapter 2 of the Handbook introduces key technical concepts linking the technological aspects of AI to human rights implications. Chapter 3 outlines general human rights principles under the ECHR and ESC relevant to AI across selected 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 consider public-private intersections using ECHR and ESC standards, as well as other international norms. It concludes in Chapter ~~IV~~ 4 with reflections on emerging challenges in AI governance, ensuring a dynamic and forward-looking approach.

2. AI SYSTEMS AND FURTHER TECHNICAL CONCEPTS RELEVANT FOR HUMAN RIGHTS

135. This chapter provides a working definition ~~n explanation~~ of “artificial intelligence systems”~~-~~, ~~and~~an basic functions, and identifies further technical concepts that are relevant in the context of this Handbook. The definitions provided below rely on a variety of sources.[68] These definitions are not exhaustive or universal. While the following chapter offers a foundational understanding, the Handbook employs a range of further technical terms in Chapters ~~III~~ 3 and ~~IV~~ 4 that are defined in the Glossary (see Appendix [x]).[69]

Commented [A32]: We believe the footnote might be misplaced

2.2.2 Explainability[70]

19. Explainability is a particularly important component of transparency. AI systems integrating machine learning (ML) or deep learning (DL) technology ~~use~~ rely on ~~algorithms~~ mathematical models ~~trained by their own process of training~~derived from their training process, rather than ~~by explicit human~~explicitly-programmed rules ~~programming~~. During the process of training, AI models can discover new correlations between certain input features and can make decisions or predictions based on highly complex models involving a large number of interacting parameters (possibly millions), making it difficult even for AI experts to understand how their outputs are subsequently produced.[71] The resulting opacity, or “**black box**” effect, not only makes decisions more difficult to understand, but it can also have direct impact on individuals since it can hide deficiencies in AI systems, such as the existence of bias, inaccuracies, or so-called “hallucinations”.

[68] Framework Convention; Explanatory Memorandum accompanying the updated definition of an artificial intelligence system in the OECD Recommendation on Artificial Intelligence (OECD/LEGAL/0449, 2019, amended 2023). (OECD Explanatory Memorandum), EU Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act); CEPEJ Cyberjustice Glossary, ISO/IEC 22989:2022 – Information technology — Artificial intelligence — Artificial intelligence concepts and terminology.

[69] The definitions correspond to the CEPEJ Cyberjustice Glossary which is based on a range of further sources.

[70] See also, ISO/IEC 22989:2022, 5.15.6.

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

109. Key AI use cases include:

- *Medical diagnostics:* AI systems that can analyse medical images (X-rays, MRIs, CT scans etc.) and assess symptoms in order to help identify disease and diagnose health conditions.
- *Predictive analytics*: AI systems used to predict patient outcomes, such as risk of disease and potential complications, by data analysis.
- *Personalised medicine*: AI systems that help tailor treatment plans to individual patients, optimizing drug therapies and medical interventions by analysing genetic information and other health data.
- *Virtual health assistants*: AI-powered chatbots and virtual assistants that provide patient support, including mental health support, by answering questions, scheduling appointments, and offering medication reminders.
- *Remote monitoring and telemedicine*: AI-powered wearable devices and telehealth platforms enabling patient monitoring outside of traditional settings.
- *Robotic surgery*: AI-powered robotic systems enhancing surgical precision and control.

Commented [A33]: We suggest including the use of AI systems in the development of medical devices themselves

3.3.3. Social services and welfare

118. Social services encompass a broad range of programs and services designed to promote human and societal well-being. In addition to fundamental public services such as education and health care, addressed in their respective chapters of this Handbook [add reference to chapter number], social services and welfare systems provide both financial and non-financial assistance. These include social security programs that offer financial support for the elderly, the disabled and survivors ~~based on workers'~~ benefits; unemployment benefits; maternity and paternity benefits; housing assistance (subsidies or social housing), and support for the homeless or those at risk of homelessness; guaranteed minimum income or in-kind benefits, such as food assistance for low-income families; child and family services including child care subsidies, programs and tools aimed at combatting domestic violence, and child welfare services; old age and disability support.

Commented [A34]: Suggest replacing by benefits

Key AI use cases

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

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

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

Non-discrimination and equality

125. 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, error or 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. Safeguards are required, including human oversight, ensuring the critical evaluation of AI outputs and thus neutralising the risk of discriminatory effects.[72]

Key AI use cases

- *Digital forensics*: Several tools and techniques for data recovery and analysis have been developed with AI components. These tools can recover deleted files, access data from damaged devices, restore fragmented pieces of information into coherent formats and investigate the digital footprint of criminals.
- *Surveillance systems*: technologies such as image classification, computer vision and biometrics including automated facial recognition, fingerprints or biometric categorisation.
- *Data analytics and predictive policing*: employing statistical methods to extract insights from vast datasets, for instance on crime records, events and environmental factors identified in criminological insights and also unstructured data originating from open-source intelligence and social media intelligence sources.
- *Natural language processing:* performing tasks through processing textual data, such as text classification and clustering, text summarization and machine translation.

Commented [A36]: NLP is more a technique or set of techniques than a use case *per se*. Such techniques are relevant throughout all public governance sectors. We would suggest providing examples so the reader can better understand what tasks would be performed through NLP in the context of law enforcement and public security. For instance, one could imagine NLP to monitor communications and flag messages that incite violence.

143. AI-~~ systems ~~driven **surveillance technologies**, including biometric monitoring and behaviour-tracking may be used also to enhance **prison security**. Placing a person under permanent video surveillance whilst in prison – which already entails a considerable limitation on a person's privacy – has to be regarded as a serious interference with the right to respect for privacy, as an element of the notion of "private life" (Article 8 ECHR).[73] Recommendation CM/Rec(2024)5 **regarding the ethical and organisational aspects of the use of AI and related digital technologies by prison and probation services** emphasises that the use of such systems for maintaining safety, security and good order should be strictly necessary, proportionate to the purpose and should avoid any negative effects on the privacy

[72] 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 generalisations to the behaviour of individuals of the same race or ethnicity perceiving them stereotypically as fraudulent or deviant.

[73] *Vasilică Mocanu v. Romania*, No. 43545/13, 6 December 2016.

and well-being of offenders and staff. The use of AI systems in monitoring should be proportionate to the purpose and used only when strictly necessary. The human-centred approach should remain a key element in decision taking for offender management, risk assessment, rehabilitation and reintegration. Under no circumstances should the use of AI systems cause intentional physical or mental harm or suffering to a person.

3.3.7. Education

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

Commented [A37]: We suggest including teaching (at schools and as part of higher education), as this seems to be implicit here

In addition, limited access to AI systems and tools can prevent individuals or groups from experiencing the benefits and advantages which they may offer, resulting in disadvantages in various sectors including education. AI literacy, which might be considered an extension or specialisation of digital literacy should be included in the basic education curriculum from the earliest years, taking into account children's developing capacities.[74] This includes technical competencies, content creation skills, and critical understanding of online risks and opportunities. Efforts should focus on schools, child-focused organisations, and parents or other reference adults, ensuring a safe and inclusive digital environment.

Page 61:
Further reading:

Commented [A38]: Ajouter ici la Recommandation de l'OCDE sur les enfants dans l'environnement numérique: OECD Legal Instruments

- ECHR, Guide on Article 2 of Protocol No. 1 - Right to education
- COE, Regulating the use of Artificial Intelligence systems in education - Preparatory study on the development of a legal instrument (2024)
- COE, The state of artificial intelligence and education across Europe – Results of a survey of Council of Europe member states (2024)
- COE, 1st Working Conference "Artificial Intelligence and education: A critical view through the lens of human rights, democracy and the rule of law" - Conference highlights (2022)
- COE, Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022)
- Regulating artificial intelligence in the education domain: a general approach (2024: Ilkka TUOMI)
- Towards a European review framework for AI EdTech systems (2024: Beth HAVINGA)
- UNESCO, Beijing Consensus on Artificial Intelligence and Education (2019)
- UNESCO, Artificial Intelligence and Education: Guidance for Policy Makers (2021)
- (UN) Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment (2021)

UNITED KINGDOM / *ROYAUME-UNI*

1. INTRODUCTION

Commented [FA39]: Could add something here on how this is potentially one of many ways to think about the intersection between HR and AI, to make it clear that this handbook is a guide and not the only way to encourage compliance?

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,

[74] Recommendation CM/Rec(2019)10 on developing and promoting digital citizenship education, 21 November 2019; Recommendation CM/Rec(2016)2 on the Internet of citizens, 10 February 2016.

by expediting judicial proceedings, enhancing healthcare through predictive diagnostics, and personalising education to meet individual learning needs. Yet alongside these opportunities come significant risks.

3. Existing Council of Europe human rights instruments such as the European Convention on Human Rights and its Protocols (ECHR) and the European Social Charter (ESC), remain applicable in the context of AI. These instruments, interpreted by the European Court of Human Rights (the Court) and the European Committee on Social Rights (ECSR) respectively, establish basic standards for the protection of human rights. While neither the Court nor the ESCR have yet directly addressed AI's impact on human rights, member States must align their legal frameworks on AI with their existing obligations under the ECHR and ESC. This is especially crucial for those specific areas that are not covered by the Framework Convention[75] but are still subject to the provisions of the ECHR and ESC, as well as for those member States that are not States parties to the Framework Convention.

Commented [FA40]: Whilst it is clear it means existing obligations, we suggest adding this to highlight that it's not about creating new rights or obligations, but about the application of existing frameworks

5. Chapter 2 of the Handbook introduces key technical concepts linking the technological aspects of AI to potential human rights implications. Chapter 3 outlines general human rights principles under the ECHR and ESC that may be relevant to AI across selected public sectors. It addresses first cross-cutting issues relevant to all sectors. Then it provides a sectoral analysis of potential 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 consider public-private intersections using ECHR and ESC standards, 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.

2. AI SYSTEMS AND FURTHER TECHNICAL CONCEPTS RELEVANT FOR HUMAN RIGHTS

6. This chapter provides an explanation of “artificial intelligence systems” for the purposes of this Handbook and their basic functions and identifies further technical concepts that are relevant in the context of this Handbook. The definitions provided below are examples of definitions ~~rely on~~from a variety of sources.[76] These definitions are not exhaustive or universal. While the following chapter offers a foundational understanding, the Handbook employs a range of further technical terms in Chapters III and IV that are defined in the Glossary (see Appendix [x]).[77]

Commented [VL41]: As below we aren't purporting to define AI outside this context

Commented [FA42]: Suggestions for language tweaks, as it's not too clear what is meant by ‘rely on’

2.1.6 Environment or Context

14. An environment or context in relation to an AI system is an observable or partially observable space perceived using data and sensor inputs and influenced through actions (through actuators). The environments influenced by AI systems can be physical or virtual and include environments describing aspects of human activity, such as biological signals or human behaviour. Sensors and actuators are either humans or components of machines or devices.[78]

Commented [FA43]: Suggest we refer to OECD explanatory report document for this as its same as EU, but has greater global buy in

[75] See below, para [x].
[76] Framework Convention; Explanatory Memorandum accompanying the updated definition of an artificial intelligence system in the OECD Recommendation on Artificial Intelligence (OECD/LEGAL/0449, 2019, amended 2023). (OECD Explanatory Memorandum), EU Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act); CEPEJ Cyberjustice Glossary, ISO/IEC 22989:2022 – Information technology — Artificial intelligence — Artificial intelligence concepts and terminology.
[77] The definitions correspond to the CEPEJ Cyberjustice Glossary which is based on a range of further sources.
[78] Idem, p. 7.

2.1.7 Input

15. Input is used both during development and after deployment. Input can take the form of knowledge, rules and code that humans put into the system during development or data. Humans and machines can provide input. During development, input is leveraged to build AI systems, e.g., with machine learning that produces a model from training data and/or human input. Input is also used by a system in operation, for instance, to infer how to generate outputs. Input can include data relevant to the task to be performed or take the form of, for example, a user prompt or a search query.[79]

Commented [FA44]: As above, same as OECD - use OECD footnote as more countries have agreed

2.1.8 Inference

16. The concept of "inference" generally refers to the step in which a system generates an output from its inputs, typically after deployment. "Infer how to generate outputs" should be understood as also referring to the build phase of the AI system, in which a model is derived from inputs/data.[80]

Commented [FA45]: Again, suggest using OECD definition:

The concept of "inference" generally refers to the step in which a system generates an output from its inputs, typically after deployment. When performed during the build phase, inference, in this sense, is often used to evaluate a version of a model, particularly in the machine learning context. In the context of this explanatory memorandum, "infer how to generate outputs" should be understood as also referring to the build phase of the AI system, in which a model is derived from inputs/data.

2.1.9 Output

17. Outputs generally reflect different tasks or functions performed by AI systems. They include, but are not limited to, recognition (identifying and categorising data, e.g., image, video, audio and text, into specific classifications as well as image segmentation and object detection), event detection (connecting data points to detect patterns, as well as outliers or anomalies), forecasting (using past and existing behaviours to predict future outcomes), personalisation (developing a profile of an individual and learning and adapting its output to that individual over time), interaction support (interpreting and creating content to power conversational and other interactions between machines and humans, possibly involving multiple media such as voice text and images), goal-driven optimisation (finding the optimal solution to a problem for a cost function or predefined goal) and reasoning with knowledge structures (inferring new outcomes that are possible even if they are not present in existing data, through modelling and simulation).[81]

Commented [FA46]: Suggest replacing with OECD instead of using EU AI Act as baseline:

The output(s) generated by an AI system generally reflect different functions performed by AI systems. AI system outputs generally belong to the broad categories of recommendations, predictions, and decisions. These categories correspond to different levels of human involvement, with "decisions" being the most autonomous type of output (the AI system affects its environment directly or directs another entity to do so) and "predictions"6 the least autonomous. For example, a driver-assist system might "predict" that a pixel region in its camera input is a pedestrian; it might "recommend" braking, or it might "decide" to apply the brake. Generative AI systems that produce "content" —including text, image, audio, and video—have gained significant momentum. Although one could, for example, view the generation of text as a sequence of decisions to output particular words (or predictions of words that would be likely to appear in a specific context), content generation systems have become such an important class of AI systems that they are included as their own output category in the present revised definition.

24. As the core instrument for economic and social rights within the Council of Europe, the ESC guarantees fundamental protections that complement the ECHR. The Revised European Social Charter (RESC) incorporates new rights and amendments. 42 out of the 46 member States of the Council of Europe are parties to either the ESC or the RESC.[82] 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.[83] While its decisions and conclusions are not directly enforceable, they represent an authoritative interpretation of the ESC's provisions. States Parties have an obligation to cooperate with the ESCR and to implement its decisions and conclusions, that arises from the application of the principle of good faith to the observance of their treaty obligations under the ESC. The rights protected in the ESC are listed in appendix [x].

Commented [VL47]: Comma to help make it clear the text after is in respect of the obligation to cooperate and implement rather than the decisions and conclusions.

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

[79] Idem, p. 8.
[80] Idem, p. 9.
[81] Idem, p. 9.
[82] Liechtenstein, Monaco, San Marino and Switzerland are not parties to either of these treaties.
[83] 16 of the 42 Parties to the ESC have ratified this Additional Protocol.

25. The Framework Convention reinforces existing international standards (such as the ECHR and the ESC) as may be applicable to each Party. It adopts a technology-neutral approach, focusing on principles rather than regulating specific technologies. It applies to activities within the lifecycle of AI systems undertaken by public authorities (including private actors acting on their behalf).[84] With regard to activities by private actors acting independently, State Parties undertake to address risks and impacts in a manner conforming with the object and purpose of the Framework Convention, either by applying directly the principles and obligations set forth in the Convention or by taking “other appropriate measures”.[85] In addition, matters relating to national defence are exempted from the scope of the treaty,[86] as well as (i) activities related to the protection of the State Parties’ “national security interests” with the understanding that such activities are conducted in a manner consistent with applicable international law, including international human rights law obligations, and with respect for its democratic institutions and processes;[87] and (ii) research and development activities, unless testing or similar activities are undertaken in such a way that they have the potential to interfere with human rights, democracy and the rule of law.[88]

27. Key requirements include the availability of remedies, to the extent any remedies are required by a Party’s international obligations for AI related ~~breaches~~ violations of human rights,[89] ensuring procedural safeguards for affected persons, including the provision of notice to persons interacting with AI systems;[90] conducting risk and impact assessments[91] on human rights, democracy, and the rule of law; and enabling the possibility of bans, moratoria or other appropriate measures in respect of certain uses of AI systems that the State Party considers incompatible with respect for human rights, the functioning of democracy or the rule of law.[92] The Framework Convention also provides for follow-up mechanisms and cooperation and introduces an obligatory monitoring mechanism.[93]

Commented [FA48]: Edited so it better reflects the language in Art 14

3.1.4 ECHR and ESC General Principles in the Context of AI

28. Neither the Court nor the ECSR has yet directly addressed AI's impact on rights under the ECHR and ESC.[94] However, established principles from the ECHR and the ESC offer guidance on how these treaties may apply to AI-related human rights challenges. While some principles overlap, others are specific to each treaty.[95]

Effective Protection of Rights

[84] Article 3 subparagraph 1 (a).
[85] Article 3 subparagraph 1 (b).
[86] Article 3 paragraph 4. Also note that under Article 1.d. of its Statute, “Matters relating to national defence do not fall within the scope of the Council of Europe”.
[87] Article 3 paragraph 2.
[88] Article 3 paragraph 3.
[89] Chapter IV (Article 14).
[90] Article 15. Where an artificial intelligence system substantially informs or takes decisions impacting on human rights, effective procedural guarantees should, for instance, include human oversight, including *ex ante* or *ex post* review of the decision by humans (Explanatory Report, § 103).
[91] Chapter V (Article 16).
[92] Article 16, paragraph 4.
[93] Chapter VII (Articles 23-26).
[94] While the Court has yet to directly address AI, it has examined cases involving new technologies and their impact on human rights, including technologies integrating AI features, such as facial recognition systems (see *Glukhin v. Russia*, Application No. 11519/20, 4 July 2023; see also Factsheet – New technologies).
[95] The ECHR and ESC treaty systems are complementary and interdependent. The Court has clarified that there is no watertight division separating civil and political rights from economic, social and cultural rights. See *Airey v Ireland*, No. 6289/73, 9 October 1979, § 24; see also Digest of Case Law of the European Committee of Social Rights, December 2022, p. 33.

29. The ECHR and the ESC are intended to guarantee rights that are not merely theoretical or illusory but practical and effective.[96] National authorities must ensure that rights holders can effectively enjoy their rights, which may involve adopting legislation, ensuring its effective application, providing adequate resources, and establishing appropriate operational procedures. Accordingly, States should safeguard the effective protection of human rights against harms related to activities within the lifecycle of AI systems, which may include ~~not only by~~ implementing laws as well as ~~but also by~~ providing resources, establishing, or human rights structures, such as national human rights institutions (NHRIs), as independent oversight mechanisms, and ensuring effective cooperation between such mechanisms and other national human rights structures.

Commented [FA49]: Edited to further clarify that legislation is not a requirement but one of many measures that could be implemented

34. Positive obligations can apply even in cases where threats originate from private individuals or entities beyond direct state control as these instruments can address both vertical relationships – between national authorities and individuals – and horizontal relationships[97], between individuals or entities. States must protect human rights in the sphere of the relations between individuals themselves (horizontal effect). This duty becomes particularly important in the context of the deployment of AI systems, where public-private partnerships and procurement from private actors are prevalent.

Commented [FA50]: Small edit to soften language

36. States' positive obligations ~~thus~~ may require them to assess proactively whether AI systems might harm human rights and to enact legislation to address those potential harms, and/or to implement measures to mitigate identified risks. The Framework Convention contains a dedicated provision prescribing the need to identify, assess, prevent and mitigate *ex ante* and, as appropriate, iteratively throughout the lifecycle of the AI system the relevant risks and potential impacts to human rights, democracy and the rule of law by following and enabling the development of a methodology with concrete and objective criteria for such assessments.[98]

Commented [FA51]: UK may have further comment on this

57. Parties to the Framework Convention are required to adopt or maintain measures to ensure the availability of accessible and effective remedies, to the extent that remedies are required by a Parties' obligations, for violations of human rights resulting from activities within the lifecycle of AI systems.[99] This includes documenting and making relevant information available, where appropriate and applicable, to affected individuals, ~~where appropriate,~~ enabling them to understand and exercise their rights. The relevant 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.[100]

Commented [FA52]: Edited language to better reflect Art 14 and for clarity

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

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

[98] Framework Convention Article 16, see also Explanatory Report, § 105.

[99] Framework Convention, Article 14.

[100] Explanatory Report, § 99

60. Under the ECHR, States can be held accountable where they acquiesce or connive in acts of private actors that ~~violate~~ abuse human rights[101] or when they fail to properly regulate private industry.[102] The concrete scope and content of State obligations depend to some extent on the human right in question and the factual circumstances. Generally, positive obligations consist of requirements to prevent human rights violations where the competent authorities had known or ought to have known of a real risk of such violations; to undertake an independent and impartial, adequate and prompt official investigation where such violations are alleged to have occurred; to undertake an effective prosecution, and to take all appropriate measures to establish accessible and effective mechanisms which require that the victims of such violations receive prompt and adequate reparation for any harm suffered.[103] However, not every failure to prevent business-related abuses will violate ECHR obligations. It may be necessary to show that the abuse would definitely have been prevented had the State taken measures that could reasonably have been expected of it in the situation at hand.[104]

Commented [EP53]: This paragraph used both "violations" and "abuses". UK position is that only States can violate human rights, so can we adjust language to read abuses when speaking about the adverse impacts of businesses

61. The ESC also affords protection against business-related human rights abuses, particularly regarding the rights of workers. ~~As part of their policy~~, member States that have ratified the ESC should national and international measures to ensure the effective realisation of the rights and principles of the ESC and consider increasing the number of accepted ~~ing additional~~ provisions.[105]

Commented [FA54]: Suggest deletion, not sure what it adds/means (e.g what 'policy' is it referring to)

Commented [VL55]: Have updated in line with Rec (2016) 3

Obligations relating to the provision of effective remedies

70. States should also provide effective remedies for business-related human rights abuses. This may include amending laws if the legal framework is inadequate[106] and to ensure that businesses comply with domestic law. Of relevance here is the right to an effective remedy (Article 13 ECHR).

Commented [FA56]: UK may come in with comment on this

83. In the AI specific context, the HUDERIA Methodology,[107] while not a specific instrument on corporate responsibility to respect human rights, is addressed to both public and private actors. It connects international human rights standards and existing technical frameworks on risk management in the AI context and provides a structured approach to risk and impact assessment of AI systems specifically tailored to the protection and promotion of human rights, democracy and the rule of law.

Commented [VL57]: This link seems to be to: European Commission for the Efficiency of Justice (CEPEJ)

PARTICIPANTS

[101] *Ilaşcu and Others v. Moldova and Russia* [GC], No. 48787/99, 8 July 2004, § 318.

[102] *Hatton and others v. the United Kingdom* [GC], No. 30622/1997, 8 July 2003, § 98

[103] Recommendation CM/Rec(2016)3 on human rights and business, para 15.

[104] *E. and Others v. the United Kingdom*, No. 33218/96, 26 November 2002.

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

[106] *Fadeyeva v. Russia*, §§89 and 92; see also *Powell and Rayner v. the United Kingdom*, No. 93101/81, 21 February 1990.

[107] The HUDERIA Methodology ("Methodology for the Risk and Impact Assessment of Artificial Intelligence Systems from the point of view of Human Rights, Democracy and the Rule of Law") is a structured tool designed to serve as guidance in assessing and mitigating risks posed by AI systems to human rights, democracy, and the rule of law. It complements, without being legally binding, the Framework Convention. It is to be supplemented by the HUDERIA Model – supporting materials such as tools and scalable recommendations to serve as a resource for risk management activities.

CONFERENCE OF INGOS OF THE COUNCIL OF EUROPE / *CONFÉRENCE DES OING DU CONSEIL DE L'EUROPE*

4. INTRODUCTION

21. 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.

22. The potential threat to human rights involved with the use of AI systems has been acknowledged by the international community and has driven global efforts to regulate this set of technologies.[108] The Council of Europe began working on the theme of AI a decade ago and has intensified its efforts in recent years, with several Council of Europe bodies and committees issuing a number of policy documents, recommendations, declarations, guidelines and other legal instruments.[109] The Council of Europe's Framework Convention on Artificial Intelligence and, Human Rights, Democracy and the Rule of Law is the first international treaty on AI and human rights (the Framework Convention).[110] 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.[111]

23. Existing Council of Europe human rights instruments such as the European Convention on Human Rights and its Protocols (ECHR) and the European Social Charter (ESC), remain applicable in the context of AI. These instruments, interpreted by the European Court of Human Rights (the Court) and the European Committee on Social Rights (ECSR) respectively, establish basic standards for the protection of human rights. While neither the Court nor the ESCR have yet directly addressed AI's impact on human rights, member States must align their legal frameworks on AI with their obligations under the ECHR and ESC. This is especially crucial for those specific areas that are not covered by the Framework Convention[112] but are still subject to the provisions of the ECHR and ESC, as well as for those member States that are not States parties to the Framework Convention.

2.1.9 Output

17. Outputs generally reflect different tasks or functions performed by AI systems. They include, but are not limited to, recognition (identifying and categorising data, e.g., image, video, audio and text, into specific classifications as well as image segmentation and object detection), event detection (connecting data points to detect patterns, as well as outliers or anomalies), forecasting (using past and existing behaviours to predict future outcomes), personalisation (developing a profile of an individual and learning and adapting its output to that individual over time), interaction support (interpreting and creating content

Commented [CK58]: Comment from International Federation of Actors (FIA) - CINGO member:
Nous souhaitons souligner l'absence dans ce document de toute référence à l'utilisation des systèmes d'IA dans le secteur culturel ainsi qu'à l'exploitation de contenus protégés par le droit d'auteur et les droits voisins à des fins d'entrainement et de génération de contenus synthétiques pouvant concurrencer de façon déloyale les créateurs sur le marché du travail. Ceci pourrait avoir un impact important sur l'exercice de leurs libertés, y compris leur liberté d'expression. Compte tenu du lien souvent indissociable entre les contenus exploités par l'IA et les données biométriques – notamment la voix et/ou l'image – des artistes qui contribuent à leur réalisation, il nous semble essentiel de souligner l'importance du respect des principes de transparence et de consentement éclairé également dans notre secteur, afin de permettre aux artistes et créateurs de faire pleinement valoir leurs droits et, notamment, de veiller au bon respect de leurs données personnelles par les fournisseurs et déployeurs d'IA générative.

Commented [CK59]: Comment from European Network Church on the Move - CINGO member:
1. Impact on employment and working conditions: AI not only influences decision making, but also transforms the labour market. It is important to consider how automations affect employment,
working conditions, and the need for new skills.
2. Ethics in AI development: In addition to regulation, it would be relevant to address the ethical responsibility of those who design and train these systems. Ethics in programming and model
development is key to avoid bias and malpractice.
3. Risks of misinformation and manipulation: With generative AI and recommendation
algorithms, the risks of misinformation and manipulation of public opinion are amplified. Citizens
may need better tools to identify reliable information.
4. Effects on mental health: The widespread use of AI on social media and digital platforms may influence people's ...

Commented [FF60]: We strongly welcome this emphasis.

Commented [CK61]: Comment from International League Against Racism and Antisemitism - CINGO member:
La Licra salue l'initiative du Comité Directeur Droits Humains et Intelligence Artificielle pour son initiative dans la création du Manuel Droits Humains et Intelligences Artificielles. Après examen, la Licra souhaiterait adresser des commentaires sur la question des biais algorithmiques et de leur impact sur les discriminations d'une part et d'autre part, la nécessité de mécanismes de contrôle et de recours pour les victimes et l'encadrement éthique contraignant des usages de l'IA dans les administrations et les entreprises. ...

Commented [CK62]: Comments from European Association of Railwaymen - CINGO member:
Remarques fondamentales:
a) les résultats de l'IA reposent pour l'essentiel sur des inputs et
algorithmes techniques qui doivent être contrôlés par des instances
indépendantes et neutres. Pour l'essentiel, le principe américain appliqué à
l'informatique (IT) :"Garbage in garbage out" devrait s'appliquer a l'IA
aussi ...

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

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

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

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

[112] See below, para [x].

to power conversational and other interactions between machines and humans, possibly involving multiple media such as voice text and images), goal-driven optimisation (finding the optimal solution to a problem for a cost function or predefined goal) and reasoning with knowledge structures (inferring new outcomes that are possible even if they are not present in existing data, through modelling and simulation).[113]

2.2 Further technical concepts relevant for AI and human rights

2.2.1 Transparency

Commented [FF63]: Comment from BASW (British Association of Social Workers) - CINGO member: Accepting that the meaning of 'transparency' is covered in some following sections, I nonetheless think the description in 2.2.1 could be improved and the imperative of transparency made clearer. This paragraph could be elaborated to explain (or give examples of) how AI decision making process and general operations can and should be made more transparent to 'appropriate AI actors...relevant stakeholders' . The current definition in 2.2.1 is opaque and mirrors the lack of transparency many user of AI experience and lack of understanding about how they can improve their knowledge of the principles behind the functioning of AI they are using , what assumptions it is working to etc.

18. Transparency refers to openness and clarity in the governance of activities within the lifecycle of AI systems. It means that the decision-making processes and general operation of AI systems should be understandable and accessible to appropriate AI actors and, where necessary and appropriate, relevant stakeholders.[114]

2.2.2 Explainability[115]

19. Explainability is a particularly important component of transparency. AI systems integrating machine learning (ML) or deep learning (DL) technology use algorithms trained by their own process of training, rather than by explicit human programming. During the process of training, AI models can discover new correlations between certain input features and can make decisions or predictions based on highly complex models involving a large number of interacting parameters (possibly millions), making it difficult even for AI experts to understand how their outputs are subsequently produced.[116] The resulting opacity, or "**black box**" effect, not only makes decisions more difficult to understand, but it can also have direct impact on individuals since it can hide deficiencies in AI systems, such as the existence of bias, inaccuracies, or so-called "hallucinations".

20. "Explainability" therefore refers to the capacity to provide, subject to technical feasibility and taking into account the generally acknowledged state of the art, sufficiently understandable explanations about why an AI system provides information, produces predictions, content, recommendations or decisions.[117]

Commented [FF64]: Comment from BASW (British Association od Social Worker) - CINGO member: What is the meant by this clause? In particular what is meant by using the phrase 'state of the art' at this point? This paragraph could be written with more clarity and precision on this important point. Amongst other improvements in this para should be some high level/in principle reference to the varying 'explanation' requirements of different types of AI users or subjects e.g. differentiated by age, ability, vulnerability, socioeconomic dis/advantage etc.

Commented [FF65]: Adding "sufficiently" is crucial, as we often hear pushbacks based on the impossibility to retrace *all* details of the way the ML operates, while we only need the essential ones.

31.1.4 ECHR and ESC General Principles in the Context of AI

Effective Protection of Rights

29. The ECHR and the ESC are intended to guarantee rights that are not merely theoretical or illusory but practical and effective.[118] National authorities must ensure that rights holders can effectively enjoy their rights, which may involve adopting legislation, ensuring its effective application, providing adequate resources, and establishing appropriate operational procedures. Accordingly, States should safeguard the

[113] Idem, p. 9.
[114] See the Explanatory Report to the Framework Convention, § 57.
[115] See also, ISO/IEC 22989:2022, 5.15.6.
[116] TechDispatch: Explainable Artificial Intelligence, European Data Protection Supervisor (2023), citing Peters, U. 'Explainable AI lacks regulative reasons: why AI and human decision-making are not equally opaque', (AI and Ethics 2023); see also CDDH-IA(2024)09, Summary of the exchange of views with external independent experts and representatives of Council of Europe intergovernmental committees (25 September), key points made by Marko Grobelnik; and CDDH-IA(2024)07, Compilation of written contributions and presentations received from experts of the exchange of views of the 1st meeting, pp. 3-16.
[117] Framework Convention Explanatory Report, § 60.
[118] *Airey v Ireland*, No. 6289/73, 9 October 1979, § 24; *International Commission of Jurists (ICJ) v. Portugal*, Complaint No. 1/1998, decision on the merits of 9 September 1999, §32; *European Federation of National Organisations working with the Homeless (FEANTSA) v. Slovenia*, Complaint No. 53/2008, decision on the merits of 8 September 2009, §28.

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, establishing, or designating and empowering existing national human rights structures, such as national human rights institutions (NHRIs), as independent oversight mechanisms, and ensuring effective cooperation between such mechanisms and other national human rights structures.

Positive Obligations

35. 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 ensure the existence of adequate and effective mechanisms under which sanctions may be imposed in particular cases, enact specific legal rules, and/or take operational steps to protect individuals from foreseeable risks to their rights.[119]

36. States' positive obligations thus require them to assess proactively whether AI systems might harm human rights and to enact legislation to address those potential harms effectively, and/or to implement measures to mitigate identified risks. The Framework Convention contains a dedicated provision prescribing the need to identify, assess, prevent and mitigate *ex ante* and, as appropriate, iteratively throughout the lifecycle of the AI system the relevant risks and potential impacts to human rights, democracy and the rule of law by following and enabling the development of a methodology with concrete and objective criteria for such assessments.[120]

Human Dignity

37. 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.[121]

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

42. 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. Limitations must be proportionate to the legitimate aim pursued, respond to pressing social needs, and use the least restrictive means.

Non-Discrimination and Equality

i. The Prohibition of Discrimination in the ECHR and the ESC

Commented [FF66]: Some of these structures also need to be effectively provided with budget, capacity and competence/powers to intervene appropriately.

Commented [FF67]: Comment from BASW (British Association of Social Workers) - CINGO member: Reference could be made here explicitly to the importance of States ensuring institutions/laws etc protect the rights of all groups in society including those likely to be marginalised in both access to opportunities and protection from harms of AI including children, elderly, people with intellectual/learning disabilities, poorer people etc

Commented [FF68]: We believe this statement should be better explained/clarified, because in our understanding, the "result" to which States are mandated is indeed the full enjoyment of the rights guaranteed. We also do not see a clear explanation of this caveat in ECHR, *Osman v. The United Kingdom*, § 115, referenced in the footnote. Formulated in this way, the statement could be misleading and interpreted as if all the States have to do is put in place measures without an obligation to assess that they **effectively** and **adequately** protect human rights. In other words: how does the Court assess that the measures are "adequate" and the mechanisms "effective" without considering the ensuing (even potential) result on the protection of the rights?

Commented [FF69]: Recalling language already used further up, it is not enough to merely tick a box by showing there is legislation in place and being enacted. The clarity, necessity and proportionality of those measures also need to be demonstrated. This due diligence obligations are adequately summarised by the qualifier "effectively".

Commented [FF70]: Comment from EUROMIL - CINGO member: Amendment: The use of AI in military decision-making, including autonomous weapons systems, must not dehumanize military personnel or violate ethical principles related to the conduct of armed forces. Commanders and personnel should retain meaningful human control over AI-assisted decisions in military operations.

Commented [FF71]: Comment from BASW (British Association of Social Workers) - CINGO member: Reference could be made here explicitly to the importance of States ensuring institutions/laws etc protect the rights of all groups in society including those likely to be marginalised in both access to opportunities and protection from harms of AI including children, elderly, people with intellectual/learning disabilities, poorer people etc

Commented [FF72]: That is exactly what we intend as "obligation of result": the "conduct" is adopting restrictions by following these parameters; the "result" is that such restrictions are effectively lawful, legitimate and necessary in a democratic society. See comment above about obligations of conduct and result. This is crucial in terms of the enforceability of the treaties' obligations and to hold the State Parties accountable in courts about their compliance with such obligations.

Commented [FF73]: Comment from EUROMIL - CINGO member: Amendment: AI must not reinforce biases in military personnel management, including recruitment, promotions, or disciplinary actions. Safeguards should be in place to prevent discrimination based on gender, ethnicity, or political opinions within armed forces as well military personnel assessments.

Formatted: Font: Not Bold

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

[120] Framework Convention Article 16, see also Explanatory Report, § 105.

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

44. The ECHR[122] and the ESC[123] prohibit discrimination but only in relation to the enjoyment of rights and freedoms set out in the respective treaty. Article 1 of Protocol No. 12 ECHR introduces a general prohibition against discrimination covering “any right set forth by law”.[124] (…)

~~ii.~~ Risks to Non-Discrimination and Equality

ii.

Commented [FF74]: Comment from EUROMIL - CINGO member:
Same remark as for paragraph 44.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Heading 5, Indent: Hanging: 0,89 cm, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Left + Aligned at: -0,38 cm + Indent at: 0,89 cm

Formatted: Heading 5, Indent: Hanging: 0,89 cm, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Left + Aligned at: -0,38 cm + Indent at: 0,89 cm

46. AI systems may pose risks to equality and non-discrimination, as they may be built upon and sustained by data and models that reproduce, perpetuate, and exacerbate existing bias, stereotypes, stigma, prejudice, and false assumptions about individuals based on actual or perceived personal characteristics and their intersections. These effects can be further compounded by information asymmetries and can be more severe for persons in vulnerable situations or marginalised communities. Among other things, such effect may lead to an increase in online and offline violence against such persons, as well as against women, who are disproportionately targeted due to existing gender inequalities, stereotypes, and power imbalances that AI systems may inadvertently amplify.[125]

Commented [FF75]: In various contexts there may be marginalised groups because od socio-cultural bias but they are not necessarily vulnerable.

The Right to Privacy and Personal Data Protection

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

Commented [FF76]: Comment from EUROMIL - CINGO member:
Amendment: Due to the specificity of their job, military personnel are often subject to extensive surveillance. AI-driven monitoring and data collection must be proportionate and respect fundamental privacy rights, ensuring that military personnel are not unfairly targeted or subjected to excessive data profiling.

48. 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.[126] Private life includes, among other things, one's image, identity, personal development, and relationships, and extends also to professional or business activities. Personal data covers information such as names, addresses, IP addresses, and sensitive data like information relating to health and ethnicity. 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 the right to respect for private life and any such interference must be lawful, pursue a legitimate aim, be necessary and proportional.

ii. Privacy and Data Protection Risks

52. The protection of privacy rights and personal data protection is a common principle required for effectively realising many other principles in the Framework Convention.[127] Effective safeguards are necessary to address risks like unauthorised data collection, misuse, and harm to individuals' dignity.[128]

[122] ECHR Article 14.

[123] RESC Article E.

[124] This Protocol has been ratified by 20 member States of the Council of Europe.

[125] Such violence has been addressed by several soft-law instruments, including the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) General Recommendation No. 1 on the digital dimension of violence against women. The Council of Europe [has also developed] a specific instrument on [combating] technology-facilitated violence against women and girls. Appendix [x] of the Handbook provides further information on concluded, ongoing, or forthcoming initiatives [to be completed].

[126] 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.

[127] Explanatory Report, § 79.

[128] 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.

States should adopt or maintain measures throughout the AI lifecycle, to ensure that individuals' privacy rights and personal data are protected including through applicable domestic and international laws, standards, and frameworks, and that effective safeguards are in place in line with domestic and international obligations.[129] The 2019 Guidelines on Artificial Intelligence and Data Protection[130] provide further guidance for policymakers and AI developers. These include that AI development involving personal data should adhere to the principles of Convention 108+, including lawfulness, fairness, purpose specification, proportionality, privacy-by-design and by default, accountability, transparency, data security, and risk management. AI applications should fully respect data subjects' rights, particularly under Article 9 of Convention 108+, and ensure meaningful control over data processing and its societal impact. In addition, cooperation should be encouraged between data protection supervisory authorities and other bodies having competence related to AI, such as: consumer protection; competition; anti-discrimination; sector regulators and media regulatory authorities.

Commented [FF77]: This is also a clear example of "obligation of results", not just of "conduct".

Commented [FF78]: This is also a clear example of "obligation of results", not just of "conduct".

Effective remedies

The right to an effective remedy

Commented [FF79]: Comment from BASW (British Association of Social Workers) - CINGO member: Effective remedy ultimately may be by judicial means, but in practice, more people will and can gain meaningful remedy for human rights breaches or risks through competent non-judicial or quasi judicial actors e.g. other public sector bodies and professions such as in health services, social services, welfare benefits services etc. This could be reflected better in this section.

24. 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.[131] Remedies must be effective in both law and practice, accessible, affordable, and capable of providing appropriate redress.[132] They can include judicial mechanisms or a quasi-judicial body such as an ombudsman[133], or a political authority such as a parliamentary commission.[134] These should be independent and procedural safeguards should be afforded to the applicant.[135] However, the Court may exceptionally find a remedy before a judicial authority to be essential (for example concerning review and supervision of secret surveillance measures ~~solitary confinement~~) or desirable.[136] Additionally, States are required to ensure that individuals have access to judicial or non-judicial mechanisms to address human rights abuses by private actors, such as businesses.[137]

Commented [FF80]: Since the main case/reference featured in the footnote (please check number of paragraph as well) is ECHR *Big Brother Watch and Others v. the United Kingdom* and it covers a case regarding abusive use of technologies, we recommend replacing the example of "solitary confinement" with the one of this case.

25. The ESC does not contain an explicit right to an effective remedy, however, the ESCR has interpreted the ESC as requiring an effective remedy in certain cases.[138]

[129] Framework Convention, Article 11.
[130] Adopted by the Consultative Committee of the Convention 108.
[131] *Boyle and Rice v. the United Kingdom*, 27 April 1988, Nos. 9659/82 and 9658/82, § 52; *Powell and Rayner v. the United Kingdom*, 21 February 1990, § 31; M.S.S. *v. Belgium and Greece* [GC], No. 30696/09, January 21 2011, § 288; *De Souza Ribeiro v. France* [GC], 2012, No. 22689/07, 13 December 2012, § 78; *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], 17 July 2014, § 148.
[132] *Paulino Tomás v. Portugal*, (dec), No. 58698/00.
[133] *Leander v. Sweden*, No. 9248/81, 26 March 1987.
[134] *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, § 67
[135] *Khan v. the United Kingdom*, No. 35394/97, 12 May 2000, §§ 44-47.
[136] See for e.g., *Big Brother Watch and Others v. the United Kingdom* [GC], Nos. 58170/13, 62322/14, and 24960/15, 25 May 2021, § 309 ~~336 :~~ "In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure". See also *Ramirez Sanchez v. France* [GC], No. 59450/00, 4 July 2006, §§ 165-166; *Danilczuk v Cyprus*, No. 21318/12, 3 April 2018, §§ 44.
[137] *Z and Others v. the United Kingdom* [GC], No. 29392/95, 10 May 2001, § 109; *Keenan v. the United Kingdom*, No. 27229/95, 3 April 2001, § 129; *Paul and Audrey Edwards v. the United Kingdom*, No. 46477/99, 14 June 2002, § 97.
[138] Employees who claim their right to equal pay must be legally protected from all forms of retaliatory action. Where an employee is the victim of retaliatory action, there must be an adequate remedy, which will both compensate the employee and serve as a deterrent to the employer, see Conclusions XV-2 (2001), Slovak Republic; National legislation should, as a minimum, require a compelling justification for special or segregated educational systems and confer an effective remedy on those who are found to have been unlawfully excluded or segregated or

ii. Risks to the Right to an Effective Remedy

56. 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 and various upstream actors in the supply chain. Individuals may lack the knowledge or access to information necessary to identify violations and the responsible person or entity. 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.

57. Parties to the Framework Convention are required to adopt or maintain measures to ensure the availability of accessible and effective remedies for violations of human rights resulting from activities within the lifecycle of AI systems.[139] 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.[140]

3.2 Business and Human Rights

58. This section explores the intersection of AI-related business activities and human rights obligations, focusing on States' positive obligations under the ECHR and ESC,[141] 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.

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

67. State decisions in relation to business activities – such as granting a licence – may also impact on human rights. Decision-making processes "concerning issues of cultural, environmental and economic impact […] must necessarily involve appropriate investigations and studies in order to allow [public authorities] to strike a fair balance between the various conflicting interests at stake".[142] To afford due respect for the interest protected by, for example, Article 8 ECHR, the decision-making process leading to measures of interference should "consider all the procedural aspects, including the type of policy or decision involved, the extent to which the views of individuals were taken into account throughout the decision-

Commented [FF81]: Comment from BASW (British Association of Social Workers) - CINGO member: This is a strong and important para that could be strengthened by emphasising the impact of social, economic, educational and other inequalities which leave some people more exposed to these risks than others. In particular, many poorer and more socially marginalised people are more likely to have more data sharing interfaces with state institutions and to be more exposed to data processing risks and to the application of opaque AI algorithms to decisions about them.

Commented [FF82]: Again, the fact that they must "accessible" and "effective" is an obligation of result.

Commented [FF83]: Comment from EUROMIL - CINGO member: Amendment: Private contractors supplying AI systems for military and defense applications must adhere to strict ethical standards. AI used in military operations must comply with international human rights law, avoiding abuses such as unlawful surveillance, autonomous targeting, or excessive restrictions on service members' rights.

Formatted: Heading 2, Indent: Left: 0,85 cm

Commented [FF84]: These procedural safeguards should cover not only the activities of States regulating/deciding on business activities but also on States' decisions on their own use of AI in the public sector.

otherwise denied an effective right to education; Under Article 15§2, anti-discrimination legislation must include the adjustment of working conditions (reasonable accommodation) and confer an effective remedy on those who are found to have been unlawfully discriminated, see Conclusions 2007, Statement of Interpretation on Article 15§1; Conclusions XIX-1 (2008), Czech Republic; States Parties are required to prove the absence of discrimination, whether direct or indirect, in terms of law and practice, and should inform of any practical measures taken to remedy cases of discrimination see Conclusions III (1973), Statement of Interpretation on Article 19§4; *European Federation of national organisations working with the Homeless (FEANSA) v. the Netherlands*, Complaint No. 86/2012, 2 July 2014, §§ 202-203.

[139] Framework Convention, Article 14.

[140] Explanatory Report, § 99

[141] States may breach their negative obligations where business-related human rights abuses are attributable to the State. This could occur, for instance, where a business is owned or controlled by the State; or a business is acting as an agent of the State. At present, relevant activities within AI systems lifecycle are largely conducted by independent private business. Therefore, the Handbook focuses on positive obligations, notwithstanding the possibility to include analysis of negative obligations in future editions.

[142] *Zammit Maempel v. Malta*, Application No. 24202/10, 22 November 2011, § 62.

making process, and the procedural safeguards available".[143] In environmental cases, this requires investigations and studies "'to predict and evaluate in advance the effects of those activities which might damage the environment and infringe individuals' rights".[144] State regulation "must also provide for appropriate procedures, taking into account the technical aspects of the activity in question, for identifying shortcomings in the processes concerned and any errors committed by those responsible at different levels".[145]

Obligations relating to the provision of effective remedies

70. States should also provide effective remedies for business-related human rights abuses. This may include amending laws if the legal framework is inadequate[146] and to ensure that businesses comply with domestic law. Of relevance here is the right to an effective remedy (Article 13 ECHR).

Commented [FF85]: Highlighting another obligation of result (effectiveness/adequacy).

Right to liberty and security (Article 5 ECHR)

Commented [FF86]: Comment from BASW (British Association of Social Workers) - CINGO member:
Deprivation of Liberty (DoL) here is used in relation primarily to criminal detention. But the same term is used in English in relation to matters of detention for reasons of protection of adults or children within Courts of Protection/civil court and mental health tribunal parts of the legal system. DoL in practice in various jurisdictions is managed and decisions made by legally empowered non-lawyer professionals and this section should surely make reference to DoL and AI risks etc in these practice contexts?

103. The key purpose of Article 5 is to prevent unlawful, arbitrary or unjustified deprivations of liberty.[147] 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 5 § 1.[148] Deprivation of liberty is also unlawful if the conviction is the result of proceedings which amount to a "flagrant denial of justice"[149] by being "manifestly contrary to the provisions of Article 6 or the principles embodied therein".[150] 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.[151]

3.2.1 Healthcare

Commented [CK87]: Comment from Mental Health Europe - CINGO member:
Mental Health Europe invites the CDDH to consider its Study on Artificial Intelligence in mental healthcare.
The report is co-authored with Piers Gooding - La Trobe University- and Hannah van Kolfschooten - University of Amsterdam and Health Action International- and it is argued that AI tools need to be developed with ethics, inclusivity, accuracy, safety and the genuine needs of end users in mind. Possible solutions mainly include robust regulation and oversight, transparency and explainability, as well as human rights-centric and co-creation approaches.
The study can be found here: https://www.mentalhealtheurope.org/mental-health-europe-launches-a-study-on-artificial-intelligence-in-mental-healthcare/

107. 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.

Right to Privacy and Data Protection

Commented [FF88]: Comment from EUROMIL - CINGO member:
Amendment: This amendment has already been used but could also have its place in this paragraph. "Military personnel are often subject to extensive surveillance. AI-driven monitoring and data collection must be proportionate and respect fundamental privacy rights, ensuring that military personnel are not unfairly targeted or subjected to excessive data profiling."

112. Article 8 ECHR protects health-related personal data.[152] 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

[143] *Taskin and Others v. Turkey*, § 118.
[144] Idem.
[145] *Öneryıldız v. Turkey* [GC], § 90.
[146] *Fadeyeva v. Russia*, §§89 and 92; see also *Powell and Rayner v. the United Kingdom*, No. 93101/81, 21 February 1990.
[147] *Selahattin Demirtaş v. Turkey* (No. 2) [GC], No. 14305/17, 22 December 2020, § 311.
[148] *S., V. and A. v. Denmark* [GC], No. 35553/12, 36678/12, and 36711/12, 22 October 2018, § 92.
[149] *Othman (Abu Qatada) v. the United Kingdom*, No. 8139/09, 17 January 2012, § 260.
[150] *Willcox and Hurford v. the United Kingdom* (dec.), Nos. 43759/10 and 43771/12, 8 January 2013, § 95; *Othman (Abu Qatada) v. the United Kingdom*, No. 8139/2009, 17 January 2012, § 259; *Stoichkov v. Bulgaria*, No. 9808/02, 24 March 2005, §§ 51, 56-58.
[151] *Vorontsov and Others v. Ukraine*, No. 58925/14 and 4 others, 21 January 2021, §§ 42-49.
[152] *Surikov v. Ukraine*, No. 42788/06, 26 January 2017, §§ 70 and 89.

regulatory frameworks.[153] The Committee of Ministers of the Council of Europe has issued specific guidelines on the protection of health-related data, by its Recommendation CM/Rec(2019)2 which seeks to ensure the principles of Convention 108, including its modernised version, are fully applied to the exchange and sharing of health-related data.

3.3.3 Social services and welfare

Commented [FF89]: Comment from BASW (British Association of Social Workers) - CINGO member:
This whole section is written very negatively. There are many risks with AI in social services context and these are quite well covered, but the positive opportunities for the use of AI are not well covered. The section also does not make reference to the imperative in social services of managing the balance of technological and human to human relationships which are core to social services practices. This section is therefore not comprehensively useful to the social services sector which is having to manage the implementation of AI often with fewer resources and research evidence then in (eg) healthcare at national level. There are examples of good use of AI in robotics, reduction of bureaucracy, self-service access to information, communication particularly with young people, online support forums, good use of algorithms to identify risks etc. Some of these are listed in the use cases but the subsequent text does not engender confidence about the possibility of better/safer use of available technologies. The fact that social services are often less well funded to implement AI than other public sectors could be highlighted as a macro level risk.

118. Social services encompass a broad range of programs and services designed to promote human and societal well-being. In addition to fundamental public services such as education and health care, addressed in their respective chapters of this Handbook [add reference to chapter number], social services and welfare systems provide both financial and non-financial assistance. These include social security programs that offer 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; guaranteed minimum income or in-kind benefits, such as food assistance for low-income families; child and family services including child care subsidies, programs and tools aimed at combatting domestic violence, and child welfare services; old age and disability support.

Key AI use cases

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

- *Predictive analytics:* AI systems that can analyse large datasets using algorithmic processes, including machine learning, to identify individuals or groups most at risk of requiring social services. This enables agencies to proactively allocate support and resources, for example, identifying children at risk who may need additional assistance.
- *Resource allocation:* AI-driven models optimize the distribution of usually limited resources, ensuring more efficient and equitable service delivery.
- *Screening and fraud detection*: AI systems used to assist in screening applicants, verifying applicant information, flagging inconsistencies, and identifying patterns indicative of fraud or misuse of welfare services, enhancing accountability and efficiency.
- *AI-driven chatbots and virtual assistants*: These systems handle routine inquiries, improve accessibility for people with disabilities through speech recognition or automated transcription, and monitor individuals' physical and mental health, issuing alerts to ensure timely interventions.
- *Overview and evaluation:* AI analyses social service outcomes to assess effectiveness, providing data-driven insights that help agencies refine policies and improve service delivery over time.
- *Professional Report Production:* AI is increasingly used to generate professional assessment, review and other reports about people accessing services. Such reports may be generated from professional's electronic or hand written notes or audio recordings. All such reports remain the responsibility of the professional commissioning and creating them by any means. AI may provide helpful reduction in time taken in administrative aspects of report production, but human review of content and meaning is essential for accuracy and for professional accountability.

Commented [FF90]: Comment from BASW (British Association of Social Workers) - CINGO member:
Proposed addition.

[153] 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".

Relevant human rights and principles

120. The provision of social services may directly interfere with an individual's enjoyment of his or her rights, such as the right to private and family life within the meaning of Article 8 ECHR,[154] the right to liberty within the meaning of Article 5,[155] or the right to property within the meaning of Article 1 of Protocol No.1.[156] In addition, effective social services contribute to the fulfilment of the State's positive obligations for the prevention of ill-treatment administered by private persons (Article 3).[157]

Commented [FF91]: Comment from Ruth Allen - BASW (British Association of Social Workers) - CINGO member:
Cross reference here with the section on Deprivation of Liberty which is applied as a concept above on in relation to criminal deprivation but which is equally applicable in civil/protection circumstances as referenced in 120.

3.3.4 Law Enforcement and Public Security

Commented [FF92]: Comment from EUROMIL - CINGO member:
Amendment: Military personnel engaged in national public security operations must be considered separately from law enforcement officers. The application of AI in military security tasks should be subject to distinct legal frameworks to ensure compliance with human rights obligations, avoiding overreach or excessive surveillance.

131. This sector involves police,[158] intelligence and assimilated services[159], including such issues as identification of individuals for law enforcement purposes, crime prevention, crime investigation, programmes regarding protection of persons in danger (e.g. victims of domestic violence or protected witnesses), arrests and detentions, prison and probation crowd management during public events and maintenance of public order, counterterrorism, national security operations, measures entailing surveillance of communications, restrictions, bans, prohibitions, lockdowns, various forms of supervision including those affecting the freedom of movement.

The right to liberty and security

133. Predictive policing systems make estimations and predictions that may be turned into concrete actions or decisions by the criminal justice system, including on arrest and detention. Due to the decisions that could be made based on such systems output, Article 5 ECHR (the right to liberty and security) issues may arise. Decisions on arrest or detention must be based on reasonable suspicion based on ~~that is~~ verifiable and objective facts directly linked to a criminal activity .[160] Should information provided by predictive policing systems be used to corroborate reasonable suspicion for a decision or arrest and detention, explainability and interpretability issues (the "black box problem") concerning AI systems may pose difficulties to meet the criteria required for verifiability and objectivity. Predictive policing methods must not lead to unlawful decisions on deprivation of liberty. Such operations carried out by public authorities must therefore be lawful, necessary, and proportionate to their intended purposes and be based on clear, foreseeable, and accessible domestic law, pursuing a legitimate aim while ensuring adequate safeguards.

Commented [FF93]: Language also consistent with the prohibitions of such AI systems within the EU Member States entered into force with EU AI Act.

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

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

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

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

[158] Police refers to traditional police forces or services and other publicly authorised and/or controlled services granted responsibility by a State, in full adherence to the rule of law, for the delivery of policing services.

[159] Government departments or units that are considered equivalent to the intelligence services in terms of their function.

[160] *Akgün v. Turkey*, No. 19699/18, 20 July 2021, §§ 156 and 175.

139. While the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, the margin of appreciation afforded to States must be narrower.[161] For bulk interceptions, a broader set of criteria beyond the six requirements (see para [x] above) apply to determine whether the State acted within its margin of appreciation.[162]

Non-discrimination and equality

146. In the context of prison and probation services, Recommendation CM/Rec(2024)5 **underlines that** safeguards must be in place to **prevent discrimination, ensure procedural fairness, and uphold human dignity**, ensuring that AI-driven prison management remains **compatible with fundamental rights and the rule of law**. When developing AI and related digital technologies in order to increase the accuracy and objectivity of risk assessment, the challenges of algorithmic biases and quality and representativeness of data should be addressed. Sensitivity to all kinds of diversity, including to gender perspective and multiculturalism, should inform the design and use of risk assessment tools in order to avoid any discrimination. When such tools are used for the personalisation of treatment and reintegration plans, this should be done with care to avoid biases. The use of such tools should not replace regular face-to-face human contact between professionals and the offenders, including, where necessary, the work with their families and children.

Right to an effective remedy

147. The application of AI system in law enforcement and public safety raises concerns about the right to an effective remedy (Article 13) [HYPERLINK].

Relevant human rights and principles[163]

150. The ECHR does not guarantee a right to enter, settle, or reside in a specific country,[164] however, non-nationals on the territory or, subject to the extraterritorial jurisdiction of a State party will enjoy the protection of the ECHR. States have the right to control the entry of non-nationals into their territory.[165] In exercising control of their borders, member States must act in conformity with ECHR standards. Caselaw only imposes certain limitations on the right of states to turn someone away from their borders, for example where this would amount to *refoulement*.[166]

Non-discrimination and equality

Commented [FF94]: The ECHR protects the right to privacy and establishes the requirements from restrictions but does not go into any specifics of the forms of restrictions. Maybe it is the ECtHR that does not prohibit the bulk interception? This is also debatable, though, based on *Big Brother Watch and Others*, because the Court distinguishes between different methods of interceptions (para 350) and states that "the interception of communications represents one of the gravest intrusions" and while "It is not in doubt that communications data is a valuable resource for the intelligence services" (para 353), "it is a matter of some concern that the intelligence services can search and examine 'related communications data' apparently without restriction." So the statement at the beginning of para 139 appears to be draconian and imprecise, since bulk interception must be assessed on a case-by-case basis and in some of these cases may be prohibited outright as inherently disproportionate.

Commented [CK95]: Comment from CINGO member Children of Prisoners Europe to include:

The use of such tools should not replace regular face to face human contact between professionals and the offenders, including, where necessary, the work with their families and children, **in line with Recommendation CM/Rec(2018)5.**

Commented [FF96]: This para could be further developed with references to explainability and accountability of the AI systems designed and deployed for public security, including proper access to risk and impact assessments conducted on the systems, so that both the judge and the plaintiffs have access to evidence of the alleged harm done by the system (see **Equality of arms and adversarial proceedings** chapter above).

Commented [FF97]: True, but for those CoE that have ratified it, Article 2, ECHR Protocol No.4 recognises Freedom of movement). We recommend at least clarifying this in a Footnote.

Formatted: Font: Italic

[161] *Big Brother Watch and Others* [not *Zoltan Varga*), ~~Ibid~~., § 347 [not clear how this para supports the text;].

[162] In examining compliance with the principles of legality and necessity, the Court considers whether the domestic legal framework clearly defines: (1) grounds for authorisation; (2) circumstances for individual interception; (3) authorisation procedures; (4) selection, examination, and use of intercept material; (5) safeguards for data sharing; (6) limits on interception duration, data storage, and erasure; (7) independent supervisory mechanisms and enforcement powers; and (8) *ex post facto* review procedures and remedies for non-compliance. See *Big Brother Watch and Others*, § 336 et seq.

[163] In addition to the ECHR and the ESC, the Council of Europe has adopted other legal instruments relevant for immigration. See https://www.coe.int/en/web/migration-and-refugees/council-of-europe-reference-documents-and-resources1

[164] *Jeunesse v. the Netherlands*, No. 12738/10, 3 October 2014, § 103; *Maslov v. Austria* [GC], No. 1638/03, § 68, ECHR 2008; *Üner v. the Netherlands* [GC], No. 46410/99, § 54, ECHR 2006-XII; *Boujlifa v. France*, No. 25404/94, 21 October 1997, § 42, Reports 1997-VI; *Abdulaziz, Cabales and Balkandali v. the United Kingdom*, Nos. 9214/80, 9473/81, and 9474/81, 28 May 1985, § 67, Series A No. 94.

[165] *Abdulaziz, Cabales and Balkandali v. the United Kingdom* App nos 9214/80, 9473/81, 9474/81, 28 May 1985, § 67.

[166] *F.G. v. Sweden* [GC], no. 43611/11, 23 March 2016, § 117.

157. Decisions based on information from AI systems may result in unlawful discrimination, including indirect and intersectional discrimination, due to bias in AI systems. In addition, technologies such as facial recognition systems that use biometric data have been described as inherently fallible since they inevitably rely on statistical probabilities and are prone to inaccuracy and errors.[167] While this issue is not exclusively related to migration, the consequences for migrants' and refugees' rights can be significant. If AI systems based facial recognition technologies are used for identification and identity verification at pre-departure or on arrival at borders, some individuals may be more exposed to inaccuracies and misidentification due to their protected characteristics. A combination of personal information about a person, as is used in visa and travel authorization systems, may also reveal protected characteristics AI-assisted decision-making tools that analyse face, speech, dialect recognition, name transliteration, or mobile phone data in visa and travel authorization systems could inadvertently reveal protected characteristics, increasing the risk of biased assessments and unequal treatment and their misuse could lead to discriminatory profiling. If such mistakes are not corrected, misidentified individuals may be denied entry, resulting in discriminatory decisions potentially impacting the right to liberty of movement (Article 2 Protocol 4). Any measure restricting the right to liberty of movement must pursue one of the legitimate aims [168] referred to in paragraph 3 of Article 2 of Protocol No. 4 and strike a fair balance between the public interest and the individual's rights.[169]

3.3.6 Labour and Employment

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

Freedom of Expression; Freedom of Assembly and Association

173. Article 10 ECHR (freedom of expression) applies in the context of labour relations, including where these are governed by the rules of private law.[170] This may entail negative and positive State obligations. In the private sphere, the responsibility of the authorities would be engaged if the facts complained of stemmed from a failure on their part to secure to the applicants the enjoyment of Article 10 ECHR.[171] Article 11 ECHR (freedom of assembly and association) protects both workers and trade unions. An employee or worker should be free to join or not join a trade union without being sanctioned or subject to disincentives.[172] In view of the sensitive character of the social and political issues involved in achieving a proper balance between the respective interests of labour and management, and given the high degree of divergence between the domestic systems in this field, States enjoy a wide margin of appreciation as to how trade union freedom and protection of the occupational interests of union members may be secured.[173]

[167] The levels of inaccuracy in biometric face recognition algorithms depend heavily on gender, skin colour and age. Studies have shown that existing face recognition algorithms had more difficulties to recognise female faces and produced more false rejections and false acceptances for female faces produced more accurate results for lighter faces than dark ones and had the highest error rate on darker female faces. See Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 5 October 2021.

[168] These are: national security or public safety, for the maintenance of public order, for the prevention of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[169] *De Tommaso v. Italy* [GC], No. 43395/09, 23 February 2017, § 104; *Pagerie v. France*, No. 24203/16, 12 January 2023, § 171; *Battista v. Italy*, No. 43978/09, 2 December 2014, § 37; *Khlyustov v. Russia*, No. 28975/05, 11 July 2013, § 64; *Labita v. Italy* [GC], No. 26772/95, 6 April 2000, §§ 194-195.

[170] *Herbai v. Hungary*, No. 11608/15, 2019 July 9, § 37; *Fuentes Bobo v. Spain*, No. 39293/98, 2000 February 29, § 38.

[171] *Herbai v Hungary*, § 37.

[172] *Associated Society of Locomotive Engineers and Firemen (ASLEF) v. the United Kingdom,* No. 11002/05, 27 February 2007, § 39.

[173] *Sindicatul "Păstorul cel Bun" v. Romania* [GC], No. 2330/09, 9 July 2013, § 133.

Commented [FF98]: This is exactly why we recommend adding a reference to Article 2, Protocol 4 right from the outset, at least in a Footnote.

Commented [FF99]: Comment from EUROMIL - CINGO member:
Amendment: The impact of AI on military personnel should be explicitly addressed, particularly in areas such as recruitment, automated performance evaluations, and deployment decision-making. AI systems must not undermine the rights of military personnel, including fair working conditions, non-discrimination, and access to legal remedies.

Commented [FF100]: Comments from EUROMIL - CINGO member:
Remarks on Freedom of Assembly and Association in the military:

- Address the ongoing legal restrictions on military trade unions: Many European states still impose unjustifiable restrictions or outright bans on military trade unions, despite ECtHR rulings and ECSR Decisions on the Merrits affirming their right to association. This section should make it clearer that these restrictions must be lifted or at least brought in line with international human rights norms.
- Emphasize that restrictions on military personnel's rights must be proportional: While military service has unique aspects, this should not justify a complete exclusion from trade union rights. Proportionality and necessity should be guiding principles in any restrictions imposed.
- Call for explicit protections against retaliation: In many military structures, indirect forms of retaliation (such as denial of promotions or forced transfers) are used to suppress trade union activity. The text should clearly demand safeguards against such practices.

Commented [FF101]: Comments from EUROMIL - CINGO member:
Amendment 1: Military personnel should not face disproportionate restrictions on their right to freedom of expression. While military discipline may justify certain limitations, such restrictions must remain strictly necessary and proportionate, ensuring that personnel can express concerns about working conditions, trade union rights, and human rights violations without undue consequences.
Amendment 2: Military personnel must be granted full trade union rights in line with international standards. While States have some discretion in balancing national security with trade union freedoms, total bans on military unions are incompatible with Article 11 ECHR. States must provide clear legal pathways for military personnel to collectively organize and negotiate their professional rights.
Amendment 3: This protection must explicitly extend to military personnel, ensuring that participation in military trade unions is not met with indirect sanctions, such as exclusion from promotions, assignments, or training opportunities.
Amendment 4: In the military context, additional safeguards should be in place to prevent retaliation against military trade unionists, including protection from arbitrary reassignment, exclusion from leadership roles, and other forms of indirect discrimination.

Conference of INGOs: Consolidated feedback to the CDDH-IA "Draft Handbook on human rights and artificial intelligence, Chapters I, II, and III CDDH-IA(2025)1REV 12/03/2025

CINGO is grateful for the opportunity to provide input and feedback on the above handbook prepared by the CDDH Drafting Group on Human Rights and Artificial Intelligence.

This short summary is intended to consolidate the responses from CINGO members in addition to the detailed comments included in the attached draft handbook. Responses to this consultation were provided directly by 9 CINGO members, as well as the CINGO appointed expert on human rights and artificial intelligence, Francesca Fanucci. Responses to this consultation were submitted by:

Mental Health Europe; European Association of Railwaymen; International Federation of Actors; European Network Church on the Move; European Organisation of Military Associations and Trade Unions; ClientEarth; International League Against Racism and Antisemitism; Children of Prisoner's Europe; and British Association of Social Workers.

Based on the views shared by CINGO members, we distil the following points for Drafting Group's consideration:

I. The handbook could benefit from offering further analysis on the need for ethical frameworks in AI development and use in public and private companies and regulatory bodies. Concerns regarding algorithmic biases in AI remain, in regard to, for example, race, religious expression, and gender: all actions concerning AI must consider the potential risks of discrimination and must not reinforce biases.

II. An analysis of the available control and redress mechanisms for victims of rights violations through automated systems.

III. An analysis of the heightened risk of misinformation and need for effective transparency and fact-checking mechanisms in multiple contexts. There is little reference to transparency and informed consent regarding how the sharing of personal data, including voice and image, are protected or how material protected by copyright may be protected from future exploitation.

IV. Consideration of AI in the context of healthcare and impacts on mental health is welcome. However, it is noted that social services is not well guided in this document. There is little balance between risks – which is the focus of the document - and opportunities of AI which are largely left out in social services. This seems to reflect the way social services are generally being 'left behind' in digi/AI momentum in many countries given relatively lower national-level investment and less research (at national and international levels) in this sector compared to (for example) healthcare.

V. Reference to the environmental impacts of AI and human rights implications is still needed. There is a suggestion to include a new chapter on human rights in the environment to highlight the violations caused and exacerbated by environmentally unsustainable AI development (See annex below with additional details).

Annex: Proposed inclusion of Section 3.4: Human Rights and the Environment

1. Climate Change Acceleration and Vulnerability

o Although efficiencies from applying AI provide green potential, AI itself has become one of the largest consumers of energy and thus drivers of climate change. AI development and deployment contribute significantly to global greenhouse gas emissions. By way of examples, training the previous generation of large language model ChatGPT – GPT3 – produced around 1 million KG of CO2. CO2 emissions of training GPT4, on even larger datasets, were significantly higher. The monthly carbon emissions of ChatGPT (not including the enormous costs of initial training) are currently at about 260,000 KG of CO2.

o The increasing energy demands of AI models intensify climate change impacts, leading to extreme weather events, rising sea levels, and environmental degradation. Vulnerable populations, including low-income communities and small island nations, bear the brunt of these consequences, exacerbating existing social and economic inequalities.

2. Air Pollution and Public Health Risks

o AI development and deployment significantly contributes to air pollution: Through emissions of criteria air pollutants such as fine particular matter, AI's lifecycle – from chip manufacturing to data centre operation – significantly degrades air quality.

o These pollutants disproportionately impact communities located near power plants and industrial zones, increasing incidences of respiratory diseases, cardiovascular issues, and overall public health disparities.

2. Energy Inequality

o AI's high energy demands present significant challenges in regions with limited access to clean and affordable electricity.

o Data centres consume vast amounts of energy, increasing global demand and therefore exacerbating energy poverty and increasing reliance on non-renewable energy sources.

3. Resource Exploitation

o AI hardware depends on rare earth minerals such as lithium, cobalt, and nickel, extracted through environmentally destructive mining practices.

o Mining activities result in deforestation, displacement of Indigenous Peoples & Local Communities (IP&LCs), habitat loss (which impacts IP&LCs), and unethical labour conditions, particularly in countries with weak regulations and enforcement.

4. Water Scarcity

o AI-driven data centres require substantial water resources for cooling, intensifying water stress in regions already facing shortages.

o A single large data centre can consume millions of gallons of water annually to prevent critical infrastructure from overheating, reducing water availability for local communities and ecosystems, with severe consequences in drought-prone regions.

5. E-waste accumulation

o Rapid AI advancements lead to increased electronic waste (e-waste), much of which is non-recyclable and hazardous, often containing mercury and lead.

o Improper disposal of AI hardware contributes to toxic pollution, disproportionately affecting marginalized communities living near e-waste dumps, where hazardous substances such as lead and mercury pose severe health risks.

OBSERVERS / *OBSERVATEURS*

EUROPEAN NETWORK OF NATIONAL HUMAN RIGHTS INSTITUTIONS (ENNHRI) / *RESEAU EUROPEEN DES INSTITUTIONS NATIONALES DES DROITS DE L'HOMME (ENNHRI)*

1. INTRODUCTION

1. Artificial intelligence (AI) is increasingly ~~influencing various aspects of~~being adopted across 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.

2. The potential threat to human rights ~~involved~~ from ~~with~~ the use of AI systems has been acknowledged by the international community and has driven global efforts to regulate this set of technologies.[174] The Council of Europe began working on the theme of AI a decade ago and has intensified its efforts in recent years, with several Council of Europe bodies and committees issuing a number of policy documents, recommendations, declarations, guidelines and other legal instruments.[175] The Council of Europe's Framework Convention on Artificial Intelligence and, Human Rights, Democracy and the Rule of Law is the first international treaty on AI and human rights (the Framework Convention).[176] 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.[177]

3. Existing Council of Europe human rights instruments such as the European Convention on Human Rights and its Protocols (ECHR) and the European Social Charter (ESC), remain applicable in the context of AI.: member States must align their legal frameworks on AI with their obligations under the ECHR and ESC.~~.~~ These instruments, interpreted by the European Court of Human Rights (the Court) and the European Committee on Social Rights (ECSR) respectively, establish basic standards for the protection of human rights. ~~While neither the Court nor the ESCR have yet directly addressed AI's impact on human rights, member~~ but are still subject to the provisions of the ECHR and ESC, as well as for those member States that are not States parties to the Framework Convention. This is especially crucial for those specific areas that are

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

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

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

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

not covered by the Framework Convention[178] but are still subject to the provisions of the ECHR and ESC, as well as for those member States that are not States parties to the Framework Convention.

3.1.4 ECHR and ESC General Principles in the Context of AI

28. ~~Neither the Court nor the ECSR has yet directly addressed AI's impact on rights under the ECHR and~~ jurisprudence from the Court and ECSR on the impact of AI technologies on rights under the ECHR and ESC.[179] However, established principles from the ECHR and the ESC offer guidance on how these treaties may apply to AI-related human rights challenges. While some principles overlap, others are specific to each treaty.[180]

Effective Protection of Rights

29. The ECHR and the ESC are intended to guarantee rights that are not merely theoretical or illusory but practical and effective.[181] National authorities must ensure that rights holders can effectively enjoy their rights, which may involve adopting legislation, ensuring its effective application, providing adequate resources, and establishing appropriate operational procedures. Accordingly, States should safeguard the effective protection of human rights against harms related to activities within the lifecycle of AI systems not only by implementing laws but also by providing resources, establishing, or designating existing national human rights structures, such as national human rights institutions (NHRIs), as independent oversight mechanisms, and ensuring effective cooperation between such mechanisms and other national human rights structures.

Commented [SH104]: ENNHRI welcomes this recommendation and underlines the importance of NHRIs having full formal and functional independence and adequate resources, as required under the UN Paris Principles.

141. As for the collection of (biometric) personal data with facial recognition technology, minimum safety measures regarding the duration, storage, usage and destruction of personal data are required to ensure appropriate safeguards. While the need to use modern technologies in states' efforts to fight against crime, and in particular against organised crime and terrorism is beyond dispute,[182] in *Glukhin v Russia* the authorities' use of facial recognition technology to investigate the applicant violated his right to respect for private life (Article 8) and freedom of expression (Article 10). Although the police measures were based on domestic law, there were no adequate and effective guarantees against abuse. Moreover, the personal data processed contained information about the applicant's participation in a peaceful protest and therefore revealed his political opinions. Personal data revealing political opinions fall within the special category of sensitive data attracting a heightened level of protection.[183] In the context of implementing facial recognition technology, it is essential to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards is greater where there is use of live facial recognition technology.[184] In addition to the Article 8 concerns, the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could

[178] See below, para [x].

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

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

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

[182] *Glukhin v. Russia*, No. 12317/16, 4 July 2023, § 85.

[183] Ibid, § 76 and 86.

[184] Ibid., § 82.

have a chilling effect in relation to the rights to freedom of expression (Article 10 ECHR) and assembly (Article 11 ECHR).[185]

Commented [SH105]: ENNHRI recommends that a more detailed explanation of what the chilling effect is would be helpful here.

[185] Ibid., § 88.