CDDH-IA(2025)01REV
14/03/2025

COMITÉ DIRECTEUR POUR LES DROITS HUMAINS

(CDDH)

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

(CDDH-IA)

[ÉBAUCHE] Manuel sur les droits humains et l'intelligence artificielle

Chapitres I, II et III

Table des matières

1. INTRODUCTION

1. L'intelligence artificielle (IA) influe de plus en plus sur divers aspects de la société, ouvrant de nouvelles perspectives d'innovation et de progrès. Elle peut notamment faire progresser les droits humains, par exemple en accélérant les procédures judiciaires, en améliorant les soins de santé grâce à des diagnostics prédictifs et en personnalisant l'éducation pour répondre aux besoins d'apprentissage individuels. Cependant, ces opportunités s'accompagnent de risques importants.

2. La menace potentielle pour les droits humains liées à l'utilisation des systèmes d'IA a été reconnue par la communauté internationale et a déclenché des efforts mondiaux pour réglementer cet ensemble de technologies[1]. Le Conseil de l'Europe a commencé à travailler sur le thème de l'IA il y a dix ans et a intensifié ses efforts ces dernières années, plusieurs organes et comités du Conseil de l'Europe ayant publié un certain nombre de documents politiques, de recommandations, de déclarations, de lignes directrices et d'autres instruments juridiques[2]. La Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit est le premier traité international sur l'IA et les droits humains[3]. Elle établit des principes et des obligations visant à garantir que les systèmes d'IA soient pleinement conformes aux droits humains, à la démocratie et à l'État de droit tout au long de leur cycle de vie, tout en étant propices au progrès technologique et à l'innovation[4].

3. Les instruments existants du Conseil de l'Europe en matière de droits humains, tels que la Convention européenne des droits de l'homme et ses protocoles (CEDH) et la Charte sociale européenne (CSE), restent applicables dans le contexte de l'IA. Ces instruments, interprétés respectivement par la Cour européenne des droits de l'homme (« la Cour ») et le Comité européen des droits sociaux (CEDS), établissent des normes de base pour la protection des droits humains. Bien que ni la Cour ni le CEDS n'aient encore abordé directement l'impact de l'IA sur les droits humains, les États membres doivent aligner leurs cadres juridiques sur l'IA avec leurs obligations en vertu de la CEDH et du CSE. Cela est particulièrement crucial pour les domaines spécifiques qui ne sont pas couverts par la Convention-cadre[5] mais qui sont toujours soumis aux dispositions de la CEDH et de la CSE, ainsi que pour les États membres qui ne sont pas parties à la Convention-cadre.

4. Ce Manuel sur les droits humains et l'intelligence artificielle (« le Manuel ») a été conçu comme un outil accessible destiné principalement à aider les fonctionnaires et les responsables politiques des États membres du Conseil de l'Europe à appliquer les normes de la CEDH, de la CSE et d'autres normes pertinentes aux défis liés à l'IA. Compte tenu de la diversité de l'audience des décideurs politiques et des fonctionnaires travaillant dans divers domaines de la gouvernance publique, ce manuel ne présume pas d'une connaissance préalable approfondie de la législation relative aux droits humains ou des questions liées à l'IA. Il ne vise pas non plus à fournir une analyse exhaustive de chaque sujet abordé. En tant que ressource pratique, il donne un aperçu de la manière dont ces normes, ainsi que des instruments tels que la Convention-cadre, peuvent s'appliquer aux activités du cycle de vie des systèmes d'IA. En se concentrant sur les principaux cas d'utilisation de l'IA dans la gouvernance publique, à la fois actuels et raisonnablement prévisibles, il offre un cadre pour évaluer les impacts

---

[1] Voir par exemple la « loi sur l'IA » de l'Union européenne ; la « Recommandation sur l'intelligence artificielle » de l'OCDE adoptée en 2019, révisée en 2023 et 2024 ; la « Recommandation sur l'éthique de l'intelligence artificielle » de l'UNESCO, adoptée en 2021. La résolution A/RES/78/265 de l'Assemblée générale des Nations unies « Saisir les opportunités offertes par des systèmes d'intelligence artificielle sûrs, sécurisés et dignes de confiance pour le développement durable » (21 mars 2024) ; et la résolution A/RES/78/311 sur « Intensifier la coopération internationale en matière de renforcement des capacités dans le domaine de l'intelligence artificielle » (1er juillet 2024).

[2] Pour un aperçu des travaux réalisés jusqu'à présent, ou prévus, par les comités intergouvernementaux et autres entités du Conseil de l'Europe dans le domaine de l'IA, voir Conseil de l'Europe et intelligence artificielle

[3] État des signatures et des ratifications au 16/01/2025 - https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=225

[4] Article 1 – Objet et but, § 1.

[5] Voir ci-dessous, paragraphe [x].

de l'IA sur les droits humains en tenant compte des normes de la CEDH et de la CSE, sans prédire les résultats spécifiques des cas futurs[6].

5. Le chapitre 2 du Manuel présente des concepts techniques clés liant les aspects technologiques de l'IA aux implications en matière de droits humains. Le chapitre 3 expose les principes généraux des droits humains au titre de la CEDH et de la CSE applicables à l'IA dans certains secteurs publics. Il aborde tout d'abord les questions transversales pertinentes pour tous les secteurs. Il fournit ensuite une analyse sectorielle des cas d'utilisation de l'IA dans la gouvernance publique, en examinant les impacts sur les droits humains, les principes juridiques pertinents et les bonnes pratiques des États membres du Conseil de l'Europe. Le Manuel examine également le rôle des entreprises dans la gouvernance de l'IA et étudie comment les décideurs politiques peuvent envisager les intersections public-privé en s'appuyant sur les normes de la CEDH et de la CSE, ainsi que sur d'autres normes internationales. Il se termine au chapitre IV par des réflexions sur les défis émergents en matière de gouvernance de l'IA, garantissant ainsi une approche dynamique et tournée vers l'avenir.

[6] Celles-ci seront fondées sur leurs circonstances factuelles spécifiques, à la lumière de la législation et de la pratique internes pertinentes de l'État membre concerné, et dans le cadre des normes européennes pertinentes qui existeront au moment de l'examen de l'affaire, voir *Zavodnik c. Slovénie,* No. 53723/13, 21 mai 2015, § 74.

2. SYSTÈMES D'IA ET AUTRES CONCEPTS TECHNIQUES PERTINENTS POUR LES DROITS HUMAINS

6. Ce chapitre explique ce que sont les « systèmes d'intelligence artificielle » et leurs fonctions de base, et identifie d'autres concepts techniques pertinents pour les droits humains dans le contexte de ce Manuel. Les définitions fournies ci-dessous s'appuient sur diverses sources[7]. Elles ne sont ni exhaustives ni universelles. Alors que le chapitre suivant offre une compréhension fondamentale, le Manuel utilise une série d'autres termes techniques dans les chapitres III et IV qui sont définis dans le glossaire (voir l'annexe [x])[8].

2.1 Système d'intelligence artificielle

7. « Système d'intelligence artificielle » : un **système basé sur une machine** qui, pour des **objectifs explicites** ou **implicites**, **déduit**, à partir des **données** qu'il reçoit, comment générer des **résultats** tels que des prédictions, du contenu, des recommandations ou des décisions susceptibles d'influencer des **environnements physiques ou virtuels**. Les différents systèmes d'intelligence artificielle varient dans leurs niveaux d'**autonomie** et d'**adaptabilité** après **déploiement**[9].

8. Cette définition reflète une compréhension large de ce que sont les systèmes d'intelligence artificielle (systèmes IA), notamment par opposition à d'autres types de systèmes logiciels traditionnels plus simples, fondés sur des règles définies uniquement par des personnes physiques pour exécuter automatiquement des opérations[10]. La définition ne vise pas à donner une signification universelle au terme concerné[11]. Les technologies de l'IA se développent à un rythme rapide et de nouvelles techniques et applications apparaîtront probablement à l'avenir[12].

2.1.1 Cycle de vie des systèmes d'IA

9. La définition d'un système d'IA adopte une perspective basée sur le cycle de vie. Les activités du cycle de vie des systèmes d'intelligence artificielle peuvent dépendre du type de technologie et d'autres éléments contextuels et évoluer dans le temps. Voici quelques exemples pertinents et non exhaustifs d'activités : (1) planification et conception, (2) collecte et traitement de données, (3) développement de systèmes d'intelligence artificielle, y compris l'élaboration de modèles et/ou l'adaptation de modèles existants à des tâches spécifiques, (4) essais, vérification et validation, (5) fourniture/mise à disposition des systèmes, (6) déploiement, (7) exploitation et surveillance, et (8) mise hors service[13]. Ces activités se déroulent souvent de manière itérative et ne sont pas nécessairement séquentielles. Elles peuvent également recommencer à zéro en cas de modifications substantielles du système ou de son utilisation prévue. La décision de mettre hors service un système d'IA peut intervenir à n'importe quel moment de la phase d'exploitation et de contrôle[14].

---

[7] Convention-cadre, Exposé des motifs accompagnant la définition actualisée d'un système d'intelligence artificielle dans la Recommandation de l'OCDE sur l'intelligence artificielle (OECD/LEGAL/0449, 2019, amendée 2023) (en anglais uniquement). (Exposé des motifs de l'OCDE), Communication à la Commission Approbation du contenu du projet de communication de la Commission - Lignes directrices de la Commission sur les pratiques interdites en matière d'intelligence artificielle telles que définies par la législation (UE) 2024/1689 (en anglais uniquement) ; Glossaire Cyberjustice de la CEPEJ, ISO/IEC 22989:2022 - Technologies de l'information - Intelligence artificielle - Concepts et terminologie de l'intelligence artificielle.

[8] Les définitions correspondent au glossaire de la CEPEJ sur la cyberjustice, qui est basé sur une série d'autres sources.

[9] Convention-cadre, article 2. La définition est tirée de la définition actualisée d'un système d'intelligence artificielle dans la Recommandation de l'OCDE sur l'intelligence artificielle (OECD/LEGAL/0449, 2019, amendée 2023). Cette définition est également utilisée dans l'article 3, paragraphe 1, de la directive européenne sur l'intelligence artificielle. Un aperçu simplifié d'un système d'intelligence artificielle est disponible dans l'exposé des motifs de l'OCDE, p. 7 (en anglais uniquement).

[10] Rapport explicatif, § 24.

[11] Idem. Si cette définition permet aux Parties à la Convention-cadre de s'entendre sur ce que sont les systèmes d'intelligence artificielle, les Parties peuvent la préciser dans leur système juridique interne pour plus de sécurité juridique et de précision, sans pour autant en limiter la portée.

[12] Idem.

[13] Rapport explicatif de la Convention-cadre, § 15.

[14] Idem.

2.1.2 Système basé sur des machines

10. Le terme « basé sur des machines » fait référence au fait que les systèmes d'IA sont développés avec des machines et fonctionnent sur celles-ci. Le terme « machine » peut être compris comme incluant à la fois les composants matériels et logiciels qui permettent au système d'IA de fonctionner. Les composants matériels désignent les éléments physiques de la machine, tels que les unités de traitement, la mémoire, les dispositifs de stockage, les unités de mise en réseau et les interfaces d'entrée/sortie, qui fournissent l'infrastructure nécessaire au calcul. Les composants logiciels englobent le code informatique, les instructions, les programmes, les systèmes d'exploitation et les applications qui gèrent la manière dont le matériel traite les données et exécute les tâches[15].

2.1.3 L'autonomie

11. L'autonomie d'un système d'IA désigne « le degré auquel un système peut apprendre ou agir sans intervention humaine après la délégation de l'autonomie et l'automatisation des processus par les humains. La supervision humaine peut avoir lieu à n'importe quelle étape du cycle de vie du système d'IA »[16]. Certains systèmes d'IA peuvent générer des résultats sans que ceux-ci soient explicitement décrits dans l'objectif du système d'IA et sans instructions spécifiques de la part d'un humain[17].

2.1.4 Capacité d'adaptation

12. La capacité d'adaptation fait référence à la capacité d'un système d'IA à évoluer et à modifier son comportement [et ses données de sortie] par une interaction directe avec les données et les entrées avant ou après le déploiement et est généralement lié aux systèmes d'IA basés sur la technologie d'apprentissage automatique[18]. Il s'agit par exemple d'un système de reconnaissance vocale qui s'adapte à la voix d'un individu ou d'un système de recommandation musicale personnalisé. Les systèmes d'IA peuvent être formés une seule fois, périodiquement ou continuellement et fonctionnent en déduisant des modèles et des relations dans les données. Grâce à cette formation, certains systèmes d'IA peuvent acquérir la capacité d'effectuer de nouvelles formes d'inférence qui n'avaient pas été envisagées au départ par leurs programmeurs[19].

2.1.5 Objectifs du système d'IA

13. Les systèmes d'IA sont conçus pour fonctionner selon un ou plusieurs objectifs. Les objectifs du système peuvent être définis de manière explicite ou implicite. Les objectifs explicites se réfèrent à des buts clairement énoncés qui sont directement encodés par le développeur dans le système. Par exemple, ils peuvent être spécifiés comme l'optimisation d'une fonction de coût, d'une probabilité ou d'une récompense cumulative. Les objectifs implicites sont des buts qui ne sont pas explicitement énoncés mais qui peuvent être déduits du comportement ou des hypothèses sous-jacentes du système. Ces objectifs peuvent découler des données d'apprentissage ou de l'interaction du système d'IA avec son environnement[20].

---

[15] Lignes directrices de la Commission européenne sur la définition d'un système d'intelligence artificielle établi par la loi sur l'IA, paragraphe 11 (en anglais uniquement)
[16] En anglais uniquement ; traduction libre. Exposé des motifs de l'OCDE, p. 6.
[17] Idem.
[18] Pour plus d'informations sur l'apprentissage automatique, voir ISO/IEC 22989:2022, 5.11.
[19] Idem.
[20] Lignes directrices de la Commission européenne sur la définition d'un système d'intelligence artificielle établi par la loi sur l'IA, paragraphe 24 (en anglais uniquement)

2.1.6 Environnement ou contexte

14. Un environnement ou un contexte en relation avec un système d'IA est un espace observable ou partiellement observable, perçu à l'aide de données et d'entrées de capteurs et influencé par des actions (par l'intermédiaire d'actionneurs). Les environnements influencés par les systèmes d'IA peuvent être physiques ou virtuels et inclure des environnements décrivant des aspects de l'activité humaine, tels que les signaux biologiques ou le comportement humain. Les capteurs et les actionneurs sont soit des êtres humains, soit des composants de machines ou d'appareils[21].

2.1.7 Donnée d'entrée

15. Les données d'entrée sont utilisées à la fois pendant le développement et après le déploiement. Les données d'entrée peuvent prendre la forme de connaissances, de règles et de codes que les humains introduisent dans le système au cours du développement ou de données. Les humains et les machines peuvent fournir des données. Au cours du développement, les données sont exploitées pour construire des systèmes d'IA, par exemple avec l'apprentissage automatique qui produit un modèle à partir de données d'apprentissage et/ou de données humaines. Les données sont également utilisées par un système en fonctionnement, par exemple pour déduire comment générer des résultats. Les données d'entrée peuvent inclure des données pertinentes pour la tâche à effectuer ou prendre la forme, par exemple, d'une invite de l'utilisateur ou d'une requête de recherche[22].

2.1.8 Inférence

16. Le concept d'« inférence » fait généralement référence à l'étape au cours de laquelle un système génère des données de sortie à partir de ses données d'entrées, généralement après le déploiement. L'expression « déduire comment générer des sorties » doit être comprise comme faisant également référence à la phase de construction du système d'IA, au cours de laquelle un modèle est dérivé des entrées/données[23].

2.1.9 Donnée de sortie

17. Les données de sortie reflètent généralement les différentes tâches ou fonctions exécutées par les systèmes d'IA. Elles comprennent, sans s'y limiter, la reconnaissance (identification et catégorisation des données, par exemple : image, vidéo, audio et texte, dans des classifications spécifiques, ainsi que la segmentation d'images et la détection d'objets), la détection d'événements (relier des points de données pour détecter des modèles, ainsi que des valeurs aberrantes ou des anomalies), la prévision (utiliser les comportements passés et existants pour prédire les résultats futurs), la personnalisation (développer le profil d'un individu et apprendre et adapter ses résultats à cet individu au fil du temps), l'aide à l'interaction (interprétation et création de contenu pour alimenter les conversations et autres interactions entre les machines et les humains, impliquant éventuellement des médias multiples tels que la voix, le texte et les images), l'optimisation axée sur les objectifs (recherche de la solution optimale à un problème pour une fonction de coût ou un objectif prédéfini) et le raisonnement avec des structures de connaissances (déduction de nouveaux résultats possibles même s'ils ne sont pas présents dans les données existantes, par le biais de la modélisation et de la simulation)[24].

2.2 Autres concepts techniques pertinents pour l'IA et les droits humains

2.2.1 La transparence

[21] Idem, p. 7.
[22] Idem, p. 8.
[23] Idem, p. 9.
[24] Idem, p. 9.

18. La transparence fait référence à l'ouverture et à la clarté dans la gouvernance des activités au cours du cycle de vie des systèmes d'IA. Cela signifie que les processus décisionnels et le fonctionnement général des systèmes d'IA doivent être compréhensibles et accessibles aux acteurs appropriés de l'IA et, le cas échéant, aux parties prenantes concernées[25].

2.2.2 Explicabilité[26]

19. L'explicabilité est une composante particulièrement importante de la transparence. Les systèmes d'IA intégrant des technologies d'apprentissage (« Machine Learning » ou « ML ») ou d'apprentissage supervisé (« Deep Learning » ou « DL ») utilisent des algorithmes formés par leur propre processus, plutôt que par une programmation humaine explicite. Au cours du processus de formation, les modèles d'IA peuvent découvrir de nouvelles corrélations entre certaines caractéristiques d'entrée et peuvent prendre des décisions ou des prédictions basées sur des modèles très complexes impliquant un grand nombre de paramètres en interaction (peut-être des millions), ce qui rend difficile, même pour les experts en IA, de comprendre comment leurs résultats sont produits par la suite[27]. L'opacité ou l'effet « **boîte noire** » qui en résulte pourrait non seulement rend les décisions plus difficiles à comprendre, mais elle peut également avoir un impact direct sur les individus puisqu'elle peut masquer les lacunes dans les systèmes d'IA, telles que l'existence de biais, d'inexactitudes ou de ce que l'on appelle des « hallucinations ».

20. L'« explicabilité » désigne donc la capacité à fournir, sous réserve de faisabilité technique et compte tenu de l'état de la technique généralement reconnu, des explications suffisamment compréhensibles sur raisons pour lesquelles un système d'intelligence artificielle fournit des informations, produit des prédictions, des contenus, des recommandations ou des décisions[28].

2.2.3 Interprétabilité

21. L'interprétabilité fait référence à la capacité de comprendre comment un système d'intelligence artificielle fait ses prédictions ou prend ses décisions ou, en d'autres termes, à la mesure dans laquelle les résultats des systèmes d'intelligence artificielle peuvent être rendus accessibles et compréhensibles pour les experts comme pour les non-experts. Il s'agit de rendre le fonctionnement interne, la logique et les processus décisionnels des systèmes d'intelligence artificielle compréhensibles et accessibles aux utilisateurs humains, y compris les développeurs, les parties prenantes et les utilisateurs finaux, ainsi qu'aux personnes concernées[29].

3. DROITS HUMAINS ET INTELLIGENCE ARTIFICIELLE

3.1 Questions générales

22. Cette section donne un aperçu de la CEDH, de la CSE et de la Convention-cadre en soulignant les principes généraux de la CEDH et de la CSE qui peuvent régir la protection des droits dans le contexte de l'IA. Elle met également en évidence les principes pertinents de la Convention-cadre lorsqu'ils offrent des orientations

[25] Voir le rapport explicatif de la Convention-cadre, § 57.
[26] Voir également ISO/IEC 22989:2022, 5.15.6.
[27] TechDispatch : Explainable Artificial Intelligence, European Data Protection Supervisor(2023), citant Peters, U (en anglais uniquement). Explainable AI lacks regulative reasons : why AI and human decision-making are not equally opaque', (AI and Ethics 2023) ; voir également : CDDH-IA(2024)09, Résumé de l'échange de vues avec des expert.e.s indépendant.e.s externes et des représentant.e.s des comités intergouvernementaux du Conseil de l'Europe (25 septembre), points clés soulevés par Marko Grobelnik ; et CDDH-IA(2024)07, Compilation des contributions écrites et des présentations reçues des experts de l'échange de vues de la 1ère réunion, pp. 3-16.
[28] Rapport explicatif de la Convention-cadre, § 60.
[29] Idem, § 61.

précieuses dans le cadre de la CEDH et de la CSE. En outre, elle examine les défis récurrents en matière de droits humains.

3.1.1 La Convention européenne des droits de l'homme (CEDH)

23. La CEDH est le principal instrument du Conseil de l'Europe en matière de droits humains. Elle fixe des normes contraignantes pour les autorités publiques des États membres. La Cour européenne des droits de l'homme veille à la mise en œuvre de la CEDH par les États. Les particuliers, les groupes, les personnes morales et les organisations non gouvernementales (ONG) peuvent porter plainte devant la Cour pour des violations présumées des droits humains, une fois que toutes les voies de recours internes ont été épuisées. Les droits et libertés protégés par la CEDH et ses protocoles sont énumérés à l'annexe [x].

3.1.2 La Charte sociale européenne (CSE)

24. En tant qu'instrument central des droits économiques et sociaux au sein du Conseil de l'Europe, la CSE garantit des protections fondamentales qui complètent la CEDH. La Charte sociale européenne révisée (CSER) intègre de nouveaux droits et amendements. 42 des 46 États membres du Conseil de l'Europe sont parties à la CSE ou à la CSER[30]. Le Comité européen des droits sociaux (CEDS) assure le suivi de la Charte par le biais de deux mécanismes : (i) les rapports réguliers des États parties sur leur mise en œuvre de la CSE et (ii) les réclamations collectives déposées par les partenaires sociaux et les organisations non gouvernementales (ONG), pour les États ayant ratifié le Protocole additionnel de 1995 instituant un système de réclamations collectives[31]. Bien que ses décisions et conclusions ne soient pas directement exécutoires, elles représentent une interprétation faisant autorité des dispositions de la CSE. Les États parties ont l'obligation de coopérer avec le CEDS et de mettre en œuvre ses décisions et conclusions qui découlent de l'application du principe de bonne foi au respect de leurs obligations conventionnelles en vertu de la CSE. Les droits protégés par la CSE sont énumérés à l'annexe [x].

3.1.3 La Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit

25. La Convention-cadre renforce les normes internationales existantes (telles que la CEDH et la CSE). Elle adopte une approche neutre sur le plan technologique, en se concentrant sur les principes plutôt qu'en réglementant des technologies spécifiques. Elle s'applique aux activités menées par les autorités publiques (y compris les acteurs privés agissant en leur nom)[32]. En ce qui concerne les activités menées par des acteurs privés agissant de manière indépendante, les États parties s'engagent à traiter les risques et les impacts d'une manière conforme à l'objet et au but de la Convention-cadre, soit en appliquant directement les principes et obligations énoncés dans la Convention, soit en prenant « d'autres mesures appropriées »[33]. En outre, les questions relatives à la défense nationale n'entrent pas dans le champ d'application du traité[34], ainsi que : (i) les activités liées à la protection des « intérêts de sécurité nationale » des États parties, étant entendu que ces activités sont menées d'une manière conforme au droit international applicable, y compris aux obligations internationales en matière de droits humains, et dans le respect de ses institutions et processus démocratiques[35] ; (ii) les activités de recherche et de développement, à moins que les essais ou activités similaires ne soient entrepris d'une manière susceptible de porter atteinte aux droits humains, à la démocratie et à l'État de droit[36].

---

[30] Le Liechtenstein, Monaco, Saint-Marin et la Suisse ne sont parties à aucun de ces traités.
[31] 16 des 42 parties à la CSE ont ratifié ce protocole additionnel.
[32] Article 3, paragraphe 1 (a).
[33] Article 3, paragraphe 1 (B).
[34] Article 3, paragraphe 4. Notez également qu'en vertu de l'article 1.d. de son statut, « les questions relatives à la défense nationale ne relèvent pas du Conseil de l'Europe ».
[35] Article 3, paragraphe 2.
[36] Article 3, paragraphe 3.

26. Les activités du cycle de vie des systèmes d'IA doivent respecter les principes suivants[37] :

- Dignité humaine et autonomie personnelle
- Transparence et contrôle
- Obligation de rendre des comptes et responsabilité
- Égalité et non-discrimination
- Respect de la vie privée et protection des données à caractère personnel
- Fiabilité
- Innovation sûre

27. Les principales exigences comprennent la mise à disposition de voies de recours en cas de violation des droits humains par l'IA[38], la garantie de garanties procédurales pour les personnes concernées, y compris la notification des personnes interagissant avec les systèmes d'IA[39] ; la réalisation d'évaluations des risques et des incidences sur les droits humains, la démocratie et l'État de droit[40], et la possibilité d'interdire, de suspendre ou de prendre d'autres mesures appropriées à l'égard de certaines utilisations des systèmes d'IA que l'État partie considère comme incompatibles avec le respect des droits humains, le fonctionnement de la démocratie ou l'état de droit.[41] La Convention-cadre prévoit également des mécanismes de suivi et de coopération et introduit un mécanisme de contrôle obligatoire.[42]

3.1.4 Les principes généraux de la CEDH et de la CSE dans le contexte de l'IA

28. Ni la Cour ni le CEDS n'ont encore directement abordé la question de l'impact de l'IA sur les droits garantis par la CEDH et la CSE.[43] Cependant, les principes établis dans le cadre de la CEDH et de la CSE fournissent des indications sur la manière dont ces traités peuvent s'appliquer aux défis liés à l'IA en matière de droits humains. Si certains principes se chevauchent, d'autres sont spécifiques à chaque traité. [44]

Protection effective des droits

29. La CEDH et la CSE visent à garantir des droits qui ne sont pas simplement théoriques ou illusoires, mais pratiques et effectifs[45]. Les autorités nationales doivent veiller à ce que les détenteurs de droits puissent effectivement jouir de leurs droits, ce qui implique non seulement d'adopter une législation, mais aussi de veiller

[37] Chapitre III (articles 6 à 13)
[38] Chapitre IV (article 14)
[39] Article 15 : « Lorsqu'un système d'intelligence artificielle contribue en grande partie à la prise des décisions ou prend des décisions ayant un impact sur les droits de l'homme, des garanties procédurales effectives devraient, par exemple, inclure un contrôle humain, y compris un examen ex ante ou ex post de la décision par des êtres humains. » (Rapport explicatif, § 103).
[40] Chapitre V (article 16).
[41] Article 16, paragraphe 4.
[42] Chapitre VII (articles 23 à 26).
[43] Bien que la Cour n'ait pas encore abordé directement l'IA, elle a examiné des affaires impliquant de nouvelles technologies et leur impact sur les droits humains, y compris les technologies intégrant des fonctionnalités d'IA, telles que les systèmes de reconnaissance faciale.
(voir *Glukhin c. Russie*, Requête No. 11519/20, 4 juillet 2023 ; voir également Factsheet – New technologies (en anglais uniquement)).
[44] Les systèmes conventionnels de la CEDH et de la CSE sont complémentaires et interdépendants. La Cour a précisé qu'il n'y a pas de division étanche entre les droits civils et politiques et les droits économiques, sociaux et culturels. Voir *Airey c. Irlande*, 9 octobre 1979, 6289/73, § 24 ; voir aussi Digest of Case Law of the European Committee of Social Rights, décembre 2022, p. 33.
[45] *Airey c. Irlande*, No. 6289/73, 9 octobre 1979, § 24 ; *Commission internationale de juristes (CIJ) c. Portugal*, réclamation No. 1/1998, décision sur le bien-fondé du 9 septembre 1999, § 32 ; *Fédération européenne des associations nationales travaillant avec les sans-abris (FEANTSA) c. Slovénie*, réclamation No. 53/2008, décision sur le bien-fondé du 8 septembre 2009, § 28.

à son application effective, de fournir des ressources adéquates et d'établir des procédures opérationnelles appropriées. En conséquence, les États devraient garantir la protection effective des droits humains contre les atteintes liées aux activités relevant du cycle de vie des systèmes d'IA, non seulement en appliquant les lois, mais aussi en fournissant des ressources, en créant ou en désignant des structures nationales de défense des droits humains existantes, telles que les institutions nationales des droits de l'homme (INDH), en tant que mécanismes de contrôle indépendants, et en assurant une coopération efficace entre ces mécanismes et les autres structures nationales de défense des droits humains.

Subsidiarité et la marge d'appréciation

30. La subsidiarité signifie que les États ont la responsabilité première de garantir à toute personne relevant de leur juridiction les droits et libertés définis dans la CEDH.[46] La Cour interprète la CEDH avec autorité et sert de garde-fou aux personnes dont les droits et libertés ne sont pas garantis au niveau national.[47]

31. Les autorités nationales peuvent bénéficier d'une « marge d'appréciation » dans la manière dont elles appliquent et mettent en œuvre la CEDH, en fonction des circonstances de l'affaire et des droits et libertés en jeu. Cela reflète le fait que le système de la CEDH est subsidiaire par rapport à la sauvegarde des droits humains au niveau national et que les autorités nationales sont en principe mieux placées qu'une cour internationale pour évaluer les besoins et les conditions locales[48]. En vertu de la Charte, les États parties disposent également d'un pouvoir discrétionnaire pour déterminer les mesures à prendre pour se conformer à ses dispositions, en mettant en balance les intérêts généraux avec les besoins de groupes spécifiques et les ressources disponibles. L'étendue de la marge d'appréciation dont jouissent les autorités nationales dépend de la nature des droits en jeu et de la gravité de la menace que l'acte ou l'omission en question ferait peser sur ces droits. En ce qui concerne les nouvelles technologies, en particulier, tout État qui revendique un rôle de pionnier dans leur développement a la responsabilité particulière de trouver le juste équilibre entre les avantages potentiels de leur utilisation à grande échelle et les droits protégés[49].

Interprétation évolutive et doctrine de l'instrument vivant

32. La CEDH et la CSE sont des « instruments vivants », interprétés de manière dynamique à la lumière des conditions actuelles pour répondre aux enjeux sociétaux et technologiques en constante évolution[50]. Les arrêts antérieurs de la Cour sur des sujets tels que l'interception des données[51], les données biométriques[52], internet et les outils numériques[53] ou la technologie de reconnaissance faciale[54] mettent en évidence sa capacité à adapter les droits aux défis modernes. De même, le CEDS a abordé le droit à la vie privée dans le contexte des nouvelles technologies émergentes[55]. En appliquant cette doctrine, la Cour et le CEDS devraient tous deux appliquer la CEDH et la CSE aux affaires liées à l'IA à l'avenir.

---

[46] CEDH, préambule, considérant 7.
[47] Rapport explicatif, Protocole No. 15 portant amendement à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (STCE No. 213), para. 8
[48] Idem, para. 9
[49] *S. et Marper c. Royaume-Uni* [GC], No. 30562/04 et 30566/04, 4 décembre 2008, § 112 : « La Cour considère que tout Etat qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière. »
[50] *Tyrer c. Royaume-Uni*, No. 5856/72, 25 avril 1978, § 31 ; *Transgender-Europe et ILGA-Europe c. République tchèque*, No. 117/2015, 15 mai 2018, §75 ; *Défense des enfants international (DEI) c. Pays-Bas*, No. 47/2008, 20 octobre 2009, §29.
[51] *Big Brother Watch et autres c. Royaume-Uni* [GC], Nos. 58170/13, 62322/14 et 24960/15, 25 mai 2021.
[52] *S. et Marper c. Royaume-Uni* [GC], nos 30562/04 et 30566/04, 4 décembre 2008.
[53] *Ahmet Yıldırım c. Turquie*, No. 3111/10, 18 mars 2013 ; *Magyar Helsinki Bizottság c. Hongrie* [GC], No. 18030/11, 8 novembre 2016.
[54] *Glukhin c. Russie*, No. 11519/20, 4 juillet 2023.
[55] CEDS, Conclusions 2012, Statement of Interpretation on Article 1§2 (en anglais uniquement)

Obligations positives

33. Les États ont le devoir, en vertu de la CEDH et de la CSE, de s'abstenir de toute ingérence injustifiée dans les droits humains (« obligations négatives ») et d'assurer leur réalisation et leur protection effectives (« obligations positives »). Les obligations positives de fond exigent les mesures de base nécessaires à la pleine jouissance des droits garantis (par exemple, des règles appropriées régissant l'intervention de la police ou interdisant les mauvais traitements). Les obligations positives de procédure exigent des procédures nationales pour assurer la protection des détenteurs de droits (par exemple, mener une enquête efficace).

34. Les obligations positives s'appliquent même dans les cas où les menaces proviennent de personnes privées ou d'entités échappant au contrôle direct de l'État, car ces instruments concernent à la fois les relations verticales - entre les autorités nationales et les individus - et les relations horizontales[56], qui impliquent des interactions entre les individus ou les entités. Les États doivent protéger les droits humains dans la sphère des relations entre les individus eux-mêmes (effet horizontal). Cette obligation revêt une importance particulière dans le contexte du déploiement des systèmes d'IA, où les partenariats public-privé et les achats auprès d'acteurs privés sont prédominants

35. Les obligations positives imposent un devoir de comportement et non de résultat. Les États doivent agir avec diligence et de manière raisonnable, en prenant les mesures appropriées dans la limite de leurs ressources et de leurs capacités. Les obligations positives peuvent exiger de l'État qu'il impose des sanctions aux personnes ou entités qui violent la CEDH, qu'il adopte des règles juridiques spécifiques et/ou qu'il prenne des mesures opérationnelles pour protéger les personnes contre les risques prévisibles pour leurs droits[57].

36. Les obligations positives des États leur imposent d'évaluer de manière proactive si les systèmes d'IA sont susceptibles de porter atteinte aux droits humains et d'adopter une législation et/ou de mettre en œuvre des mesures pour atténuer les risques. La Convention-cadre contient une disposition spécifique prescrivant la nécessité d'identifier, d'évaluer, de prévenir et d'atténuer ex ante et, le cas échéant, de manière itérative tout au long du cycle de vie du système d'IA, les risques pertinents et les impacts potentiels sur les droits humains, la démocratie et l'État de droit en suivant et en permettant le développement d'une méthodologie avec des critères concrets et objectifs pour de telles évaluations[58].

Dignité humaine

37. Le respect de la dignité humaine implique le respect de la valeur inhérente à chaque individu, indépendamment de ses antécédents, de ses caractéristiques ou de sa situation, et se réfère en particulier à la manière dont tous les êtres humains doivent être traités[59].

---

[56] La Cour a reconnu le devoir des États de protéger les droits humains dans ces contextes horizontaux, tels que le droit au respect de la vie privée et familiale (article 8 de la CEDH), voir *X et Y c. Pays-Bas,* No. 8978/80, 26 mars 1985, § 23 *;* la liberté d'expression (article 10 de la CEDH), voir *Plate-forme " Ärzte für das Leben " c. Autriche*, No. 10126/82, 21 juin 1986, § 23 ; et la liberté d'association (article 11 de la CEDH), voir *Khurshid Mustafa et Tarzibachi c. Suède*, No. 23883/06, 16 décembre 2008, § 32 ; *Parti populaire chrétien-démocrate c. Moldova* (nº 2), No. 25196/04, 2 février 2010, § 25.

[57] Pour la CEDH, voir par exemple, *Osman c. Royaume-Uni* [GC], nos 87/1997/871/1083, § 115. Pour la CSE, voir, par exemple, CEDS, Conclusions 2020, Albanie sur l'article 1§2, Conclusions 2005, Déclaration interprétative sur l'article 11, *Fédération internationale pour la planification familiale - Réseau européen (IPPF EN) c. Italie*, réclamation No. 87/2012, décision sur le fond du 10 septembre 2013, §66 ; voir également *Confédération générale italienne du travail (CGIL) c. Italie*, No. 91/2013, 12 octobre 2015, §162 et 190.

[58] Article 16 de la Convention-cadre, voir également le Rapport explicatif, § 105.

[59] Rapport explicatif sur la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (Rapport explicatif), §54.

38. Dans le système de la CEDH, la dignité humaine est invoquée par la Cour pour affirmer la valeur intrinsèque et l'égalité des individus[60]. La Cour a déclaré que « le respect de la dignité humaine fait partie de l'essence même de la Convention »[61]. Le système de la CSE reconnaît également que la dignité humaine est centrale à la réalisation effective des droits économiques et sociaux et constitue un principe fondamental dont il ne peut être dérogé[62].

39. La Convention-cadre exige également que le respect de la dignité humaine figure parmi les principes qui régissent l'intelligence artificielle.[63] Les activités du cycle de vie de l'IA ne doivent pas déshumaniser les individus, porter atteinte à leur autonomie ou les réduire à des points de données, et l'IA ne doit pas être anthropomorphisée d'une manière qui porte atteinte à la dignité humaine[64].

Autonomie personnelle et autodétermination

40. L'autonomie personnelle est un principe important qui sous-tend l'interprétation des garanties de la CEDH[65]. Elle constitue un aspect important de la dignité humaine et renvoie à la capacité d'autodétermination des individus, c'est-à-dire à leur aptitude à faire des choix et à prendre des décisions, y compris sans contrainte, et à vivre leur vie librement. Dans le contexte de l'IA, l'autonomie individuelle exige que les individus aient le contrôle de l'utilisation et de l'impact des technologies de l'IA dans leur vie, et que leur agence et leur autonomie ne soient pas diminuées pour autant[66]. La Convention-cadre exige également expressément que le respect de l'autonomie individuelle figure parmi les principes qui régissent l'intelligence artificielle[67].

Légalité, but légitime, nécessité, proportionnalité et juste équilibre

41. Certains droits de la CEDH sont absolus et ne peuvent faire l'objet de dérogations en cas d'urgence, d'exception ou d'ingérence autorisée. Toutefois, les États parties sont autorisés à restreindre certains droits énoncés dans la CEDH[68] et la CSE[69], mais uniquement si l'ingérence peut être justifiée. La CEDH et la CSE contiennent certaines exigences générales qui s'appliquent à presque tous les droits. L'ingérence doit être (i) 'prévue par la loi' ou 'conforme à la loi' (condition de légalité)[70]. Cela signifie qu'elle doit avoir une base claire dans le droit national, garantissant qu'elle est ancrée dans des cadres juridiques établis. En outre, la base juridique doit être accessible au public, ce qui signifie que les individus peuvent connaître et comprendre les lois

[60] ***Lăcătuş c. Suisse***, requête, No. 14065/15, fond et satisfaction équitable, 19 janvier 2021.
[61] *Magyar Helsinki Bizottság c. Hongrie* [GC], No. 18030/11, fond et satisfaction équitable, 8 novembre 2016, paragraphe 155.
[62] *Fédération internationale pour les droits humains (FIDH) c. France*, No. 14/2003, 8 septembre 2004, §31.
[63] Convention-cadre, article 7.
[64] Rapport explicatif, § 53.
[65] *Pretty c. Royaume-Uni*, No. 2346/02, § 61 et arrêt [GC] du 11 janvier 2006, *Sorensen et Rasmussen c. Danemark*, No. 52562/99 et 52620/99, § 54.
[66] Rapport explicatif de la Convention-cadre, §55.
[67] Convention-cadre, article 7.
[68] Aucune dérogation n'est autorisée en temps de guerre à certaines dispositions de la CEDH et de ses protocoles : le droit à la vie en vertu de l'article 2 (sauf en cas de décès résultant d'actes de guerre licites) ; l'interdiction de la torture et des peines ou traitements inhumains ou dégradants en vertu de l'article 3 ; l'interdiction de l'esclavage et de la servitude en vertu de l'article 4 (mais pas l'interdiction du travail forcé ou obligatoire en vertu de l'article 4(2)) ; l'interdiction des peines non prévues par la loi en vertu de l'article 7 ; l'abolition de la peine de mort en temps de paix (Protocole No. 6, article 1) ; le droit de ne pas être jugé ou puni deux fois (ne bis in idem) (Protocole No. 7, article 4) ; et l'abolition de la peine de mort en toutes circonstances (Protocole No. 13, article 1). La Convention prévoit des exceptions à certains droits, comme le droit de ne pas être arbitrairement privé de liberté en vertu de l'article 5. Dans de tels cas, la Cour a clairement établi que la liste des exceptions dans un article donné est exhaustive et que seule une interprétation étroite de ces exceptions est conforme à l'objectif de cet article.
[69] Les États parties sont autorisés à restreindre les droits inscrits dans la Charte sociale européenne. Ces conditions de restriction sont énoncées à l'article 31 de la CSE et l'article G de la Charte sociale européenne révisée.
[70] Leyla Şahin c. Turquie [GC], Requête No. 44774/98, 10 novembre 2005, § 88 (avec de nombreuses autres références) ; Biržietis c. Lituanie, Requête No. 49304/09, 14 juin 2016, § 50.

qui affectent leurs droits.[71] L'ingérence doit également être prévisible, ce qui permet aux personnes d'anticiper comment et quand leurs droits pourraient être restreints[72]. Enfin, elle doit être exempte d'arbitraire et mise en œuvre avec des garanties procédurales appropriées pour assurer l'équité et la diligence[73]. L'ingérence dans le droit doit (ii) poursuivre un but légitime[74] et elle doit être (iii) nécessaire (dans une société démocratique) pour atteindre le but légitime poursuivi[75].

42. Les États devront démontrer que toute restriction des droits de la CEDH ou des droits économiques, sociaux et culturels résultant d'activités du cycle de vie des systèmes d'IA qui s'apparentent à une ingérence est légale, poursuit des objectifs légitimes et est nécessaire dans une société démocratique. Les limitations doivent être proportionnées à l'objectif légitime poursuivi, répondre à des besoins sociaux urgents et utiliser les moyens les moins restrictifs.

3.1.5 Principales questions relatives aux droits humains dans les secteurs de la gouvernance publique

43. L'utilisation des systèmes d'IA a un impact sur une série de droits humains, certaines questions émergeant systématiquement dans tous les contextes. Il s'agit notamment des risques pour (i) la non-discrimination et l'égalité ; (ii) la protection des données personnelles et de la vie privée ; et (iii) la capacité à contester efficacement les décisions fondées sur l'IA et les voies de recours effectives. Les obligations concurrentes en matière de droits humains dans le contexte de l'IA peuvent également poser problème dans différents secteurs. Ces défis récurrents sont des préoccupations transversales en matière de droits humains dans le cycle de vie des systèmes d'IA et ne se limitent donc pas à un ou plusieurs secteurs publics.

Non-discrimination et égalité

i. L'interdiction de la discrimination dans la CEDH et la CSE

44. La CEDH[76] et la CSE[77] interdisent la discrimination, mais uniquement en ce qui concerne la jouissance des droits et libertés énoncés dans les traités respectifs. L'article 1 du protocole n° 12 de la CEDH introduit une interdiction plus large de la discrimination, couvrant « tout droit prévu par la loi [nationale] »[78]. Les motifs de discrimination explicitement mentionnés dans ces instruments sont « le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation ». La notion d'« autre statut » signifie que les motifs énumérés ne sont pas exhaustifs. La Cour a interprété l'expression « autre situation » de manière extensive et à la lumière des conditions actuelles pour y inclure des caractéristiques telles que la nationalité, l'origine ethnique, le sexe, l'orientation sexuelle, l'identité et l'expression de genre, les caractéristiques sexuelles, l'âge, l'état de santé, le handicap, l'état matrimonial, le statut de migrant ou de réfugié[79]. L'interdiction de la discrimination s'applique dans les relations verticales et horizontales. La discrimination peut être directe ou indirecte. La discrimination directe résulte d'une différence de traitement entre « des personnes placées dans des situations analogues ou similaires »[80] et lorsque cette différence est « fondée sur une caractéristique

[71] *The Sunday Times c. Royaume-Uni* (No. 1), requête No. 6538/74, 26 avril 1979, § 48.
[72] Idem.
[73] *R.Sz. c. Hongrie*, requête No. 41838/11, 2 juillet 2013, § 36.
[74] *S.A.S. c. France* [GC], Requête No. 43835/11, 1er juillet 2014, § 114 ; *Merabishvili c. Géorgie* [GC], Requête No. 72508/13, 28 novembre 2017, §§ 295-296.
[75] *Vavřička et autres c. République tchèque* [GC], Nos. 47621/13 et 5 autres, 8 avril 2021, §§ 273-275 ; *Association internationale Autisme-Europe (AIAE) c. France*, No. 13/2000, 4 novembre 2003, § 52
[76] Article 14 de la CEDH.
[77] Article E de la CSER.
[78] Ce protocole a été ratifié par 20 États membres du Conseil de l'Europe
[79] Voir le Rapport explicatif de la Recommandation CM/Rec(2024)7 du Comité des Ministres aux États membres sur la protection effective des droits humains dans les situations de crise.
[80] *Burden c. Royaume-Uni* [GC], No. 13378/05, 29 avril 2008, § 60.

identifiable ».[81] La discrimination indirecte se produit lorsque la législation en question, apparemment neutre, affecte de manière disproportionnée et injustifiée un groupe particulier de personnes[82].

45. Le principe d'égalité et de non-discrimination de la convention-cadre[83] se réfère au « risque réel et bien documenté de biais pouvant constituer une discrimination illicite découlant des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle. »[84], et sa disposition relative à la non-discrimination interdit explicitement la discrimination dans la mise en œuvre de la Convention[85]. Elle s'inspire directement de normes internationales établies, notamment de la CEDH et de la CSE[86].

ii. Risques pour la non-discrimination et l'égalité

46. Les systèmes d'IA peuvent présenter des risques pour l'égalité et la non-discrimination, car ils peuvent construits et soutenus par des données et des modèles qui reproduisent, perpétuent et exacerbent les préjugés, les stéréotypes, la stigmatisation, les préjudices et les fausses hypothèses existants sur les individus, sur la base de caractéristiques personnelles réelles ou perçues et de leurs intersections. Ces effets peuvent être encore aggravés par des asymétries d'information et peuvent être plus graves pour les personnes en situation de vulnérabilité. Entre autres, un tel effet peut entraîner une augmentation de la violence en ligne et hors ligne contre ces personnes, ainsi que contre les femmes, qui sont ciblées de manière disproportionnée en raison des inégalités entre les sexes, des stéréotypes et des déséquilibres de pouvoir existants que les systèmes d'IA peuvent involontairement amplifier[87].

47. Les systèmes d'IA peuvent être sujets à la discrimination par procuration. Cela signifie que des informations apparemment neutres qui sont indirectement liées à des caractéristiques protégées peuvent dissimuler des préjugés, ce qui rend de plus en plus difficile la traçabilité et la détection d'une discrimination par procuration basée sur l'IA. Par exemple, l'utilisation de variables telles que les codes postaux ou les habitudes de consommation, semblent neutres mais peuvent refléter indirectement des caractéristiques telles que l'origine ethnique, le genre ou le statut socio-économique, pouvant rendre difficile la traçabilité et la détection d'une discrimination indirecte basée sur l'IA[88]. Une autre préoccupation concerne la capacité des systèmes d'IA à opérer une discrimination intersectionnelle, c'est-à-dire lorsque plusieurs motifs de discrimination se recoupent[89].

---

[81] *Biao c. Danemark [GC],* No. 38590/10, § 89.
[82] *D.H. et autres c. République tchèque* [GC], No. 57325/00, 13 novembre 2007.
[83] Convention-cadre, article 10.
[84] Rapport explicatif, § 75.
[85] Convention-cadre, article 17.
[86] Rapport explicatif, § 71.
[87] Plusieurs instruments juridiques non contraignants ont été adoptés pour lutter contre cette violence, notamment la Recommandation générale No. 1 du Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO) sur la dimension numérique de la violence à l'égard des femmes. Le Conseil de l'Europe [a également élaboré] un instrument spécifique sur [la lutte contre] la violence à l'égard des femmes et des filles, facilitée par la technologie. L'annexe [x] du manuel fournit de plus amples informations sur les initiatives conclues, en cours ou à venir [à compléter].

[88] D'autres exemples de variables de substitution incluent la pointure de chaussure comme variable de substitution du sexe, les noms comme variable de substitution de l'origine ethnique ou de l'âge, la profession comme variable de substitution du sexe, etc. Voir Agence des droits fondamentaux de l'Union européenne, Bias in Algorithms – Artificial Intelligence and Discrimination (2022), p. 24. Pour d'autres exemples, voir le Fundamental Rights Agency, Bias in Algorithms – Artificial Intelligence and Discrimination, (2022), p. 24 et voir le Report of the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance A/HRC/56/68 publié le 3 juin 2024, paragraphes 18, 32, 40 ; *Discrimination, intelligence artificielle et prise de décision algorithmique, étude du* Conseil de l'Europe, Direction générale de la démocratie, 2018.
[89] Voir l'Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel de promotion de l'égalité, y compris l'égalité de genre, et les risques qu'ils peuvent entraîner en matière de non-discrimination (2023), p. 67, « En raison de la granularité du profilage algorithmique, les systèmes d'IA sont capables de déduire plusieurs appartenances sociales protégées et de regrouper potentiellement les utilisateurs en fonction de différentes classifications problématiques. Par exemple, les profils algorithmiques peuvent contenir des informations concernant le sexe, l'âge, l'origine ethnique, les croyances religieuses,

Le droit à la vie privée et à la protection des données à caractère personnel

i. Le droit à la vie privée et à la protection des données dans la CEDH et d'autres instruments pertinents

48. L'article 8 (droit au respect de la vie privée et familiale), par le biais de protection de la vie privée, s'applique à la collecte et au traitement des données à caractère personnel[90]. La vie privée comprend, entre autres, l'image, l'identité, le développement personnel et les relations d'une personne, et s'étend également aux activités professionnelles ou commerciales. Les données à caractère personnel couvrent des informations telles que les noms, les adresses, les adresses IP, ainsi que des données sensibles telles que les informations relatives à la santé et à l'origine ethnique. La Cour a également abordé la question de l'interception des communications, telles que les courriels et les appels téléphoniques, sous l'angle de ce droit. Elle a estimé que de telles mesures constituent une ingérence dans le droit à la vie privée et qu'elles doivent être légales, poursuivre un but légitime, être nécessaires et proportionnelles.

49. La Convention n° 108 du Conseil de l'Europe et son protocole d'amendement (la convention 108(+) 'modernisée')[91] protègent les individus en ce qui concerne le traitement automatique des informations à caractère personnel les concernant[92]. La Convention n° 108 définit les données à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable »[93]. Les principes clés du traitement des données personnelles sont la légalité, la loyauté, la limitation des finalités, la minimisation des données, l'exactitude et le contrôle de l'utilisateur sur ses informations. Les personnes doivent être informées de la manière dont leurs données sont collectées et traitées et conserver le droit d'en demander la correction ou l'effacement. Le consentement, qui doit être libre, spécifique et éclairé, joue un rôle central dans la légitimation du traitement des données[94]. La Cour s'est référée aux normes de la Convention n° 108 dans ses arrêts concernant la protection des données.[95]

50. La Convention-cadre oblige les parties à adopter ou à maintenir des mesures garantissant la protection de la vie privée et des données à caractère personnel tout au long du cycle de vie des systèmes d'IA[96]. Il s'agit notamment de se conformer aux lois nationales et internationales applicables, telles que la CEDH et la Convention n° 108[97].

ii. Risques liés à la protection de la vie privée et des données

---

l'orientation sexuelle ou l'identité de genre, sur la base de l'analyse des comportements en ligne, des préférences des consommateur·ices, etc. »

[90] Pour la jurisprudence de la Cour sur la protection des données personnelles, voir T-PD(2023)1 Jurisprudence sur la protection des données (décembre 2022) et le Guide sur l'article 8 de la Convention européenne des droits de l'homme.

[91] STCE No. 223.

[92] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE No. 108)

[93] Article 2.

[94] La Convention 108 (+) actualisée renforce ces protections en relevant les défis numériques émergents et en mettant l'accent sur la responsabilité des responsables du traitement des données et des sous-traitants.

[95] *Z. c. Finlande*, No. 22009/93, 25 février 1997§ 95, ; *Amann c. Suisse* [GC], No. 27798/95, 16 février 2000, § 65 ; *Rotaru c. Roumanie* [GC], No. 28341/95, 4 mai 2000, § 43 ; *P.G. et J.H. c. Royaume-Uni*, No. 44787/98, 25 décembre 2001, § 57 ; *Sofianopoulos et autres c. la Grèce* (déc.), No. 1977/02, 1988/02 et 1997/02, 16 février 2000 ; *Peck c. Royaume-Uni*, No. 44647/98, 28 avril 2003, § 78, ; *Von Hannover c. Allemagne*, No. 59320/00, 24 septembre 2004, § 42 ; *Cemalettin Canlı c. Turquie*, No. 22427/04, 18 février 2009, §§ 17 et 34 ; *S. et Marper c. Royaume-Uni*, No. 30562/04 et 30566/04, 4 décembre 2008, §§ 41, 66, 68, 76, 103, 104 et 107 ; *Uzun c. Allemagne*, No. 35623/05, 2 septembre 2010, § 47.

[96] Article 11.

[97] Rapport explicatif, §§ 80-82.

51. La protection des données et le droit à la vie privée sont des questions transversales dans le contexte de l'IA, car ces systèmes reposent largement sur la collecte, le traitement et l'analyse de grandes quantités de données qui peuvent inclure des données personnelles. Les risques comprennent l'utilisation non autorisée des données, des garanties inadéquates et des décisions de traitement des données personnelles prises à l'insu des personnes ou sans leur consentement, ce qui menace la vie privée et la protection des données personnelles. En outre, les systèmes d'IA pourraient être utilisés pour la surveillance de masse (y compris la surveillance biométrique) ou le profilage.

52. La protection des droits à la vie privée et des données personnelles est un principe commun nécessaire à la réalisation effective de nombreux autres principes de la Convention-cadre[98]. Des garanties efficaces sont nécessaires pour faire face à des risques tels que la collecte non autorisée de données, leur utilisation abusive et l'atteinte à la dignité des personnes[99]. Les États devraient adopter ou maintenir des mesures tout au long du cycle de vie de l'IA, afin de garantir que les droits à la vie privée et les données personnelles des individus sont protégés, notamment par le biais des lois, normes et cadres nationaux et internationaux applicables, et que des garanties efficaces sont en place conformément aux obligations nationales et internationales[100]. Les lignes directrices 2019 sur l'intelligence artificielle et la protection des données[101] fournissent des orientations supplémentaires aux décideurs politiques et aux développeurs d'IA. Celles-ci prévoient notamment que le développement de l'IA impliquant des données à caractère personnel doit respecter les principes de la Convention 108+, notamment la licéité, l'équité, la spécification de la finalité, la proportionnalité, la protection de la vie privée dès la conception et par défaut, la responsabilité, la transparence, la sécurité des données et la gestion des risques. Les applications d'IA doivent respecter pleinement les droits des personnes concernées, en particulier en vertu de l'article 9 de la Convention 108+, et garantir un contrôle significatif du traitement des données et de son impact sociétal. En outre, il convient d'encourager la coopération entre les autorités de contrôle de la protection des données et les autres organismes compétents en matière d'IA, tels que les organismes de protection des consommateurs, de la concurrence et de la lutte contre la discrimination, les régulateurs sectoriels et les autorités de régulation des médias.

53. En ce qui concerne la gestion des données pour les systèmes algorithmiques, l'annexe de la Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme souligne que les États devraient veiller à ce que la conception, le développement et le déploiement continu des systèmes algorithmiques permettent aux individus d'être informés à l'avance du traitement des données qui y est associé (y compris ses finalités et ses résultats possibles) et de contrôler leurs données, notamment grâce à l'interopérabilité.

Des recours effectifs

i. Le droit à un recours effectif

54. L'article 13 de la CEDH garantit à toute personne le droit à un recours effectif en cas de violation des droits et libertés qui lui sont reconnus par la CEDH. Les recours doivent être disponibles et capables de traiter la substance de la violation alléguée et de fournir une réparation appropriée[102]. Les recours doivent être efficaces

[98] Rapport explicatif, § 79

[99] La recommandation CM/Rec(2021)8 sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage met en avant le droit des personnes physiques de s'opposer au profilage et exige des garanties solides, en particulier lorsque le profilage affecte de manière significative leurs droits.

[100] Convention-cadre, article 11.

[101] Adopté par le Comité consultatif de la Convention 108.

[102] *Boyle et Rice c. Royaume-Uni*, 27 avril 1988, No. 9659/82 et 9658/82, § 52 ; *Powell et Rayner c. Royaume-Uni*, 21 février 1990, § 31 ; M.S.S. *c. Belgique et Grèce* [GC], No. 30696/09, 21 janvier 2011, § 288 ; *De Souza Ribeiro c. France* [GC], 2012, No. 22689/07, 13 décembre 2012, § 78 ; *Centre for Legal Resources au nom de Valentin Câmpeanu c. Roumanie* [GC], 17 juillet 2014, § 148.

en droit et en pratique, accessibles, abordables et capables d'offrir une réparation appropriée[103]. Il peut s'agir de mécanismes judiciaires ou d'un organe quasi judiciaire tel qu'un médiateur[104], ou d'une autorité politique telle qu'une commission parlementaire[105]. Ces instances doivent être indépendantes et des garanties procédurales doivent être accordées au requérant[106]. Toutefois, la Cour peut exceptionnellement juger qu'un recours devant une autorité judiciaire est essentiel (par exemple en ce qui concerne l'isolement cellulaire) ou souhaitable[107]. En outre, les États sont tenus de veiller à ce que les individus aient accès à des mécanismes judiciaires ou non judiciaires pour traiter les violations des droits humains par des acteurs privés, tels que les entreprises[108].

55. La CSE ne prévoit pas explicitement le droit à un recours effectif, mais la CSER a interprété la CSE comme exigeant un recours effectif dans certains cas[109].

ii. Risques pour le droit à un recours effectif

56. L'exercice du droit à un recours effectif peut être entravé dans le cas de violations présumées causées par des systèmes d'IA en raison de leur complexité technique, de leur opacité et de leur dépendance à l'égard de vastes ensembles de données et de divers acteurs en amont de la chaîne d'approvisionnement. Les individus peuvent ne pas avoir les connaissances ou l'accès aux informations nécessaires pour identifier les violations et la personne ou l'entité responsable. Ils peuvent ne pas être conscients de l'ampleur des atteintes à leurs droits ou avoir du mal à comprendre les processus décisionnels sous-jacents. Par conséquent, les recours doivent être accessibles - disponibles et compréhensibles pour les individus - et efficaces, c'est-à-dire qu'ils doivent permettre de traiter et de réparer de manière adéquate les dommages causés par les systèmes d'IA.

57. Les parties à la Convention-cadre sont tenues d'adopter ou de maintenir des mesures visant à garantir l'accès à des recours accessibles et efficaces en cas de violations des droits humains résultant d'activités menées dans le cadre du cycle de vie des systèmes d'IA[110]. Cela inclut la documentation et la mise à disposition des informations pertinentes aux personnes concernées, afin de leur permettre de comprendre et d'exercer leurs droits. Le contenu pertinent des mesures liées à l'information doit être adapté au contexte, suffisamment clair et significatif et, surtout, donner à la personne concernée la possibilité effective d'utiliser les informations en question

---

[103] *Paulino Tomás c. Portugal*, décision, 2003, No. 58698/00.
[104] Leander c. Suède, No. 9248/81, 26 mars 1987.
[105] *Klass et autres c. Allemagne*, No. 5029/71, 6 septembre 1978, § 67.
[106] *Khan c. Royaume-Uni*, No. 35394/97, 12 mai 2000, §§ 44-47.
[107] Voir par exemple *Big Brother Watch et autres c. Royaume-Uni* [GC], No. 58170/13, 62322/14 et 24960/15, 25 mai 2021, § 336 : « Dans un domaine où les abus dans des cas individuels sont potentiellement si faciles et pourraient avoir des conséquences aussi néfastes pour la société démocratique dans son ensemble, la Cour a estimé qu'il est en principe souhaitable de confier le contrôle de la surveillance à un juge, le contrôle judiciaire offrant les meilleures garanties d'indépendance, d'impartialité et de procédure régulière ». Voir également *Ramirez Sanchez c. France* [GC], No. 59450/00, 4 juillet 2006, §§ 165-166 ; *Danilczuk c. Chypre*, No. 21318/12, 3 avril 2018, §§ 44.
[108] *Z et autres c. Royaume-Uni* [GC], No. 29392/95, 10 mai 2001, § 109 ; *Keenan c. Royaume-Uni*, No. 27229/95, 3 avril 2001, § 129 ; *Paul et Audrey Edwards c. Royaume-Uni*, No. 46477/99, 14 juin 2002, § 97.
[109] Les employés qui revendiquent leur droit à un salaire égal doivent être légalement protégés contre toute forme de représailles. Lorsqu'un employé est victime de représailles, il doit exister un recours adéquat, qui à la fois indemnisera l'employé et servira de moyen de dissuasion à l'employeur, voir Conclusions XV-2 (2001), République slovaque ; La législation nationale devrait, au minimum, exiger une justification convaincante pour les systèmes éducatifs spéciaux ou ségrégés et conférer un recours effectif à ceux qui se sont vus illégalement exclus ou ségrégués ou à qui l'on a refusé un droit effectif à l'éducation ; en vertu de l'article 15§2, la législation anti-discrimination doit inclure l'adaptation des conditions de travail (aménagement raisonnable) et conférer un recours effectif à ceux qui se sont vus illégalement discriminés, voir Conclusions 2007, Déclaration interprétative de l'article 15§1 ; Conclusions XIX-1 (2008), République tchèque ; les États parties sont tenus de prouver l'absence de discrimination, directe ou indirecte, en droit et en pratique, et doivent informer de toute mesure pratique prise pour remédier aux cas de discrimination voir Conclusions III (1973), Déclaration interprétative de l'article 19§4 ; Fédération européenne des associations nationales travaillant avec les sans-abri (FEANSA) c. Pays-Bas, Requête No. 86/2012, décision sur le fond du 2 juillet 2014, §§ 202-203.
[110] Convention-cadre, article 9.

pour exercer ses droits dans le cadre de la procédure relative aux décisions pertinentes affectant ses droits humains[111].

3.2 Entreprises et droits humains

58. Cette section explore l'intersection entre les activités commerciales liées à l'IA et les obligations en matière de droits humains, en se concentrant sur les obligations positives des États en vertu de la CEDH et de la CSE[112], sur l'équilibre entre les droits humains des entreprises et ceux des individus, et sur la responsabilité des entreprises de respecter les droits humains dans le cadre plus large des normes internationales non contraignantes.

3.2.1 Obligations positives en vertu de la CEDH et de la CSE

59. La CEDH et la CSE n'imposent pas directement des obligations des entreprises en matière de droits humains. Si les particuliers ne peuvent pas porter plainte directement contre des entreprises devant la Cour ou le CEDS, ils peuvent intenter des actions contre les États qui n'ont pas empêché ou traité les abus résultant d'activités liées aux entreprises.

60. En vertu de la CEDH, les États peuvent être tenus pour responsables lorsqu'ils tolèrent ou ferment les yeux sur des actes d'acteurs privés qui violent les droits humains[113] ou lorsqu'ils ne réglementent pas correctement le secteur privé[114]. La portée et le contenu concrets des obligations des États en matière de prévention et de réparation des violations des droits humains liées aux entreprises dépendent dans une certaine mesure du droit humain en question et des circonstances factuelles. En général, les obligations positives consistent à prévenir les violations des droits humains lorsque les autorités compétentes ont eu connaissance ou auraient dû avoir connaissance d'un risque réel de telles violations ; à mener une enquête officielle indépendante et impartiale, adéquate et rapide lorsque de telles violations sont présumées avoir eu lieu ; à engager des poursuites efficaces et à prendre toutes les mesures appropriées pour mettre en place des mécanismes accessibles et efficaces exigeant que les victimes de telles violations reçoivent une réparation rapide et adéquate pour tout préjudice subi[115]. Cependant, tous les manquements à l'obligation de prévenir les abus liés aux activités commerciales ne constituent pas une violation des obligations de la CEDH. Il peut être nécessaire de démontrer que l'abus aurait certainement été évité si l'État avait pris les mesures que l'on pouvait raisonnablement attendre de lui dans la situation en question[116].

61. La CSE offre également une protection contre les violations des droits humains liées aux activités commerciales, en particulier en ce qui concerne les droits des travailleurs. Dans le cadre de leur politique, les États membres devraient prendre toutes les mesures nationales et internationales appropriées pour assurer la réalisation effective des droits et principes de la CSE et envisager d'accepter des dispositions supplémentaires[117].

---

[111] Rapport explicatif, § 99

[112] Les États peuvent manquer à leurs obligations négatives lorsque des violations des droits humains liées aux entreprises sont imputables à l'État. Cela peut se produire, par exemple, lorsqu'une entreprise est détenue ou contrôlée par l'État ou lorsqu'une entreprise agit en tant qu'agent de l'État. À l'heure actuelle, les activités pertinentes dans le cycle de vie des systèmes d'IA sont largement menées par des entreprises privées indépendantes. Par conséquent, le manuel se concentre sur les obligations positives, nonobstant la possibilité d'inclure une analyse des obligations négatives dans les éditions futures.

[113] *Ilaşcu et autres c. Moldova et Russie* [GC], no. 48787/99, 8 juillet 2004, § 318 *: «* si les autorités d'un Etat contractant approuvent, formellement ou tacitement, les actes des particuliers violant dans le chef d'autres particuliers soumis à sa juridiction les droits garantis par la Convention, la responsabilité dudit Etat peut se trouver engagée au regard de la Convention. »

[114] Hatton et autres c. Royaume-Uni [GC], No. 30622/1997, 8 juillet 2003, § 98

[115] Recommandation CM/Rec(2016)3 sur les droits de l'homme et les entreprises, paragraphe 15.

[116] *E. et autres c. Royaume-Uni*, No. 33218/96, 26 novembre 2002.

[117] Recommandation CM/Rec(2016)3 sur les droits de l'homme et les entreprises, paragraphe 16 ; voir également *Marangopoulos Foundation for Human Rights (MFHR) c. Grèce*, réclamation No. 30/2005, décision sur la recevabilité du 10

62. Des obligations positives au titre de la CEDH peuvent se présenter dans un large éventail de situations, telles que l'ingérence des entreprises de médias dans la liberté d'expression[118] ; les abus dans les hôpitaux[119] et les écoles privés[120] ; les restrictions vestimentaires sur le lieu de travail affectant le droit de manifester sa religion[121] ; la fourniture aux travailleurs d'informations permettant d'évaluer les risques pour la santé et la sécurité au travail[122] ; ou les atteintes aux droits humains liées à l'environnement causées par les activités des entreprises[123]. En vertu de la CSE, des obligations positives peuvent découler du droit à la santé en vertu de l'article 11[124], de la prévention du travail forcé et d'autres formes d'exploitation par le travail[125], ou de la prise de mesures préventives appropriées (campagnes d'information, de sensibilisation et de prévention sur le lieu de travail ou en relation avec le travail) afin de lutter contre le harcèlement moral[126].

63. La jurisprudence de la Cour, dans des circonstances spécifiques, met en évidence (i) les obligations positives de réglementer et de contrôler les opérations commerciales ; (ii) les obligations procédurales positives de permettre la participation du public et la prise de décisions en connaissance de cause ; et (iii) les obligations positives de fournir des recours efficaces en cas de violations des droits humains liées aux entreprises.

Obligations de réglementer et de surveiller les activités des entreprises

64. Les États ont l'obligation de réglementer et de surveiller les activités commerciales de manière à établir un juste équilibre entre les droits de l'individu et les intérêts de la communauté dans son ensemble. La Cour évalue si « on pouvait raisonnablement attendre de l'État qu'il ag[isse] de manière à prévenir la violation alléguée des droits du requérant »[127] ou si « les autorités nationales ont pris les mesures nécessaires pour assurer la protection effective des droits de l'intéressée »[128]. Dans les affaires environnementales, il est important de savoir si les autorités de l'État étaient au courant des problèmes et si elles exerçaient une surveillance suffisante sur l'activité commerciale en imposant des conditions d'exploitation et en supervisant leur mise en œuvre[129]. Dans le contexte de l'article 2 (droit à la vie), la Cour considère que les mesures « raisonnables » et « nécessaires » impliquent « le devoir primordial de mettre en place un cadre législatif et administratif visant une prévention efficace et dissuadant de mettre en péril le droit à la vie »[130].

65. La Cour a également tenu les États responsables de leur manquement à informer le public des risques liés à des activités dangereuses et à émettre des avertissements.[131] Dans le cadre des articles 8 (droit au respect de la vie privée et familiale) et 2 (droit à la vie), il existe une obligation de fournir au public des informations

---

octobre 2005, §14, le CEDS a décidé que l'État est responsable de l'application des droits inscrits dans la Charte dans sa juridiction, même si l'État n'a pas agi en tant qu'opérateur mais a simplement omis de mettre fin aux violations alléguées en sa qualité de régulateur. Dans l'Interprétation de l'article 17§2 – Participation du secteur privé à l'éducation, Conclusions 2019, les États parties sont tenus de réglementer et de superviser strictement la participation du secteur privé à l'éducation, en veillant à ce que le droit à l'éducation ne soit pas compromis.

[118] *Axel Springer AG c. Allemagne* [GC], No. 39954/08, 7 février 2012 et *Von Hannover c. Allemagne* [No. 2] [GC], No. 40660/08 et 60641/08, 7 février 2012.

[119] *Storck c. Allemagne*, No. 61603/00, 16 juin 2005.

[120] *Costello-Roberts c. Royaume-Uni*, No. 13134/87, 25 mars 1993.

[121] *Eweida et autres c. Royaume-Uni*, No. 48420/10 et 3 autres, 27 mai 2013.

[122] *Vilnes et autres c. Norvège*, No. 52806/09 et 22703/10, 24 mars 2014.

[123] *Lopez Ostra c. Espagne*, No. 16798/90, 9 décembre 1994 ; *Guerra et autres c. Italie* [GC], No. 116/1996/735/932, 19 February 1998, 19 février 1998, § 58 ; ***Taşkin et autres c. Turquie***, No. 46117/99, 30 mars 2005 ; *Fadeyeva c. Russie*, No. 55723/00, 9 juin 2005, § 89.

[124] CSER, Conclusions 2005 - Déclaration interprétative - Article 11

[125] CSER, Conclusions 2020, Albanie

[126] CSER, Conclusions 2014, Azerbaïdjan ; Conclusions 2005, République de Moldavie

[127] *Fadeyeva c. Russie*, No. 55723/00, 9 juin 2005, § 89.

[128] *López Ostra c. Espagne, § 55 ; Guerra et autres c. Italie, § 58.*

[129] Voir par exemple *López Ostra c. Espagne* ; *Dubetska et autres c. Ukraine*, No. 30499/03, 10 février 2011.

[130] *Öneryıldız c. Turquie* [GC], no 48939/99, § 89.

[131] Tătar c. Roumanie, requête No. 67021/01, 27 janvier 2009, §§ 113-116, 121-124.

essentielles sur les activités dangereuses liées à l'activité commerciale[132]. En outre, le « droit du public à l'information » ne doit pas se limiter aux risques qui se sont déjà matérialisés, mais doit figurer parmi les mesures préventives à prendre.[133]

66. Les États devraient examiner si les entreprises impliquées dans le cycle de vie de l'IA sont soumises à une surveillance adéquate. L'accent mis par la Cour sur la question de savoir si « l'on peut raisonnablement attendre de l'État qu'il agisse de manière à prévenir ou à mettre fin à la violation alléguée des droits du demandeur » pourrait s'appliquer aux manquements de l'État à traiter, par exemple, les « biais algorithmiques » ou les processus décisionnels opaques de l'IA.

Obligations procédurales positives pour permettre la participation du public et une prise de décision en connaissance de cause

67. Les décisions de l'État relatives aux activités commerciales - telles que l'octroi d'une licence - peuvent également avoir une incidence sur les droits humains. Les processus décisionnels « concernant des questions d'impact culturel, environnemental et économique [...] doivent nécessairement faire l'objet d'enquêtes et d'études appropriées afin de permettre [aux autorités publiques] de trouver un juste équilibre entre les différents intérêts contradictoires en jeu » [en anglais uniquement ; traduction libre][134]. Afin de respecter les intérêts protégés par l'article 8 de la CEDH, par exemple, le processus décisionnel conduisant à des mesures d'ingérence doit « prendre en considération tous les aspects procéduraux, y compris le type de politique ou de décision en cause, la mesure dans laquelle les opinions des individus ont été prises en compte tout au long du processus décisionnel et les garanties procédurales disponibles. »[135] Dans les affaires environnementales, cela nécessite des enquêtes et des études « de manière à prévenir et évaluer à l'avance les effets des activités qui peuvent porter atteinte à l'environnement et aux droits des individus ».[136] La réglementation nationale « par ailleurs prévoir des procédures adéquates tenant compte des aspects techniques de l'activité en question et permettant de déterminer ses défaillances ainsi que les fautes qui pourraient être commises à cet égard par les responsables à différents échelons »[137].

68. Dans la Convention-cadre, les principes de transparence et de contrôle[138] exigent « l'ouverture et la clarté dans la gouvernance des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle et signifie spécifiquement que les processus décisionnels et le fonctionnement général des modèles d'intelligence artificielle devraient être compréhensibles et accessibles aux acteurs appropriés de l'intelligence artificielle et, le cas échéant, aux parties prenantes concernées. »[139]

69. Afin de garantir le plein exercice des droits humains et des libertés démocratiques, la CM/Rec(2020)1 recommande aux États de sensibiliser le grand public aux capacités, aux pouvoirs et aux conséquences des systèmes algorithmiques, y compris leur utilisation potentielle pour manipuler, exploiter, tromper ou distribuer des ressources, en vue de permettre à tous les individus et groupes de connaître leurs droits et de savoir comment les mettre en pratique, ainsi que d'utiliser les technologies numériques à leur avantage. En outre, tous les acteurs concernés, y compris ceux des secteurs public, privé et de la société civile dans lesquels des systèmes algorithmiques sont envisagés ou utilisés, devraient promouvoir, encourager et soutenir de manière adaptée et inclusive (en tenant compte de la diversité en ce qui concerne, par exemple, l'âge, le sexe, la race, l'origine ethnique, le contexte culturel ou socio-économique) un niveau de maîtrise des médias, du numérique et de

[132] Vilnes et autres c. Norvège, nos 52806/09 et 22703/10, 24 mars 2014, § 235 ; *Roche c. Royaume-Uni* [GC], No. 32555/96, 19 octobre 2005 §162.
[133] *Vilnes et autres c. Norvège*, No. 52806/09 et 22703/10, 24 mars 2014, § 235.
[134] Zammit Maempel c. Malte, requête No. 24202/10, 22 novembre 2011, § 62.
[135] *Taskin et autres c. Turquie, § 118.*
[136] Idem.
[137] *Öneryıldız c. Turquie* [GC], § 90.
[138] Voir l'article 8 de la Convention-cadre.
[139] Rapport explicatif, paragraphe 57.

l'information qui permette une prise en compte et une utilisation compétentes et critiques des systèmes algorithmiques.[140]

Obligations relatives à la mise en place de voies de recours effectives

70. Les États devraient également prévoir des recours efficaces pour les violations des droits humains liées aux entreprises. Cela peut inclure la modification des lois si le cadre juridique est inadéquat[141] et la garantie que les entreprises respectent le droit national. Le droit à un recours effectif (article 13 de la CEDH) est pertinent à cet égard.

Marge d'appréciation dans le cadre des obligations positives

71. Il est important de noter que les États jouissent généralement d'une large marge d'appréciation pour décider de la manière de remplir leurs obligations en ce qui concerne les activités commerciales susceptibles d'avoir un impact sur les droits humains. Cette marge d'appréciation interprétée par la Cour se réduit toutefois si les mesures prises par l'État interfèrent avec un « aspect des plus intimes de la vie privée d'une personne »[142], ainsi qu'en cas de menaces graves pour les droits humains[143]. De plus, « il incombe à l'État de justifier, à l'aide de données détaillées et rigoureuses, une situation dans laquelle des individus supportent un lourd fardeau au nom du reste de la communauté »[144].

72. Ainsi, si les États disposent d'une marge d'appréciation pour réglementer les technologies d'IA dans le cadre des activités commerciales, leur pouvoir discrétionnaire pourrait être considérablement limité lorsque les systèmes d'IA constituent une menace sérieuse pour les droits humains.

3.2.2 Équilibrer les droits des entreprises dans le contexte de la gouvernance de l'IA

73. Les exigences de transparence et d'explicabilité concernant, par exemple, l'atténuation des préjugés soulèvent des questions relatives à l'intersection des droits des individus et des lois sur la propriété intellectuelle et les secrets d'affaires. Le système d'IA d'une entreprise peut être couvert par la législation sur la propriété intellectuelle et les secrets commerciaux. De plus, les entreprises ont également droit à la protection des droits humains spécifiques en vertu de la CEDH, tels que les droits de propriété (Article 1 du protocole 1 CEDH qui inclut la propriété intellectuelle)[145] ou la liberté d'expression (article 10 de la CEDH).[146] Dépendant des circonstances, ces droits doivent être mis en balance avec les droits des personnes concernées et peuvent l'emporter sur ces derniers.

74. Si les détenteurs de droits affirment que les systèmes d'IA violent leurs droits, la réponse de l'État devra peut-être trouver un équilibre entre ces intérêts concurrents. Par exemple, l'obligation de fournir des informations essentielles au public peut entrer en conflit avec les droits de propriété intellectuelle d'une entreprise (protégés par le droit de propriété - article 1 du protocole 1 de la CEDH). Les tribunaux nationaux ou les régulateurs nationaux doivent soigneusement peser ces intérêts afin de garantir un résultat juste et proportionnel.

75. Les rédacteurs de la Convention-cadre ont noté, en ce qui concerne le principe de transparence (article 8 de la Convention-cadre), que « mise en oeuvre de ce principe, de trouver un juste équilibre entre les divers

---

[140] Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme, section B, paragraphe 1.3.
[141] *Fadeyeva c. Russie*, §§89 et 92 ; voir aussi *Powell et Rayner c. Royaume-Uni*, No. 93101/81, 21 février 1990.
[142] *Hatton & autres c. Royaume-Uni* [GC], 7 août 2003, § 102.
[143] *Brincat et autres c. Malte*, requête No. 60908/11 et al., 24 juillet 2014, § 116.
[144] Dubetska et autres c. Ukraine, requête No. 30499/03, 10 février 2011, § 145.
[145] *Anheuser-Busch Inc. c. Portugal* [GC], no 73049/01, 11 janvier 2007, § 72.
[146] *Axel Springer AG c. Allemagne* [GC], no. 39954/08, arrêt du 7 février 2012.

intérêts concurrents et de procéder aux ajustements nécessaires dans les cadres pertinents sans altérer ou modifier fondamentalement le régime sous-jacent des droits de l'homme applicables ».[147]

76. Dans le contexte des systèmes algorithmiques, la recommandation CM/Rec(2020)1 du Conseil de l'Europe sur les impacts des systèmes algorithmiques sur les droits de l'homme prévoit que les cadres législatifs relatifs à la propriété intellectuelle ou aux secrets commerciaux ne doivent pas empêcher la transparence ou être exploités pour faire obstacle à la responsabilité, et que la confidentialité ou les secrets commerciaux ne doivent pas entraver la réalisation d'évaluations efficaces de l'impact sur les droits humains[148]. De plus, les États devraient établir des niveaux de transparence appropriés en ce qui concerne les critères et méthodes de passation de marchés publics, d'utilisation, de conception et de traitement de base des systèmes algorithmiques mis en œuvre par et pour eux, ou par des acteurs du secteur privé[149].

3.2.3 Principaux cadres non contraignants sur les entreprises, les droits humains et l'IA

Instruments non contraignants pertinents

77. Les **principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme (UNGP)** font partie des cadres de gouvernance mondiaux et régionaux pertinents. Ces principes directeurs prévoient une série de principes que les États et les entreprises devraient appliquer ou envisager d'appliquer (selon les circonstances), en utilisant le cadre « Protéger, respecter et réparer » : (i) le devoir de l'État de protéger contre les abus, (ii) la responsabilité des entreprises de respecter les droits de l'homme et (iii) l'accès à des voies de recours pour les victimes.

78. S'appuyant sur les principes directeurs des Nations unies, le Comité des ministres du Conseil de l'Europe a adopté la **recommandation CM/Rec(2016)3 sur les droits de l'homme et les entreprises**. Elle fournit des orientations spécifiques pour aider les États membres à prévenir les violations des droits humains par les entreprises et à y remédier, et insiste sur les mesures visant à inciter les entreprises à respecter les droits humains.

79. Les **principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises**, qui fournissent des recommandations détaillées sur la conduite responsable des entreprises adressées par les gouvernements aux entreprises multinationales, constituent un autre instrument pertinent.

80. Pour les États membres du Conseil de l'Europe, l'obligation de protéger contre les violations des droits humains liées aux entreprises et de fournir des recours efficaces est illustrée au mieux par la jurisprudence de la Cour et la pratique du CEDS, comme indiqué ci-dessus. La section suivante se concentrera donc sur les responsabilités des entreprises en matière de respect des droits humains dans le contexte de l'IA à travers le cadre des UNGP.

Responsabilité des entreprises en matière de respect des droits humains

81. Les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme préconisent que les entreprises mettent en place des politiques et des processus, notamment (i) des engagements politiques pour assumer leur responsabilité en matière de respect des droits humains ; (ii) une diligence raisonnable en

[147] Convention-cadre, Rapport explicatif, § 62.
[148] CM/Rec(2020)1, § 5.2.
[149] Id., § 4.1 Les niveaux de transparence en question devraient être aussi élevés que possible et proportionnels à la gravité des incidences négatives sur les droits de l'homme. L'utilisation de tels systèmes dans les processus décisionnels qui comportent un risque élevé pour les droits de l'homme devrait être soumise à des normes particulièrement élevées.

matière de droits humains pour identifier, prévenir et traiter les impacts négatifs sur les droits humains ; (iii) des processus permettant de remédier à leurs impacts négatifs sur les droits humains[150]. Les entreprises doivent utiliser des indicateurs qualitatifs et quantitatifs, intégrer ce suivi dans les processus internes et solliciter le retour d'information des parties prenantes (principe 20). Lorsque les entreprises causent ou contribuent à des impacts négatifs, elles doivent mettre en place des mesures correctives ou coopérer à leur mise en œuvre par le biais de processus légitimes (principe 22). Si les impacts sont liés aux activités de l'entreprise mais ne sont pas directement causés par elle, l'entreprise n'est pas tenue d'y remédier elle-même mais peut jouer un rôle de soutien dans le cadre d'efforts plus larges. Lorsqu'il est nécessaire d'établir un ordre de priorité, les entreprises doivent se concentrer en premier lieu sur les impacts les plus graves ou irrémédiables afin de minimiser les dommages (principe 24). La communication sur ces mesures doit être transparente et accessible, en conciliant les préoccupations légitimes de confidentialité et la nécessité de rendre des comptes (principe 21).

82. À ce jour, aucune orientation spécifique à l'IA sur la responsabilité des entreprises en matière de droits humains n'a été élaborée[151]. Les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme peuvent toutefois fournir un cadre permettant d'aborder les incidences sur les droits humains tout au long de la chaîne de valeur de l'IA. Les entreprises doivent évaluer et atténuer les risques en matière de droits humains tout au long du cycle de vie de l'IA, de la conception au déploiement, en plaçant la transparence et la responsabilité au cœur de leurs principes. La diligence raisonnable en matière de droits humains devrait évaluer les impacts directs et indirects, en se concentrant sur les risques pour les individus, et devrait être adaptée de manière dynamique à la nature évolutive des technologies de l'IA. Il conviendrait sans doute d'élaborer et d'appliquer des évaluations d'impact sur les droits humains spécifiques à l'IA afin d'identifier les risques en matière de droits humains, y compris ceux découlant de l'utilisation de systèmes d'IA par des tiers.

83. Dans le contexte spécifique de l'IA, la méthodologie HUDERIA[152], bien qu'elle ne soit pas un instrument spécifique sur la responsabilité des entreprises en matière de respect des droits humains, s'adresse aux acteurs publics et privés. Elle relie les normes internationales en matière de droits humains et les cadres techniques existants sur la gestion des risques dans le contexte de l'IA et fournit une approche structurée de l'évaluation des risques et des impacts des systèmes d'IA spécifiquement adaptée à la protection et à la promotion des droits de l'homme, de la démocratie et de l'État de droit.

84. Enfin, conformément à la Recommandation CM/Rec(2016)3 sur les droits de l'homme et les entreprises, les États devraient appliquer les mesures nécessaires pour encourager ou, le cas échéant, exiger que les entreprises domiciliées sur leur territoire ayant des activités dans le cycle de vie de l'IA appliquent une diligence raisonnable en matière de droits humains tout au long de leurs opérations et effectuent une diligence raisonnable en matière de droits humains en ce qui concerne ces activités, y compris des évaluations de l'impact sur les droits humains spécifiques au projet, en fonction de la taille de l'entreprise et de la nature et du contexte de l'opération[153]. Les États devraient encourager et, le cas échéant, exiger de ces entreprises qu'elles fassent preuve d'une plus

---

[150] Principes directeurs des Nations unies, principes 15-24.

[151] L'OCDE élabore actuellement des lignes directrices sur la diligence raisonnable en matière de conduite responsable des entreprises dans le développement et l'utilisation de systèmes d'IA fiables. En outre, le projet B-Tech des Nations unies sur les droits humains a identifié trois grands thèmes et formulé des recommandations pratiques sur la manière dont les législateurs, les organismes de normalisation, les entreprises et la société civile peuvent tirer parti des Principes directeurs des Nations unies pour promouvoir une gouvernance et des pratiques commerciales capables de faire face aux impacts et aux risques de l'IA générative sur les droits humains (voir Advancing Responsible Development and Deployment of Generative AI: A UN B-Tech foundational paper | OHCHR).

[152] La méthodologie HUDERIA (« Méthodologie d'évaluation des risques et des impacts des systèmes d'intelligence artificielle du point de vue des droits de l'homme, de la démocratie et de l'État de droit ») est un outil structuré conçu pour servir de guide dans l'évaluation et l'atténuation des risques que les systèmes d'IA font peser sur les droits de l'homme, la démocratie et l'État de droit. Il complète, sans être juridiquement contraignant, la Convention-cadre. Il doit être complété par le modèle HUDERIA, qui comprend des supports tels que des outils et des recommandations évolutives destinés à servir de ressources pour les activités de gestion des risques.

[153] CM/Rec(2016)3, para 20.

grande transparence afin de leur permettre de mieux « connaître et montrer » leur responsabilité d'entreprise en matière de respect des droits humains et, le cas échéant, exiger de ces entreprises qu'elles fournissent régulièrement, ou en tant que de besoin, des informations sur leurs efforts en matière de responsabilité d'entreprise en matière de respect des droits de humains dans le contexte de l'IA[154].

3.3 Analyse sectorielle de la gouvernance publique

85. Ce chapitre examine l'impact des systèmes d'IA dans des domaines clés de la gouvernance publique, en se concentrant sur leurs implications pour les droits humains. S'appuyant sur la CEDH et la CSE, ainsi que sur d'autres instruments internationaux le cas échéant, il explore les secteurs où l'intégration des systèmes d'IA peut porter gravement atteinte aux droits humains et où une telle intégration est avancée ou raisonnablement envisageable.

3.3.1 Administration de la justice

86. L'administration de la justice englobe les systèmes, les processus et les institutions chargés de faire respecter la loi, de résoudre les litiges et de garantir l'équité et la justice. Elle comprend les tribunaux, les juges, les procureurs et les avocats, ainsi que les organismes chargés de l'application de la loi.

Principaux cas d'utilisation de l'IA

87. 125 systèmes intégrés d'IA ont été jusqu'ici documentés comme étant utilisés ou pilotés au sein de systèmes judiciaires à travers l'Europe et dans d'autres pays participant au Réseau européen de cyberjustice du Conseil de l'Europe[155]. Si les systèmes d'IA conçus pour des tâches administratives auxiliaires présentent un risque minime[156], ceux qui aident directement les autorités judiciaires à rechercher, interpréter les faits et appliquer la loi à des cas spécifiques présentent des risques importants pour le droit à un procès équitable et les droits humains connexes. L'administration de la justice a été l'un des premiers secteurs de la gouvernance publique dans lesquels le Conseil de l'Europe a abordé les implications de l'utilisation des systèmes d'IA sur les droits en publiant sa « Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement » (la « Charte éthique »)[157].

88. Les principaux cas d'utilisation de l'IA dans ce contexte sont les suivants :

- *Recherche, examen, analyse et découverte à grande échelle facilités par l'IA* : Systèmes d'IA qui créent une collection consultable de descriptions de jurisprudence, de textes juridiques et d'autres informations à partager avec des experts juridiques pour une analyse plus approfondie et une découverte à grande échelle sur des volumes importants de documents électroniques. Il s'agit par exemple de moteurs de recherche avec des interfaces appliquées à la jurisprudence et aux dossiers judiciaires.
- *Aide à la décision* : Systèmes qui facilitent ou automatisent les étapes du processus décisionnel. Il s'agit par exemple de résumer des textes, d'extraire des informations spécifiques dans une application, de

[154] Idem, para 20.

[155] Le Centre de ressources sur la cyberjustice et l'IA sert de point de contact accessible au public pour obtenir des informations fiables sur les systèmes d'IA et autres outils de cyberjustice, dans le but de fournir un point de départ pour un examen plus approfondi de leurs risques et avantages pour les professionnels et les utilisateurs finaux. Il est supervisé par le Comité d'experts sur l'intelligence artificielle de la CEPEJ (https://www.coe.int/en/web/cepej/ai-advisory-board).

[156] Comme l'anonymisation ou la pseudonymisation de décisions judiciaires, de documents ou de données, la communication entre le personnel et l'automatisation d'autres tâches administratives.

[157] La Charte éthique, adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ) du Conseil de l'Europe, est l'un des premiers documents réglementaires sur l'IA qui fournit un ensemble de principes à mettre en œuvre par les acteurs publics et privés responsables de la conception et du développement d'outils et de services d'IA dans l'administration de la justice.

fournir des lignes directrices et des points de repère et de calculer des barèmes pour les condamnations et les indemnisations. Jusqu'à présent, aucun processus décisionnel entièrement automatisé sans supervision humaine n'a été signalé en Europe.

- *Prédiction des résultats judiciaires* : Systèmes qui apprennent à partir de grands ensembles de données afin d'identifier des modèles dans les données qui sont ensuite utilisés pour visualiser, simuler ou prédire de nouvelles issues de litiges.
- *Règlement en ligne des litiges ('Online dispute resolution' ou 'ODR'*) : Il s'agit des technologies utilisées pour la résolution des litiges entre les parties avec une intervention humaine limitée. Il s'agit principalement de modes alternatifs de résolution des conflits, mais aussi de la résolution des conflits dans le cadre des tribunaux.
- *La nomination des juges et l'attribution des affaires basées sur l'IA* : Systèmes utilisés pour accomplir ou faciliter des tâches telles que l'attribution des affaires aux tribunaux et aux juges et l'établissement de niveaux de priorité.

89. D'autres applications, telles que l'utilisation de l'IA pour l'interprétation pendant les audiences ou l'enregistrement, la transcription ou la traduction, pourraient également mettre en cause des éléments du droit à un procès équitable en fonction des circonstances.

Droits humains et principes pertinents

90. Les principes identifiés dans la Convention-cadre[158] et la non-contraignante Charte éthique européenne d'utilisation de l'intelligence artificielle correspondent à des préoccupations importantes et réelles concernant l'utilisation de l'IA dans l'administration de la justice et ses éventuelles répercussions négatives sur les droits humains protégés par la CEDH et la convention 108(+). Les principes de la Charte éthique européenne sur l'utilisation de l'intelligence artificielle comprennent le respect des droits fondamentaux, la non-discrimination, la qualité et la sécurité de l'IA, la transparence, l'impartialité et l'équité, ainsi que le principe du « contrôle par l'utilisateur »[159].

91. Le droit humain le plus touché dans ce secteur est le droit à un procès équitable, garanti par l'article 6 de la CEDH[160].

Le droit à un procès équitable

92. Le principe clé régissant l'article 6 est l'équité[161]. Comme l'a souligné la Cour, ce qui constitue un procès équitable ne peut faire l'objet d'une règle unique et constante, mais doit dépendre des circonstances de chaque affaire et à la lumière de l'équité globale de la procédure[162]. Certains principes subsidiaires d'équité sont particulièrement pertinents dans le contexte de l'AI :

(i) Indépendance et impartialité

[158] Convention-cadre (articles 4 à 13).
[159] En évitant une approche prescriptive et en veillant à ce que les utilisateurs soient des acteurs informés et maîtres de leurs choix.
[160] Ainsi que d'autres instruments internationaux relatifs aux droits de l'homme (articles 10 et 11 de la Déclaration universelle des droits de l'homme, article 14 du Pacte international relatif aux droits civils et politiques, article 47 de la Charte des droits fondamentaux de l'Union européenne, article 8 de la Convention américaine relative aux droits de l'homme - Pacte de San José, article 7 de la Charte africaine des droits de l'homme et des peuples) et dans l'ordre juridique constitutionnel des pays démocratiques.
[161] *Vacher c. France*, No. 20368/92, 17 décembre 1996.
[162] *Ibrahim et autres c. Royaume-Uni [GC],* Nos. 50541/08, 50571/08, 50573/08, 40351/09, 13 septembre 2016, § 250.

93. L'article 6 garantit, pour la détermination des droits et obligations de caractère civil ou de toute accusation en matière pénale, le droit d'être entendu par un tribunal indépendant et impartial établi par la loi[163]. Le tribunal doit être indépendant à la fois des autres branches du gouvernement, telles que l'exécutif et le législatif, et des parties impliquées dans l'affaire[164]. Le tribunal doit également être impartial, c'est-à-dire subjectivement libre de tout préjugé ou parti pris personnel, et doit offrir des garanties suffisantes pour exclure tout doute légitime à cet égard[165].

94. La partialité des systèmes d'IA peut ne pas être facilement discernable par le juge en raison de la perception généralisée de la « neutralité » algorithmique/mathématique et de la partialité technologique des juges eux-mêmes. Cela pourrait conduire à des résultats discriminatoires. Le recours intensif à l'IA pourrait conduire à une « standardisation » des décisions judiciaires, les juges se sentant obligés de suivre les recommandations de l'IA en raison de la « supériorité » perçue, en particulier dans les systèmes où leur mandat n'est pas permanent mais soumis à un vote populaire, ou dans lesquels leur responsabilité personnelle (disciplinaire, civile ou même pénale) est susceptible d'être engagée[166].

(ii) Présomption d'innocence

95. Le principe de la présomption d'innocence dans les procédures pénales exige, entre autres, que : (i) les juges (et les jurés le cas échéant) doivent aborder leurs fonctions sans aucune idée préconçue de la culpabilité de l'accusé ; (ii) la charge de la preuve incombe à l'accusation, et (iii) tout doute doit profiter à l'accusé[167].

96. En raison du biais algorithmique, l'inclusion potentielle dans les systèmes d'IA de variables telles que les antécédents criminels et familiaux signifie que le sort d'une personne peut être affecté par le comportement passé d'un certain groupe sans qu'une attention appropriée soit accordée aux antécédents spécifiques de la personne accusée, à ses motivations et, en fin de compte, à sa culpabilité. Cela pourrait avoir pour conséquence d'interférer avec le droit d'une personne à être présumée innocente jusqu'à ce que sa culpabilité soit prouvée par un tribunal. Si l'utilisation d'outils prédictifs par les juges dans les procès pénaux est très rare en Europe[168], il existe dans d'autres juridictions des exemples concrets d'effets négatifs[169].

(iii) L'égalité des armes et procédure contradictoire

97. L'égalité des armes est une caractéristique inhérente à un procès équitable. Elle exige que chaque partie ait une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation désavantageuse par rapport à son adversaire et s'applique aux procédures pénales et civiles[170]. Dans un contexte pénal, le droit à une procédure contradictoire signifie que l'accusé a la possibilité de prendre connaissance et de commenter toutes les preuves produites ou observations déposées en vue d'influencer la décision du tribunal, leur existence, leur contenu et leur authenticité sous une forme et dans un délai approprié[171]. Le fait de ne pas divulguer à la défense des éléments de preuve matériels qui pourraient permettre à l'accusé de se disculper ou de voir sa peine réduite constituerait un refus des facilités nécessaires à la préparation de la défense, et donc

[163] Voir *Deweer c. Belgique*, no 6903/75, 27 février 1980, § 49, Série A No. 35 ; *Kart c. Turquie* [GC], No. 8917/200, 3 décembre 2009, No. 8917/2005, § 67.
[164] *Beaumartin c. France*, No. 15287/89, 24 novembre 1994, § 38 ; Sramek c. Autriche, No. 8790/79, 22 octobre 1984, § 42.
[165] *Findlay c. Royaume-Uni*, No. 22107/93, 25 février 1997, § 73 ; *Micallef c. Malte* [GC], No. 17056/06, 2009 § 93.
[166] *Charte éthique*, § 140.
[167] *Barberà, Messegué et Jabardo c. Espagne*, 6 décembre 1988, requête No. 10590/83, § 77
[168] Charte éthique, paragraphe 124.
[169] Idem, paragraphes 128-131.
[170] *Öcalan c. Turquie* [GC], No. 46221/99, 12 mai 2005, § 140 ; *Foucher c. France*, No. 22209/93, 18 mars 1997, § 34 ; *Bulut c. Autriche*, No. 17358/90, 22 février 1996 ; *Faig Mammadov c. Azerbaïdjan*, No. 60802/09, 26 janvier 2017, § 19.
[171] *Rowe et Davis c. Royaume-Uni* [GC], No.28901/95, 16 février 2000, § 60 ; *Kress c. France* [GC], No. 39594/98, 7 juin 2001, § 74 ; *Krčmář et autres c. République tchèque*, No. 35376/97, 3 mars 2000, § 42.

une violation de l'article 6[172]. Le droit à une procédure contradictoire ne peut être méconnu pour gagner du temps et accélérer la procédure[173].

98. Des problèmes peuvent se poser si une partie se voit refuser un accès suffisant pour examiner les données analysées par l'IA et utilisées comme éléments de preuve[174]. Le droit à une procédure contradictoire exige vraisemblablement l'accès à un système d'IA, sa compréhension et la possibilité de contester sa validité scientifique, ses préjugés et ses erreurs potentielles. Toutefois, les droits de propriété intellectuelle et les lois sur les secrets commerciaux peuvent restreindre cet accès. Même sans ces obstacles, la complexité des modèles utilisés (« le problème de la boîte noire » peut constituer un défi majeur pour le défendeur. En outre, si les systèmes d'IA peuvent accélérer les procédures en permettant de gagner du temps, le droit à une procédure contradictoire ne peut être négligé à cette fin.

99. Dans les procédures civiles, l'égalité des armes pourrait être remise en cause par un éventuel déséquilibre entre les parties au litige dans leur compréhension et leur capacité à utiliser les outils d'IA, en fonction de leurs moyens disponibles, y compris financiers, ou même de leur niveau de culture numérique. Dans ce contexte, la Recommandation CM/Rec(2016)3 du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises souligne que lorsque des victimes présumées de violations des droits humains liées aux entreprises intentent des actions civiles contre des entreprises pour de telles violations, les États membres devraient veiller à ce que leurs systèmes juridiques garantissent suffisamment l'égalité des armes au sens de l'article 6 de la CEDH. En particulier, ils devraient prévoir dans leurs systèmes juridiques des régimes d'aide juridique pour les plaintes concernant de telles violations. Cette aide juridique devrait pouvoir être obtenue de manière pratique et efficace.[175]

(iv) Accès aux tribunaux

100. Le droit d'accès à un tribunal est un aspect inhérent aux garanties consacrées par l'article 6, et n'est pas plus absolu en matière pénale qu'en matière civile. Toute personne a le droit de porter devant une cour ou un tribunal toute réclamation relative à ses « droits et obligations de caractère civil »[176]. Un individu doit « avoir une possibilité claire et pratique de contester un acte qui constitue une ingérence dans ses droits »[177]. La nature pratique et effective de ce droit peut être altérée, par exemple, par une interprétation excessivement formaliste des règles de procédure.

101. Dans ce contexte, le recours à des systèmes d'IA ne devrait pas entraver le droit d'accès à un tribunal au sens de l'article 6[178] ni remettre en cause le contrôle humain sur la prise de décision[179]. L'accès au tribunal ne

---

[172] *Natunen c. Finlande,* No. *21022/04,* 31 mars 2009, No. 21022/04, §43.
[173] *Nideröst-Huber c. Suisse*, No. 18990/91, 18 février 1997, § 30.
[174] Voir *Sigurður Einarsson et autres c. Islande,* No. 39757/15, 4 septembre 2019. Dans cette affaire, les requérants se plaignaient de ne pas avoir accès à l'ensemble des données traitées par un système d'e-Discovery utilisé par l'accusation. La Cour a reconnu que le refus d'accès concernant au moins l'un des ensembles de preuves soulevait une question au regard de l'article 6 § 3 b) (§91), mais a conclu à la non-violation en raison du fait que l'accusation n'avait pas non plus connaissance du contenu de la collection complète de données et que les requérants n'avaient à aucun moment formellement demandé une ordonnance judiciaire pour accéder à la collection complète de données (§§89-93). Voir également l'opinion partiellement dissidente du juge Pavli, qui se concentre sur les questions relatives à l'utilisation des systèmes d'intelligence artificielle.
[175] CM/Rec(2016)3, para 41.
[176] *Golder c. Royaume-Uni*, No. 4451/70, 21 février 1975, § 36.
[177] *Bellet c. France*, No. 23805/94, 4 décembre 1995, § 38.
[178] Voir la Résolution 2081 (2015) de l'Assemblée parlementaire du Conseil de l'Europe (APCE), "Accès à la justice et Internet : potentiel et défis", dans laquelle l'APCE a appelé à garantir que *"les parties qui s'engagent dans des procédures ODR conservent le droit d'accéder à une procédure d'appel judiciaire satisfaisant aux exigences d'un procès équitable conformément à l'article 6 de la Convention*". Voir aussi *les Lignes directrices de* la CEPEJ *sur les modes alternatifs de résolution des conflits en ligne* (2023), https://rm.coe.int/cepej-2023-19final-en-guidelines-online-alternative-dispute-resolution/1680adce33
[179] Le droit à la surveillance humaine est également énoncé à l'article 9, paragraphe 1, point a), de la convention 108+.

devrait pas non plus être entravé par des obstacles techniques liés à un système d'IA spécifique. À cet égard, la Cour a estimé qu'en ne tenant pas compte des obstacles pratiques liés à l'utilisation obligatoire d'un système de dépôt électronique et en n'autorisant pas le dépôt alternatif (sur papier), une juridiction nationale avait adopté une approche formaliste qui était excessive et conduisait à une violation de l'article 6§1[180].

102. Les préoccupations relatives au droit à la liberté et à la sécurité (articles 5) sont liées au droit à un procès équitable.

Droit à la liberté et à la sûreté (article 5 de la CEDH)

103. Le principal objectif de l'article 5 est d'empêcher les privations de liberté illégales, arbitraires ou injustifiées[181]. Pour satisfaire à l'exigence de légalité, la détention doit être « conforme à une procédure prévue par la loi » et fondée sur une décision de justice ou une décision de condamnation. Les défauts d'un ordre de détention ne rendent pas automatiquement la détention illégale, mais des questions telles que l'insuffisance de la motivation sont prises en compte au titre de l'article 5, paragraphe 1[182]. La privation de liberté est également illégale si la condamnation résulte d'une procédure qui équivaut à un « déni de justice flagrant »[183] en étant « manifestement contraire aux dispositions de l'article 6 ou aux principes qui y sont consacrés »[184]. Un procès sommaire, qui ne permet pas une évaluation approfondie et objective de l'affaire, pourrait donc constituer une violation non seulement du droit à un procès équitable (article 6), mais aussi de l'article 5. [185]

104. Le manque de transparence ou de responsabilité des systèmes d'IA potentiels pourrait compromettre l'équité des décisions en matière de privation de liberté. Ils risquent de perpétuer les préjugés, ce qui pourrait conduire à des détentions provisoires injustes, à des condamnations disproportionnées ou à des refus injustes de libération conditionnelle. En outre, leur opacité compromet la capacité des individus à contester efficacement les décisions, ce qui soulève des questions quant à l'équité et à la responsabilité.

Vie privée et protection des données dans le cadre de l'administration de la justice

105. Les tribunaux et les autorités impliquées dans l'administration de la justice traitent et conservent des données à caractère personnel, y compris des données sensibles dont l'utilisation abusive pourrait entraîner des violations des données et de la vie privée ainsi que des discriminations[186]. L'article 8 est violé lorsque des données sensibles sont conservées sans garanties adéquates, telles que des délais ou une possibilité réelle de contrôle par la personne concernée[187]. Un juste équilibre doit être maintenu entre la nécessité de rendre publiques les décisions judiciaires et le respect des droits fondamentaux des parties ou des témoins[188].

---

[180] Voir *Xavier Lucas c. France*, 9 juin 2022, No. 15567/20, § 57, où la Cour a conclu à la violation de l'article 6 § 1 du fait que la Cour de cassation française n'avait pas pris en considération les obstacles pratiques, y compris les défauts techniques et matériels, d'une plateforme e-barreau qui avait empêché le requérant de soumettre par voie électronique une demande d'ouverture d'une procédure. Voir également ***Farcaş et autres c. Roumanie***, No. 30502/05, 5 juin 2018, où la Cour a estimé que le droit d'accès à la justice des requérants était devenu illusoire du fait que les documents judiciaires avaient été signifiés uniquement par publication (sur papier et en ligne) dans le Bulletin des procédures d'insolvabilité, alors que les requérants n'avaient ni les ressources financières pour consulter la version papier ni l'accès à Internet pour consulter la version électronique.

[181] ***Selahattin Demirtaş c. Turquie*** (nº 2) [GC], No. 14305/17, 22 décembre 2020, § 311.

[182] *S., V. et A. c. Danemark* [GC], No. 35553/12, 36678/12 et 36711/12, 22 octobre 2018, § 92.

[183] *Othman (Abu Qatada) c. Royaume-Uni*, No. 8139/09, 17 janvier 2012, § 260.

[184] *Willcox et Hurford c. Royaume-Uni (déc.),* Nos. 43759/10 et 43771/12, 8 janvier 2013, § 95 *; Othman (Abu Qatada) c. Royaume-Uni,* No. 8139/2009, 17 janvier 2012, § 259 *; Stoichkov c. Bulgarie,* No. 9808/02, 24 mars 2005, §§ 51, 56-58.

[185] Vorontsov et autres c. Ukraine, No. 58925/14 et 4 autres, 21 janvier 2021, §§ 42-49.

[186] Convention 108(+), article 6.

[187] *S. et Marper c. Royaume-Uni [GC], nos 30562 et 30566/2004, 4 décembre 2008, §103 ; M.M. c. Royaume-Uni, no 24029/2007, 13 novembre 2012, no 24029/2007, §195*

[188] Sauf dans les cas où la nécessité de protéger la confidentialité de certains types de données à caractère personnel est contrebalancée par l'intérêt de la recherche et de la poursuite d'infractions et de la publicité des procédures judiciaires. *Avilkina et autres c. Russie*, 2013, § 45 ; *Z c. Finlande*, 1997, § 97.

106. Les outils d'anonymisation ou de pseudonymisation intégrant la technologie de l'IA, tels que ceux déjà en place dans plusieurs États membres du Conseil de l'Europe, peuvent s'avérer utiles pour dissimuler systématiquement toute information permettant d'identifier les individus. Toutefois, Les préoccupations générales concernant le risque que représentent les systèmes d'IA pour la vie privée et la protection des données continuent de s'appliquer à mesure que ces outils sont développés.[189]

Pour en savoir plus

- CEPEJ, *Charte éthique européenne sur l'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement* (2018), https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b
- Centre de ressources sur la cyberjustice et l'IA, Centre de ressources sur la cyberjustice et l'IA - Commission européenne pour l'efficacité de la justice (CEPEJ), Des informations détaillées sur le déploiement et l'utilisation des outils numériques dans l'administration de la justice sont disponibles dans les profils nationaux individuels.
- Glossaire sur la cyberjustice et l'IA : Glossaire Cyberjustice de la CEPEJ - Commission européenne pour l'efficacité de la justice (CEPEJ)
- On AI systems geared towards the private sector: *First Global Report on the State of Artificial Intelligence in Legal Practice*, 2023 https://globalailawreport.com/wp-content/uploads/2024/04/E-Book-First-Global-Report-on-AI-in-Legal-Practice.pdf (en anglais uniquement)
- *Lignes directrices de* la CEPEJ *sur la numérisation des dossiers judiciaires ('e-filing') et la digitalisation des tribunaux* (2021), https://rm.coe.int/cepej-2021-15-fr-numerisation-dossiers-digitalisation-tribunaux/1680a4cf2e
- *Lignes directrices de* la CEPEJ *sur les modes alternatifs de règlement en ligne des* (2023), https://rm.coe.int/cepej-2023-19final-fr-directrices-sur-les-modes-alternatives-de-reglem/1680adce34, y compris les bonnes pratiques liées aux lignes directrices.
- *Note d'information de* la CEPEJ *sur l'utilisation de l'IA générative par les professionnels de la justice dans un contexte professionnel* (2024) https://rm.coe.int/cepej-gt-cyberjust-2023-5final-fr-note-ia-generative/1680ae8e02
- Résolution 2081 (2015) de l'APCE sur l'*accès à la justice et internet : potentiel et défis,* https://pace.coe.int/fr/files/22283/html
- Résolution 2342(2020) de l'APCE sur la *Justice par algorithme - Le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale* https://pace.coe.int/fr/files/28805/html
- Comité européen de coopération juridique, *Intelligence artificielle et droit administratif,* étude comparative (2022) https://www.coe.int/documents/22298481/0/CDCJ%282022%2931F+-+FINAL+6.pdf/c01b86be-ce0e-ee18-f4b5-3b082c371eac?t=1670943281280

[189] *Charte éthique,* 2.3.1, §40 : « le volume et la variété d'informations qui sont contenues dans les décisions de justice, alliés à la facilité grandissante de procéder à des croisements avec d'autres bases de données, rendent en pratique impossible de garantir que la personne concernée ne soit pas ré-identifiée. En l'absence d'une telle garantie, ces données ne peuvent être qualifiées d'anonymes et relèvent donc du régime de protection des données personnelles. »

3.3.2 Soins de santé

107. Les soins de santé impliquent la fourniture de services médicaux visant à maintenir ou à améliorer le bien-être physique et mental, y compris la prévention, le diagnostic, le traitement et la rééducation, dispensés par des professionnels tels que des médecins et des infirmières dans des environnements tels que les hôpitaux, les cliniques, les établissements de soins primaires et les soins à domicile.

Principaux cas d'utilisation de l'IA

108. Les avancées technologiques majeures dans les systèmes d'IA ont le potentiel de faire progresser la biomédecine et de bénéficier aux soins de santé, mais leur impact et l'orientation de leurs développements sont encore incertains. Les systèmes d'IA sont développés pour une variété d'applications[190], englobant des applications auxiliaires, telles que l'automatisation des tâches administratives de routine, mais aussi des applications ayant un impact significatif sur la fourniture de services de santé de qualité et le traitement des patients, comme l'imagerie radiologique.

109. Les principaux cas d'utilisation de l'IA sont les suivants :

- *Pose de diagnostic médical :* Systèmes d'IA capables d'analyser des images médicales (radiographies, IRM, scanners, etc.) et d'évaluer les symptômes afin d'aider à identifier les maladies et à diagnostiquer les problèmes de santé.
- *Analyse prédictive* : Les systèmes d'IA utilisés pour prédire les résultats des patients, tels que le risque de maladie et les complications potentielles, grâce à l'analyse des données.
- *Médecine personnalisée* : Les systèmes d'IA qui aident à adapter les plans de traitement à chaque patient, en optimisant les thérapies médicamenteuses et les interventions médicales grâce à l'analyse des informations génétiques et d'autres données de santé.
- *Assistants de santé virtuels* : Les 'chatbots' et les assistants virtuels alimentés par l'IA qui apportent un soutien aux patients, notamment en matière de santé mentale, en répondant aux questions, en fixant des rendez-vous et en proposant des rappels de médicaments.
- *Télésurveillance et télémédecine* : Dispositifs portables alimentés par l'IA et plateformes de télésanté permettant le suivi des patients en dehors des cadres traditionnels.
- *Chirurgie robotique* : Les systèmes robotiques alimentés par l'IA améliorent la précision et le contrôle des opérations chirurgicales.

Droits humains et principes pertinents

110. Les États ont à la fois une obligation négative de ne pas interférer directement avec la santé d'un individu (sauf d'une manière justifiée par la CEDH) et une obligation positive, en vertu de l'article 8 de la CEDH, de prendre des mesures pour protéger la santé des personnes relevant de leur juridiction, selon ce qui est nécessaire et approprié dans les circonstances spécifiques. Bien que les questions de politique de santé relèvent en principe de la marge d'appréciation des États[191], les obligations positives exigent des États qu'ils légifèrent ou mettent en

[190] Pour un aperçu des applications de l'IA dans le domaine de la santé, voir Comité directeur pour les droits de l'homme dans le domaine de la biomédecine et de la santé (CDBIO), Rapport sur l'application de l'intelligence artificielle dans les soins de santé et son impact sur la relation « patient-médecin », septembre 2024, pp. 9-11. Pour plus de détails, Organisation mondiale de la santé, *Éthique et gouvernance de l'intelligence artificielle pour la santé* (2021), pp. 6-16.

[191] *Vavricka et autres c. République tchèque [GC],* No. 47621/13 et 5 autres, 8 avril 2021, §§ 274, 285.

œuvre des mesures pratiques pour protéger la santé et la vie des individus et veiller à ce qu'ils soient informés des risques sanitaires[192], qu'ils établissent des réglementations obligeant les hôpitaux à protéger la vie des patients[193], et qu'ils respectent des normes professionnelles élevées parmi les prestataires de soins de santé[194]. La Cour a interprété l'article 8 comme couvrant le droit à la protection de l'intégrité physique, morale et psychologique, ainsi que le droit d'exercer son autonomie personnelle et son autodétermination en faisant des choix concernant son corps, y compris en refusant un traitement médical ou en demandant une forme particulière de traitement médical[195]. Les autres articles à travers lesquels la Cour aborde les questions de santé sont l'article 2 (droit à la vie)[196], l'article 3 (interdiction de la torture)[197] et l'article 14 (interdiction de la discrimination)[198]. Dans sa jurisprudence concernant la santé, la Cour se réfère souvent à la Convention No. 108[199], la Convention d'Oviedo[200], ainsi qu'à d'autres instruments pertinents dans le cadre du Conseil de l'Europe ou au-delà[201].

111. La CSE garantit explicitement le droit à la santé (article 11) et à l'assistance sociale et médicale (article 13). L'accès aux soins de santé est une condition préalable à la préservation de la dignité humaine.[202] Les États doivent veiller à ce que les services de santé soient accessibles, efficaces et inclusifs en allouant des ressources suffisantes, en mettant en œuvre des procédures opérationnelles solides et en répondant aux besoins spécifiques des groupes vulnérables.[203] L'article 11 impose trois obligations essentielles pour les États, soit directement, soit en collaboration avec des organisations publiques ou privées : (i) prendre des mesures appropriées pour éliminer autant que possible les causes de maladie ; (ii) mettre en place des services consultatifs et éducatifs pour promouvoir la santé et encourager la responsabilité individuelle; et (iii) prendre des mesures pour prévenir autant que possible les maladies épidémiques, endémiques et autres, ainsi que les accidents. Les États sont en outre tenus de protéger les groupes vulnérables[204], tels que les sans-abris, les personnes âgées, les personnes handicapées et les personnes en situation irrégulière, en veillant à ce que leur droit à la santé ne soit pas entravé, même par des restrictions. Les étrangers résidant ou travaillant légalement sur le territoire d'une Partie ont droit à la protection de la santé en vertu de la CSE.

Droit à la vie privée et à la protection des données

112. L'article 8 de la CEDH protège les données personnelles relatives à la santé[205]. L'article 10 de la Convention d'Oviedo stipule que toute personne a) a droit au respect de sa vie privée s'agissant des informations

---

[192] *Brincat et autres c. Malte,* No. 60908/11 et 4 autres, 24 juillet 2014, § 101 *; Guerra et autres c. Italie,* No. 116/1996/735/932, 19 février 1998, §§ 57-60 *; Roche c. Royaume-Uni (GC),* No. 32555/96, 19 octobre 2005. 32555/96, 19 octobre 2005

[193] *Calvelli et Ciglio c. Italie [GC],* No. 32967/96, 17 janvier 2002, § 49 *; Mehmet Ulusoy et autres c. Turquie,* No. 54969/09, 25 juin 2019, § 90

[194] *Lopes de Sousa Fernandes c. Portugal* [GC], No. 56080/13, 19 décembre 2017, §§ 186-190.

[195] *Niemietz c. Allemagne*, No.13710/88, 16 décembre 1992, § 29 ; *Glass c. Royaume-Uni*, No. 61827/00, 9 mars 2004, §§ 74-83 ; *Tysiąc c. Pologne*, No.5410/03, 20 mars 2007, § 107 ; *Pindo Mulla c. Espagne* [GC], No.12345/19, 15 avril 2024, § 98 ; *Pretty c. Royaume-Uni*, No.2346/02, 29 avril 2002, § 63 ; *Taganrog LRO et autres c. Russie*, No.s 32401/10 et 19 autres, 7 novembre 2019, § 162.

[196] *Centre de ressources juridiques pour le compte de Valentin Campeanu c. Roumanie [GC],* No. 47848/08, 17 juillet 2014, §§ 145-147 *; Oyal c. Turquie,* No. 4864/05, 23 mars 2010, § 72

[197] *Paposhvili c. Belgique* [GC], No. 41738/10, 13 décembre 2016, §§ 183-193 ; *D. c. Royaume-Uni*, no. 30240/96, 2 mai 1997, § 54 ; *Aswat c. Royaume-Uni*, No.17299/12, 16 avril 2013, §§ 55-57.

[198] *Kiyutin c. Russie,* No. 2700/10, 10 mars 2011, §§ 56-58, 74

[199] Par exemple, *S. et Marper c. Royaume-Uni* [GC], 2008, §§ 41 et 103.

[200] *Glass c. Royaume-Uni*, 2004, § 58.

[201] Par exemple, voir la référence dans *Biriuk c. Lituanie* (no 23373/03, 25 novembre 2008, § 21) à la Recommandation no. R (89) 14 du Comité des Ministres du Conseil de l'Europe sur « Les incidences éthiques de l'infection VIH dans le cadre sanitaire et social » (1989) ou la référence dans Pindo Mulla c. Espagne, (GC) No.15541/20, 17 septembre 2024, § 77, à la Déclaration universelle sur la bioéthique et les droits de l'homme adoptée par l'UNESCO en 2005.

[202] *Fédération internationale pour les droits humains (FIDH) c. France*, No. 14/2003, 3 novembre 2004, §31.

[203] Déclaration d'interprétation sur le droit à la protection de la santé en cas de pandémie, 21 avril 2020.

[204] *Commission internationale de juristes (CIJ) et Conseil européen pour les réfugiés et les exilés (ECRE) c. Grèce,* réclamation No. 173/2018, décision sur le fond du 26 janvier 2021, §218.

[205] *Surikov c. Ukraine*, No. 42788/06, 26 janvier 2017, §§ 70 et 89.

relatives à sa santé et b) a le droit de connaître toute information collectée sur sa santé. Les données personnelles relatives à la santé sont explicitement considérées comme sensibles en vertu de la Convention 108 (article 6) ainsi que des cadres réglementaires régionaux et nationaux[206]. Le Comité des Ministres du Conseil de l'Europe a publié des lignes directrices spécifiques sur la protection des données relatives à la santé dans sa Recommandation CM/Rec(2019)2, qui vise à garantir que les principes de la Convention No. 108, y compris sa version modernisée, sont pleinement appliqués à l'échange et au partage des données relatives à la santé.

113. Les systèmes d'IA dans le domaine de la santé peuvent s'appuyer fortement sur des données sensibles relatives aux patients, notamment des dossiers médicaux et des informations biométriques, pour la prise de décisions, les prédictions, la formation, les tests et la validation. La sécurité des données, la confidentialité et l'utilisation abusive potentielle, comme les violations ou le partage non autorisé, font partie des préoccupations[207]. En outre, les individus peuvent être confrontés à des difficultés pour exercer un contrôle sur leurs données, en particulier lorsqu'elles sont incluses dans des ensembles de données d'entraînement à l'IA. La divulgation de données sur la santé peut avoir de profondes répercussions sur la vie privée et familiale, ainsi que sur la situation sociale et professionnelle, avec un risque de stigmatisation et d'exclusion. C'est pourquoi les législations nationales doivent prévoir des garanties pour empêcher le partage ou la divulgation non autorisés, afin de respecter les garanties de l'article 8[208].

Non-discrimination et accès équitable aux soins de santé

114. La CEDH et la CSE interdisent la discrimination.[209] En vertu de l'article 3 de la convention d'Oviedo, les États parties sont tenus de prendre les mesures appropriées en vue d'assurer, dans les limites de leur juridiction, un accès équitable à des soins de santé de qualité appropriée.

115. Les biais dans les données utilisées pour développer et entraîner les systèmes d'IA peuvent fausser l'évaluation des besoins de santé et des traitements des patients. Il est à noter que les modèles d'IA formés principalement à partir de données provenant de populations spécifiques peuvent poser des diagnostics erronés ou sous-estimer la gravité de la maladie dans les groupes sous-représentés tels que les femmes et les filles, les personnes appartenant à des minorités ethniques, les populations autochtones, les personnes âgées ou les personnes handicapées[210]. On peut citer comme exemples les systèmes de hiérarchisation des greffes de rein, où des données historiques biaisées ont faussé les résultats au détriment de certains patients.[211] De même, une

[206] Comme exemple de cadre régional (qui est également le cadre national des trente États membres du Conseil de l'Europe qui l'appliquent), voir les articles 4 et 9 et les considérants 35 et 53 du GDPR, avec les définitions des termes « données de santé », « données génétiques », « données biométriques ».

[207] Voir également le rapport du CDBIO sur le rôle des professionnels de la santé et des prestataires de soins de santé dans la collecte, la génération et l'enrichissement, ainsi que dans la sauvegarde des données de santé, pp. 21-23, qui fait référence à une décision rendue en 2017 par l'Information Commissioner's Office (ICO) du Royaume-Uni, constatant une violation de la loi applicable en matière de protection des données et du droit à la vie privée dans le cas d'un établissement de soins de santé ayant accordé à une société privée l'accès à plus d'un million de fichiers de données de patients pseudonymisés afin de tester un système d'intelligence artificielle en cours de développement.

[208] *Z. c. Finlande*, No. 22009/93, 25 février 1997, § 95

[209] Voir le préambule de l'année 1961 du CES et la partie V-article E de la Charte sociale européenne (révisée).

[210] Voir par exemple le rapport du CDBIO, p. 26 ; voir également OMS, Ethics and governance of artificial intelligence for health (2021), pp. 54-57. En outre, sur la sous-représentation et la faible qualité des données des femmes, ainsi que des personnes de divers genres dans la recherche scientifique, l'étude GEC/CDADI, p. 25. Également (p. 26) sur la discrimination structurelle intégrée dans les systèmes d'IA à l'égard des patients systématiquement défavorisés issus de minorités ethniques. Voir également l'OMS, Ageism in artificial intelligence for health (2022), qui montre que les systèmes algorithmiques utilisés dans le secteur de la santé sont entraînés sur les données de populations majoritairement jeunes, ce qui entraîne des performances disproportionnellement plus faibles de ces systèmes pour les patients plus âgés, y compris des diagnostics erronés www.who.int/publications/i/item/9789240040793.
En anglais uniquement : www.technologyreview.com/2019/10/25/132184/a-biased-medical-algorithm-favored-white-people-for-healthcare-programswww.weforum.org/stories/2024/02/racial-bias-equity-future-of-healthcare-clinical-trial

[211] Voir, par exemple (en anglais uniquement) : www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients ; https://algorithmwatch.org/en/racial-health-bias-switzerland.

représentation inadéquate dans les ensembles de données de formation a conduit à des diagnostics erronés d'affections cutanées[212]. En outre, on craint que l'accès aux avantages offerts par l'IA dans le domaine des soins de santé ne soit pas également disponible pour tous. Le déploiement de ces soins peut être inégal sur le plan géographique dans un pays donné, ou dépendre des moyens financiers des patients[213]. Les États devraient adopter des mesures pour veiller à ce que les systèmes d'IA soient développés et déployés de manière équitable, avec des données de formation représentatives et des garanties contre les préjugés.

Consentement éclairé, autonomie et prise de décision

116. Le consentement éclairé et l'autonomie de décision du patient[214] sont garantis par l'article 8 de la CEDH[215] et l'article 11 de la CSE[216]. L'article 5 de la convention d'Oviedo exige un consentement libre et éclairé pour les interventions sanitaires, avec une information préalable sur l'objectif, les risques et les conséquences. Le consentement peut être retiré à tout moment. Une attention particulière est accordée aux situations d'urgence et aux personnes incapables de donner leur consentement[217].

117. Les individus doivent pouvoir donner ou refuser librement leur consentement à toute intervention, comprenant tous les actes médicaux, y compris ceux effectués à des fins de soins préventifs, de diagnostic, de traitement, de rééducation ou de recherche. Leur consentement est considéré comme libre et éclairé lorsqu'il est donné sur la base d'informations objectives fournies par le professionnel de santé responsable, qui répond notamment de manière adéquate aux demandes d'informations complémentaires. La nature « boîte noire » de nombreux systèmes d'IA qui produisent des résultats probabilistes rend difficile la compréhension et l'évaluation de la nécessité ou de l'utilité de l'intervention. Il est donc difficile pour les individus de prendre une décision sur le consentement. C'est également un défi pour les médecins chargés d'interpréter les résultats des systèmes d'IA.[218] En outre, en l'absence d'exigences adéquates en matière de transparence et de contrôle des systèmes d'IA et de formation des médecins qui les utilisent, on peut craindre une « déqualification » des professionnels de santé et une dépersonnalisation de la relation patient-médecin.[219]

Pour en savoir plus

- CDBIO, *Rapport sur l'application de l'intelligence artificielle dans les soins de santé et son impact sur la relation 'patient-médecin'* (2024) : https://www.coe.int/fr/web/human-rights-and-biomedicine/ai-in-healthcare

[212] Voir, par exemple (en anglais uniquement) : www.theguardian.com/society/2021/nov/09/ai-skin-cancer-diagnoses-risk-being-less-accurate-for-dark-skin-study

[213] Rapport CDBIO, p. 26. Concernant la discussion sur la possibilité que la fracture numérique existante (y compris en ce qui concerne l'IA) et les inégalités (au sein des pays et entre eux, ainsi qu'entre les groupes sociaux) exacerbent la répartition inégale des soins de santé et les problèmes d'accès effectif aux soins de santé, voir la recommandation PACE 2185 (2020), *Intelligence artificielle et santé : défis médicaux, juridiques et éthiques* à venir. Une préoccupation supplémentaire pourrait être liée à l'utilisation de l'IA pour l'allocation des ressources et la hiérarchisation des cas.

[214] L'autonomie va au-delà du consentement éclairé et engendre un rôle plus actif pour le patient dans la prise de décision partagée, englobant, par exemple, le choix de prendre des mesures préventives, de demander un deuxième avis ou d'introduire ses propres valeurs, préférences et perspectives dans les communications patient-médecin (Rapport CDBIO p. 13).

[215] *Trocellier c. France* (déc.), No. 75725/01, 13 avril 2007, § 4 ; *Mayboroda c. Ukraine*, No. 14709/07, § 52.

[216] Trocellier c. France (déc.), No. 75725/01, 13 avril 2007, § 4 ; Mayboroda c. Ukraine, No. 14709/07, § 52.

[217] Articles 6 à 8. Voir également le rapport explicatif de la convention d'Oviedo, paragraphes 35-36.

[218] Concernant la fiabilité des normes professionnelles qui examinent la sécurité, la qualité et l'efficacité des systèmes d'IA, la surveillance humaine et l'explicabilité des résultats de l'IA, voir le rapport du CDBIO, p. 28.

[219] Conformément à l'article 4 de la Convention d'Oviedo, toute intervention dans le domaine de la santé doit être effectuée dans le respect des obligations et des normes professionnelles pertinentes. Cela est interprété comme une obligation pour les professionnels de la santé de prêter une attention particulière aux besoins spécifiques de chaque patient. Voir les paragraphes 32 et 33 du rapport explicatif de la Convention d'Oviedo.

- Rapport de l'expert consultant sur l'impact de l'intelligence artificielle sur la relation médecin-patient, Brent Mittelstadt, chercheur principal et directeur de recherche à l'Oxford Internet Institute, Université d'Oxford, Royaume-Uni.
- *Plan d'action stratégique sur les droits de l'homme et les technologies en biomédecine (2020-2025),* 2019 : https://rm.coe.int/plan-d-action-strategique-final-f/1680a2c5d1
- Recommandation CM/Rec (2019)2 du Comité des Ministres aux États membres sur la « *Protection des des données relatives à la santé* » : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168093b26b
- Recommandation 2185 (2020) de l'APCE, L'*intelligence artificielle dans les soins de santé : défis médicaux, juridiques et éthiques à venir* : https://pace.coe.int/fr/files/28813/html
- Commission pour l'égalité entre les femmes et les hommes et Comité directeur sur la lutte contre la discrimination, la diversité et l'inclusion, *Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel de promotion de l'égalité, y compris de l'égalité de genre, et les risques qu'ils peuvent entraîner en matière de non-discrimination* (2023) : https://edoc.coe.int/fr/intelligence-artificielle/11646-etude-sur-limpact-des-systemes-dintelligence-artificielle-leur-potentiel-de-promotion-de-legalite-y-compris-legalite-de-genre-et-les-risques-quils-peuvent-entrainer-en-matiere-de-non-discrimination.html
- OMS, *Éthique et gouvernance de l'intelligence artificielle pour la santé* (2021) : https://iris.who.int/bitstream/handle/10665/350568/9789240037427-fre.pdf?sequence=1
- OMS *Ethics and governance of artificial intelligence for health* (2021) (en anglais uniquement) https://www.who.int/publications/i/item/9789240029200
- OMS, *Éthique et gouvernance de l'intelligence artificielle pour la santé : Orientations concernant les grands modèles multimodaux* (2024) : https://iris.who.int/bitstream/handle/10665/350568/9789240037427-fre.pdf?sequence=1
- PNUE, *Navigating New Horizons, A global foresight report on planetary health and human well-being* (2024) (en anglais uniquement) : https://www.unep.org/resources/global-foresight-report

3.3.3 Services sociaux et protection sociale

118. Les services sociaux englobent un large éventail de programmes et de services destinés à promouvoir le bien-être de l'homme et de la société. Outre les services publics fondamentaux tels que l'accès à l'éducation et aux soins de santé, abordés dans leurs chapitres respectifs de ce Manuel [ajouter la référence au numéro de chapitre ultérieurement], les services sociaux et les systèmes de protection sociale fournissent une aide financière et non financière. Il s'agit notamment des de sécurité sociale qui offrent un soutien financier aux personnes âgées, aux personnes handicapées et aux survivants sur la base des cotisations des travailleurs ; des allocations de chômage ; de l'aide au logement (subventions ou logements sociaux) et du soutien aux sans-abri ou aux personnes risquant de le devenir ; du revenu minimum garanti ou des prestations en nature, telles que l'aide alimentaire aux familles à faible revenu ; des services à l'enfance et à la famille, y compris les subventions pour la garde d'enfants, les programmes et outils visant à lutter contre la violence domestique, et les services de protection de l'enfance ; du soutien aux personnes âgées et handicapées.

Principaux cas d'utilisation de l'IA

119. L'IA est de plus en plus intégrée aux services sociaux, allant de l'automatisation des tâches de routine telles que la prise de notes et la gestion des dossiers à des applications plus complexes ayant un impact significatif. Les principales fonctions basées sur l'IA sont les suivantes :

- *Analyse prédictive :* Les systèmes d'IA capables d'analyser de grands ensembles de données à l'aide de processus algorithmiques, y compris l'apprentissage automatique, pour identifier les individus ou les groupes les plus susceptibles d'avoir besoin de services sociaux. Cela permet aux agences d'allouer de manière proactive le soutien et les ressources, par exemple en identifiant les enfants à risque qui pourraient avoir besoin d'une aide supplémentaire.
- *Allocation des ressources :* Les modèles basés sur l'IA optimisent la distribution de ressources généralement limitées, garantissant une prestation de services plus efficace et plus équitable.
- *Filtrage et détection des fraudes* : Les systèmes d'IA sont utilisés pour aider à filtrer les candidats, vérifier leurs informations, signaler les incohérences et identifier les schémas révélateurs de fraude ou d'utilisation abusive des services sociaux, améliorant ainsi la responsabilité et l'efficacité.
- *Les 'chatbots' et les assistants virtuels pilotés par l'IA* : Ces systèmes traitent les demandes de routine, améliorent l'accessibilité pour les personnes handicapées grâce à la reconnaissance vocale ou à la transcription automatique, et surveillent la santé physique et mentale des individus, en émettant des alertes pour assurer des interventions en temps utile.
- *Vue d'ensemble et évaluation :* L'IA analyse les résultats des services sociaux pour évaluer leur efficacité, en fournissant des informations basées sur des données qui aident les agences à affiner leurs politiques et à améliorer la prestation de services au fil du temps.

Droits humains et les principes pertinents

120. La fourniture de services sociaux peut interférer directement avec la jouissance par un individu de ses droits, tels que le droit à la vie familiale au sens de l'article 8 de la CEDH[220], le droit à la liberté au sens de l'article

[220] Par exemple, en ce qui concerne les décisions relatives au déplacement des enfants, au placement et à l'adoption, à la détermination du droit de garde et du droit de visite, voir *B. c. Royaume-Uni,* 8 juillet 1987, no 9840/82, §§ 60-65 ; *Saviny c. Ukraine,* 18 décembre 2008, 39948/06, §§ 57-42 ; *A.K. et L. c. Croatie*, 8 janvier 2013, 37956/11, §§ 58-60. Voir aussi, pour les obligations des autorités nationales de faciliter les visites familiales et, dans des cas exceptionnels, d'assurer un abri aux personnes particulièrement vulnérables, *A et autres c. Italie*, 7 décembre 2003, 17791/22, §§ 93-104.

5[221], ou le droit à la propriété au sens de l'article 1 du Protocole n° 1[222]. En outre, des services sociaux efficaces contribuent à l'accomplissement des obligations positives de l'État en matière de prévention des mauvais traitements administrés par des personnes privées (article 3)[223].

121. Les États disposent d'une marge d'appréciation dans les domaines impliquant l'application de politiques sociales ou économiques[224]. En outre, la Cour respecte généralement les choix politiques nationaux, à moins qu'ils ne soient « manifestement dépourvu de base raisonnable »[225]. C'est particulièrement le cas dans le contexte de l'allocation des ressources limitées de l'État[226]. La Cour a ainsi estimé qu'il était légitime pour les États de mettre en place des critères selon lesquels une prestation peut être attribuée, lorsque l'offre est insuffisante pour satisfaire la demande, pour autant que ces critères ne soient pas arbitraires ou discriminatoires[227]. Cela signifie que lorsqu'un État décide d'accorder de telles prestations, il doit le faire de manière non discriminatoire (article 14 de la CEDH et article 12 de la CSE). La marge d'appréciation de l'État est considérablement réduite lorsque la distinction de traitement est fondée sur une caractéristique personnelle inhérente ou immuable telle que la race, le sexe, la nationalité ou le handicap, et des « raisons très sérieuses » seraient nécessaires pour justifier la différence de traitement en question[228].

122. La CSE oblige les États parties à garantir un accès non discriminatoire à la sécurité sociale[229], à l'assistance sociale et médicale[230] et aux services de protection sociale[231]. Elle exige qu'un système de sécurité sociale garantisse l'accès effectif aux prestations prévues par chaque branche[232]. L'égalité de traitement doit être assurée aux ressortissants d'autres États parties résidant légalement ou travaillant régulièrement sur le territoire de l'État partie concerné, ainsi qu'aux réfugiés et aux apatrides.[233]

Droit à la vie privée et à la protection des données

123. L'utilisation de l'IA dans les services sociaux implique le traitement de données personnelles sensibles, ce qui soulève de sérieuses préoccupations en matière de respect de la vie privée au titre de l'article 8 de la

---

[221] Par exemple, en ce qui concerne l'enfermement obligatoire des personnes « incapables de discernement ». Voir, entre autres, *Ilnseher c. Allemagne* [GC]*,* 4 décembre 2018, No.10211/12 et 27505/14, §§ 126-134.

[222] Pour une synthèse complète de la jurisprudence de la Cour relative à la sécurité sociale/aux prestations sociales, voir *Béláné Nagy c. Hongrie* [GC], 13 décembre 2016, No/ 53080/13, §§ 80-89 ; *Yavaş et autres c. Turquie*, No. 36366/06, 5 mars 2019, 36366/06, §§ 39-43.

[223] Voir, entre autres, *Z. et autres c. Royaume-Uni,* 10 mai 2001, No. 29392/95, §121, concernant le manquement des services sociaux de l'Etat défendeur à prendre des mesures de protection adéquates dans un cas de maltraitance d'enfant ; ainsi que V.C. *c. Italie,* 1er février 2018, No. 54227/14, §89. De même, en ce qui concerne l'absence de protection des victimes de violence domestique, voir *Opuz c. Turquie,* 9 juin 2009, No. 33401/02, §159 ; *Talpis c. Italie,* 2 mars 2017, No. 41237/14, § 141, également en liaison avec l'article 14 et l'absence de garantie par l'Etat du droit des femmes à une égale protection devant la loi.

[224] Par exemple, en ce qui concerne le logement, voir, entre autres, *Hudorovič et autres c. Slovénie*, 10 mars 2020, Nos. 24816/14 et 25140/14 et *Forum européen des Roms et des Gens du voyage (ERTF) c. France*, No. 64/2011, 24 janvier 2012, § 95 ; concernant les pensions de vieillesse, *Fábián c. Hongrie*, 5 septembre 2017, No. 78117/13, § 67 ; concernant les pensions de réversion, *Muñoz Díaz c. Espagne*, 8 décembre 2009, No.49151/07, §§ 48-49, etc. ; concernant les politiques de l'emploi, voir, *Fédération générale des employés de la société nationale d'électricité (GENOP-DEI) / Confédération des syndicats de fonctionnaires grecs (ADEDY) c. Grèce*, No. 66/2011, 23 mai 2012, §20.

[225] *Stec et autres c. Royaume-Uni* [GC], 12 avril 2006, Nos. 65731/01 et 65900/01, § 52

[226] *Šaltinytė c. Lituanie*, 26 octobre 2021, No. 32934/19, §§ 64 et 77.

[227] *Bah c. Royaume-Uni*, 27 décembre 2011, No. 56328/07, § 52

[228] *Savickis c. Lettonie* [GC], 9 juin 2022, No. 49270/11, § 83 ; *J.D. et A. c. Royaume-Uni*, 24 octobre 2019, No. 32949/17, No. 34614/17, §§ 88-89, 97 et 104 ; *Andrejeva c. Lettonie* [GC], 18 février 2009, No. 55707/00, § 87 ; *Ribać c. Slovénie*, 5 mars 2018, No. 57101/10, § 53.

[229] CSE, article 12 ; voir également le recueil de jurisprudence du Comité européen des droits sociaux, décembre 2022, p. 119 et suivantes.

[230] CSE, article 12.

[231] CSE, article 14.

[232] Digest de jurisprudence du Comité européen des droits sociaux, décembre 2022, p. 120.

[233] CSE, article 12, paragraphe 4 ; paragraphe 1 de l'annexe de la CSE.

CEDH. L'agrégation de données sensibles, telles que les dossiers médicaux, les antécédents financiers et professionnels et d'autres détails personnels, qui permet à l'État d'acquérir un profil détaillé des aspects les plus intimes de la vie des citoyens, peut entraîner une ingérence particulièrement envahissante dans la vie privée[234]. Par exemple, des préoccupations liées au respect de l'article 8 de la CEDH ont été soulevées dans l'affaire « SyRi », où le tribunal de district de La Haye a estimé qu'un algorithme utilisé pour identifier les fraudes potentielles à l'aide sociale (le 'Systeem Risico Indicatie' ou 'SyRi') et la législation correspondante ne répondaient pas aux exigences de nécessité et de proportionnalité requises par l'article 8, paragraphe 2, de la CEDH[235].

124. Un risque supplémentaire est l'utilisation abusive des données personnelles collectées dans les services sociaux, y compris la surveillance non autorisée, le profilage sans consentement, ou les violations accidentelles. L'implication des entreprises dans le développement ou la maintenance des systèmes d'IA ou l'externalisation des services sociaux auprès d'entreprises privées suscitent également des inquiétudes Étant donné que les systèmes d'IA stockent de grandes quantités de données sensibles, il convient d'accorder une importance particulière à la sécurité des données, y compris lorsqu'un système d'IA particulier est développé et entretenu par des fournisseurs tiers (privés).

Non-discrimination et égalité

125. L'utilisation de l'IA dans les services sociaux peut perpétuer la discrimination (y compris indirecte et intersectionnelle) en raison des préjugés intégrés dans les données sociétales, tels que les préjugés raciaux, sexistes ou socio-économiques. Cela peut conduire à un refus injuste de services ou de prestations, affectant de manière disproportionnée les groupes marginalisés et compromettant l'égalité d'accès à ces services. Les systèmes d'analyse prédictive, de détection des fraudes et d'allocation des ressources sont particulièrement vulnérables aux préjugés, car ils reposent sur des données historiques et sont susceptibles d'exacerber les discriminations structurelles et les stéréotypes. Par exemple, un système de détection des fraudes formé sur des données qui reflètent de manière disproportionnée les expériences de certains groupes est susceptible de développer des profils de risque et de créer des liens basés sur des préjugés, tels qu'un statut socio-économique inférieur ou des antécédents en matière d'immigration. Cela peut conduire à des recommandations biaisées et finalement à la violation du droit à la non-discrimination non seulement des individus mais aussi de populations entières perçues par le système comme homogènes, à moins qu'il n'y ait des garanties, y compris une supervision humaine, assurant l'évaluation critique des résultats de l'IA et neutralisant ainsi le risque d'effets discriminatoires[236].

126. La Cour a estimé que les autorités de l'État ont le devoir de prendre toutes les mesures raisonnables pour vérifier, par l'intermédiaire d'un organisme indépendant, si un certain traitement a été influencé par une attitude discriminatoire et de mener une enquête efficace à cet égard[237].

---

[234] *Szabó et Vissy c. Hongrie*, No. 37138/146, 12 janvier 2016, § 70.

[235] The Hague District Court, *NCJM* et al. *and FNV v The State of the Netherlands*, 6 mars 2020, disponible en anglais sur uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 (ECLI:NL:RBDHA:2020:865). Il s'agit du 'Systeem Risico Indicatie' ou 'SyRi'. Il convient de noter que le rapporteur spécial des Nations unies sur l'extrême pauvreté et les droits humains a présenté un mémoire d'*amicus curiae* soulignant en particulier l'effet discriminatoire et stigmatisant du SyRi, qui visait principalement les pauvres et d'autres groupes vulnérables, ou, comme l'a admis l'État lors des audiences, les 'quartiers à problèmes'.
https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf (en anglais uniquement)

[236] Il convient toutefois de noter que l'implication humaine ne suffit pas à elle seule à neutraliser les risques de discrimination ; dans le scandale des allocations familiales néerlandaises, par exemple, un fonctionnaire était chargé d'examiner manuellement les demandes présentant le score de risque le plus élevé, sans toutefois recevoir d'informations sur les raisons pour lesquelles le système avait attribué un score de risque élevé à une demande spécifique. Toutefois, on a observé que les fonctionnaires avaient tendance à généraliser le comportement des individus de la même race ou de la même ethnie, les percevant de manière stéréotypée comme frauduleux ou déviants.

[237] *Basu c. Allemagne*, No. 215/19, 18 octobre 2022, §38.

Transparence et responsabilité

127. Comme nous l'avons déjà observé, les processus décisionnels de l'IA peuvent être opaques, de sorte qu'il est difficile de comprendre comment et pourquoi une décision a été prise. Ce manque de transparence peut nuire à la responsabilité dans la prestation des services sociaux, en particulier lorsque des personnes se voient refuser des prestations ou des services sur la base de décisions de l'IA. Si une personne est désavantagée par une décision d'IA (par exemple, si elle se voit refuser à tort des prestations sociales), il peut être difficile pour elle de faire appel ou de contester la décision en raison de la nature « boîte noire » de nombreux systèmes d'IA, que ce soit intentionnel (c'est-à-dire pour des considérations de propriété intellectuelle) ou intrinsèque (c'est-à-dire trop compliqué pour quelqu'un qui n'a pas de compétences numériques particulièrement poussées).

128. Le manque de transparence et de responsabilité dans l'utilisation des systèmes d'IA peut conduire à priver les sujets des décisions d'IA d'une explication ou de la possibilité de faire appel contre des décisions qui, dans certains cas, peuvent être d'une importance vitale pour eux. Dans les cas où les événements en question relèvent entièrement, ou en grande partie, de la connaissance exclusive des autorités, comme ce serait sans doute le cas lorsque des systèmes d'IA sont impliqués, ou lorsqu'il serait extrêmement difficile en pratique pour le demandeur de prouver la discrimination, la Cour/ le CEDS a déplacé la charge de la preuve sur les autorités[238].

Accessibilité et qualité des soins

129. Les groupes vulnérables tels que les personnes âgées, les personnes handicapées ou celles dont la culture numérique ou l'accès aux technologies modernes sont limités peuvent être mal équipés pour interagir avec les systèmes d'IA. Ces groupes peuvent rencontrer des difficultés pour accéder aux services basés sur l'IA, qu'il s'agisse de simples plateformes d'application en ligne, de ‘chatbots’ ou d'assistants virtuels. Cela pourrait entraîner l'exclusion des services sociaux et, par conséquent, exacerber les inégalités existantes.

130. À l'autre extrémité de la prestation de services sociaux, le recours aux systèmes d'IA soulève des questions liées à la qualité. Dans la plupart des cas, ces systèmes sont conçus pour soutenir les décisions prises par des professionnels humains et ne doivent pas remplacer le jugement humain. Néanmoins, comme le montre la jurisprudence nationale, il peut y avoir des cas où les professionnels manquent de temps, de ressources ou sont simplement enclins à l'automatisation et réticents à utiliser leur expertise professionnelle pour parvenir à une décision différente de celle recommandée par le système. Les systèmes d'IA ne sont toutefois pas à l'abri des erreurs[239], et les erreurs en matière de bien-être peuvent être fatales pour certains des membres les plus vulnérables de nos sociétés. En outre, on craint que les services sociaux ‘numériques par conception’ et le recours excessif à l'IA ne conduisent à l'érosion des compétences des travailleurs sociaux, ce qui nuirait à la qualité du service, en particulier dans les cas complexes et délicats.

Pour en savoir plus

---

[238] *Salman c. Turquie* [GC], NO. 21986/93 , 27 juin 2000, No. 21986/93, § 100 ; *Anguelova c. Bulgarie*, No. 8361/97, 13 juin 2002, 38361/97 § 111 ; No. 3891/19, *Cînţa c. Roumanie*, 18 février 2020, No. 3891/19, § 79 ; *Mental Disability Advocacy Centre (MDAC) c. Bulgarie*, No. 41/2007, 3 juin 2008, § 52.

[239] Par exemple, au Royaume-Uni, l'arrêt *Johnson et autres c. SSWP* (EWCA Civ 778, Judgement, *Secretary of State for Work et Pensions c Johnson et al*, *Case Nos : CO/1643/2018 CO/1552/2018*, https://www.judiciary.uk/wp-content/uploads/2019/01/johnson-and-others-judgment-final.pdf) a soulevé d'importantes questions découlant de la mise en œuvre d'un système d'IA prenant des décisions en matière de prestations et d'aide sociale pour le système alors nouvellement introduit du crédit universel (un paiement unique d'aide sociale comprenant un montant personnel de base reflétant également les besoins en matière de garde d'enfants, de logement et d'autres besoins prescrits). Les demandeurs ont fait valoir que le système d'évaluation automatisé utilisé pour calculer le montant du crédit universel payable à chaque demandeur était illégal et pouvait créer une insécurité des revenus, tandis que l'État a reconnu que la méthode était "malheureuse" et "arbitraire", mais que la refonte du système « à partir de zéro » pour tenir compte des ajustements serait trop onéreuse. Cette défense a été rejetée et la contestation a abouti, au motif que les effets, dans ces cas, ont été jugés contraires à la politique et aux objectifs des règlements sous-jacents de l'UC et donc « irrationnels ».

- Recommandation CM/Rec(2011)12 du Comité des Ministres aux États membres sur les droits de l'enfant et les services sociaux adaptés aux enfants et aux familles : https://www.coe.int/t/dg3/children/keylegaltexts/SocialServicesSept2012_fr.pdf
- Conseil de l'Europe, *Children rights and social services, Report on the implementation of the Council of Europe Recommendation on children's rights and social services friendly to children and families (*2016) (en anglais uniquement) : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680649301
- (En anglais uniquement) Report of the Special Rapporteur on extreme poverty and human rights on the "privatization of public services", United Nations General Assembly document A/73/396, 26 September 2018
- (En anglais uniquement) Report of the Special Rapporteur on extreme poverty and human rights on the "digital welfare state", United Nations General Assembly document A/74/493, 11 October 2019
- (En anglais uniquement) Amnesty International, Xenophobic Machines : Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal, 2021: https://www.amnesty.org/en/documents/eur35/4686/2021/en/
- GEC et CDADI, *Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel de promotion de l'égalité, y compris de l'égalité de genre, et les risques qu'ils peuvent entraîner en matière de non-discrimination,* préparée par Ivana Bartoletti et Raphaële Xenidis, 2023 : https://edoc.coe.int/fr/intelligence-artificielle/11646-etude-sur-limpact-des-systemes-dintelligence-artificielle-leur-potentiel-de-promotion-de-legalite-y-compris-legalite-de-genre-et-les-risques-quils-peuvent-entrainer-en-matiere-de-non-discrimination.html
- Commission de Venise, *Pays-Bas - Avis sur la protection juridique des citoyens,* Avis n° 1031/2021, document CDL-AD(2021)031,
- https://www.venice.coe. int/webforms/documents/?pdf=CDL-AD(2021)031-e Déclaration du Comité des Ministres sur le risque de prise de décision assistée par ordinateur ou fondée sur l'intelligence artificielle dans le domaine de la protection sociale, Decl(17/03/2021)2, https://rm.coe.int/0900001680a1cb98

3.3.4 Application de la loi et sécurité publique

131. Ce secteur comprend la police[240], les services de renseignement et assimilés[241], y compris des questions telles que l'identification des personnes à des fins d'application de la loi, la prévention de la criminalité, les enquêtes criminelles, les programmes concernant la protection des personnes en danger (par exemple, les victimes de violence domestique ou les témoins protégés), les arrestations et les détentions, la prison et la probation la gestion des foules lors d'événements publics et le maintien de l'ordre public, la lutte contre le terrorisme, les opérations de sécurité nationale, les mesures impliquant la surveillance des communications, les restrictions, les interdictions, les fermetures, les diverses formes de surveillance, y compris celles qui affectent la liberté de mouvement.

Principaux cas d'utilisation de l'IA[242]

- *La criminalistique numérique* : Plusieurs outils et techniques de récupération et d'analyse des données ont été développés avec des composants d'IA. Ces outils permettent de récupérer des fichiers effacés, d'accéder à des données provenant d'appareils endommagés, de restituer des éléments d'information fragmentés dans des formats cohérents et d'étudier l'empreinte numérique des criminels.
- *Systèmes de surveillance* : technologies telles que la classification d'images, la vision par ordinateur et la biométrie, y compris la reconnaissance faciale automatisée, les empreintes digitales ou la catégorisation biométrique.
- *Analyse de données et police prédictive* : utilisation de méthodes statistiques pour extraire des informations de vastes ensembles de données, par exemple sur les casiers judiciaires, les événements et les facteurs environnementaux identifiés dans les études criminologiques, ainsi que des données non structurées provenant de sources de renseignements en libre accès et de sources de renseignements sur les médias sociaux.
- *Traitement du langage naturel :* exécution de tâches par le traitement de données textuelles, telles que la classification et le regroupement de textes, le résumé de textes et la traduction automatique.

Droits humains et principes pertinents

132. L'utilisation de systèmes d'IA dans le domaine de l'application de la loi et de la sécurité publique pourrait présenter des risques particuliers pour les droits humains. En effet, les décisions qui pourraient être prises sur la base des résultats des systèmes d'IA, telles que la surveillance, les perquisitions et les saisies, ou les arrestations et les détentions, ont un fort impact sur les droits humains. L'utilisation de systèmes d'IA dans ce secteur peut interférer avec les articles 5 (droit à la liberté et à la sécurité), 8 (droit au respect de la vie privée et familiale), 10 (liberté d'expression) et 11 (liberté de réunion et d'association) de la CEDH. Les États peuvent justifier l'ingérence dans les articles 8, 10 et 11 de la CEDH par les buts légitimes énumérés dans le texte de ces articles, notamment la sécurité nationale, la sûreté publique ou la défense de l'ordre et la prévention des infractions pénales.

Le droit à la liberté et à la sécurité

---

[240] La police désigne les forces ou services de police traditionnels et d'autres services autorisés et/ou contrôlés par l'État, chargés par ce dernier, dans le plein respect de l'État de droit, de fournir des services de maintien de l'ordre.

[241] Départements ou unités du gouvernement qui sont considérés comme équivalents aux services de renseignement du point de vue de leur fonction.

[242] Basé sur le rapport suivant : Europol : AI and policing - The benefits and challenges of artificial intelligence for law enforcement (2024).

133. Les systèmes de police prédictive font des estimations et des prédictions qui peuvent être transformées en actions ou décisions concrètes par le système de justice pénale, y compris en matière d'arrestation et de détention. En raison des décisions qui pourraient être prises sur la base des résultats de ces systèmes, des questions relatives à l'article 5 de la CEDH (droit à la liberté et à la sûreté) peuvent se poser. Les décisions d'arrestation ou de détention doivent être fondées sur des soupçons raisonnables, vérifiables et objectifs[243]. Si les informations fournies par les systèmes de police prédictive sont utilisées pour corroborer les soupçons raisonnables justifiant une décision d'arrestation ou de détention, les questions d'explicabilité et d'interprétabilité (le « problème de la boîte noire ») concernant les systèmes d'IA peuvent poser des difficultés pour satisfaire aux critères requis de vérifiabilité et d'objectivité. Les méthodes de police prédictive ne doivent pas conduire à des décisions illégales de privation de liberté. Ces opérations menées par les autorités publiques doivent donc être légales, nécessaires et proportionnées aux objectifs poursuivis et se fonder sur un droit interne clair, prévisible et accessible, poursuivant un but légitime tout en assurant des garanties adéquates.

Vie privée et protection des données ; liberté d'expression et liberté de réunion et d'association

134. L'utilisation de systèmes d'IA dans le cadre de l'application de la loi peut avoir une incidence sur les articles 8 (droit au respect de la vie privée et familiale), 10 (liberté d'expression) et 11 (liberté de réunion et d'association) de la CEDH.

135. Le simple fait de stocker des données relatives à la vie privée d'une personne constitue une ingérence au sens de l'article 8[244] et le besoin de garanties sera d'autant plus grand en ce qui concerne la protection des données à caractère personnel faisant l'objet d'un traitement automatisé[245]. Le fait que le matériel stocké soit sous forme codée, intelligible uniquement à l'aide de l'informatique et ne pouvant être interprété que par un nombre limité de personnes, n'a aucune incidence sur cette constatation[246]. Une mesure de surveillance implique généralement une ingérence dans la vie privée[247].

136. Toute ingérence dans la vie privée d'un individu ne peut être justifiée au regard de l'article 8 § 2 que si elle est prévue par la loi, poursuit un ou plusieurs buts légitimes (tels que la sécurité nationale, la sûreté publique ou la défense de l'ordre et la prévention du crime) et est nécessaire, dans une société démocratique, pour atteindre l'un de ces buts[248]. L'exigence « conformément à la loi » de l'article 8 § 2 requiert, en général, que la mesure contestée ait une certaine base en droit interne[249]. Quant à la qualité de la loi en question, elle doit être compatible avec la prééminence du droit, claire et accessible à la personne concernée, qui doit, en outre, être en mesure de prévoir ses conséquences pour elle[250]. Dans le contexte particulier des mesures secrètes de surveillance, telles que l'interception des communications, la « prévisibilité » signifie que le droit interne doit être suffisamment clair pour donner aux citoyens une indication adéquate des circonstances et des conditions dans

[243] *Akgün c. Turquie*, No. 19699/18, 20 juillet 2021, §§ 156 et 175.
[244] *Leander c. Suède*, No. 9248/81, 26 mars 1987, § 48.
[245] *S. et Marper*, § 103.
[246] *S. et Marper*, §§ 67 et 75.
[247] *Amann c. Suisse* [GC], No. 27798/95, §§ 69-70, CEDH 2000-II ; *Leander c. Suède*, No. 9248/81, 26 mars 1987, série A No. 116 ; *Kopp c. Suisse*, 25 mars 1998 ; *Rotaru c. Roumanie* [GC], No. 28341/95, §§ 43-44, CEDH 2000-V ; *McGinley et Egan c. Royaume-Uni*, 9 juin 1998, § 101.
[248] *Roman Zakharov c. Russie* [GC], No. 47143/06, 4 décembre 2015, § 227 ; voir aussi *Kennedy c. Royaume-Uni*, No. 26839/05, 18 mai 2010, § 130.
[249] *Vavřička et autres c. République tchèque* [GC], nos 47621/13 et 5 autres, 8 avril 2021, §266 avec une référence supplémentaire.
[250] *Plechlo c. Slovaquie*, No. 25132/13, 18 avril 2017, § 43 ; voir aussi *Big Brother Watch et autres c. Royaume-Uni* [GC], Nos. 58170/13, 62322/14 et 24960/15, 25 mai 2021, § 332 ; *Roman Zakharov c. Russie* [GC], No. 47143/06, 4 décembre 2015, § 228 ; voir aussi, parmi de nombreuses autres autorités, *Rotaru c. Roumanie* [GC], No. 28341/95, § 52, CEDH 2000-V ; *S. et Marper c. Royaume-Uni* [GC], Nos. 30562/04 et 30566/04, 4 décembre 2008, § 95 ; *Kennedy c. Royaume-Uni*, no 26839/05, 18 mai 2010, § 151.

lesquelles les autorités publiques sont habilitées à recourir à de telles mesures[251]. La Convention 108(+) autorise également des exceptions aux dispositions relatives à la protection des données à caractère personnel pour des raisons de sécurité nationale, de sûreté publique et d'enquête sur des infractions pénales ; elle exige toutefois des États parties qu'ils mettent en place des garanties et des limitations pour s'assurer que toute exception reste nécessaire et proportionnée[252]. En outre, les activités de traitement à des fins de sécurité nationale doivent faire l'objet d'un examen et d'un contrôle indépendants et efficaces dans le cadre de la législation nationale de la partie concernée[253].

137. Les pouvoirs de surveillance secrète des citoyens ne sont tolérables au regard de la CEDH que dans la mesure où ils sont strictement nécessaires à la sauvegarde des institutions démocratiques[254]. Une telle ingérence dans le cadre de l'article 8 doit être étayée par des raisons pertinentes et suffisantes et doit être proportionnée au but légitime poursuivi[255]. Pour ce qui est de savoir si une ingérence était « nécessaire dans une société démocratique » à la poursuite d'un but légitime, les autorités nationales jouissent d'une large marge d'appréciation pour choisir la meilleure manière d'atteindre les buts légitimes que sont, entre autres, la protection de la sécurité nationale[256]. Toutefois, « compte tenu du risque qu'un système de surveillance secrète visant à protéger la sécurité nationale porte atteinte à la démocratie, voire la détruise, sous couvert de la défendre », des garanties adéquates et effectives contre les abus sont nécessaires[257]. Des facteurs tels que « la nature, la portée et la durée des mesures possibles, les motifs requis pour les ordonner, les autorités compétentes pour les autoriser, les exécuter et les contrôler, ainsi que le type de recours prévu par le droit national » sont pertinents pour déterminer la conformité avec la CEDH[258].

138. Six garanties minimales sont requises pour éviter les abus lorsque des communications sont interceptées dans le cadre d'enquêtes pénales : la nature de l'infraction justifiant l'interception, les catégories de personnes concernées, les délais, les procédures de traitement des données, les garanties pour le partage des données et les conditions d'effacement[259]. Ces garanties s'appliquent également à la surveillance de la sécurité nationale, avec des exigences supplémentaires comprenant (i) des dispositions pour superviser la mise en œuvre des mesures de surveillance secrète, (ii) des mécanismes de notification et (iii) les recours prévus par le droit national[260]. Dans un domaine où les abus dans des cas individuels sont potentiellement si faciles et peuvent avoir des conséquences si néfastes pour la société démocratique dans son ensemble, il est en principe souhaitable de confier le contrôle de surveillance à un juge, le contrôle judiciaire offrant les meilleures garanties d'indépendance, d'impartialité et de régularité de la procédure[261]. Toutefois, la surveillance par des organes non judiciaires peut également être considérée comme conforme à la CEDH si l'organe de surveillance est indépendant des autorités chargées de la surveillance et est doté de pouvoirs suffisants pour exercer un contrôle effectif et continu[262]. Dans l'affaire *Szabó et Vissy c. Hongrie*, l'autorisation et la supervision des mesures de surveillance secrète par le ministre de la Justice (sans autorisation judiciaire préalable) étaient intrinsèquement incapables de garantir

---

[251] *Big Brother Watch et autres c. Royaume-Uni* [GC], Nos 58170/13, 62322/14 et 24960/15, 25 mai 2021, § 333 ; *Leander c. Suède*, no 9248/81, 26 mars 1987, § 51.
[252] Article 11, paragraphe 1, point a), et paragraphe 3.
[253] Ibid.
[254] *Rotaru c. Roumanie* [GC], No. 28341/95, 4 mai 2000, § 47 ; Szabó et Vissy c. Hongrie, No. 37138/14, 12 janvier 2016, § 54 avec d'autres références.
[255] *Segerstedt-Wiberg et autres c. Suède*, No. 62332/00, 6 juin 2006, § 88.
[256] Ibid ; *Škoberne c. Slovénie*, No. 1310/10, 12 décembre 2017, § 124.
[257] *Plechlo c. Slovaquie*, No. 25132/13, 18 avril 2017, § 43.
[258] *Škoberne c. Slovénie*, No. 1310/10, 12 décembre 2017, § 124 ; voir aussi *Roman Zakharov c. Russie* [GC], No. 47143/06, 4 décembre 2015, § 232 ; *İrfan Güzel c. T*urquie, No. 35285/08, 7 février 2017, § 85 ; E*kimdzhiev et autres c. B*ulgarie, No.. 70078/12, 11 janvier 2022, §§ 418-419 ; voir aussi *Big Brother Watch et autres c. Royaume-Uni* [GC], Nos 58170/13, 62322/14 et 24960/15, 25 mai 2021 ; *Centrum för rättvisa c. Suède* [GC], no 35252/08, 25 mai 2021 ; *Podchasov c. Russie*, No. 33618/19, 2024, § 64.
[259] *Big Brother Watch et autres*, § 335.
[260] *Roman Zakharov c.* Russie [GC], No. 47143/06, 4 décembre 2015, § 238.
[261] *Big Brother Watch et autres*, § 336.
[262] *Roman Zakharov c. Russie* [GC], No. 47143/06, 4 décembre 2015, § 275.

l'évaluation requise de la stricte nécessité[263]. En outre, lorsqu'un juge ou un tribunal chargé du contrôle adopte une attitude passive et se contente d'approuver, sans véritablement vérifier les faits, les actions des services de sécurité, ce contrôle n'est pas compatible avec l'article 8[264].

139. Si la Convention n'interdit pas le recours à l'interception de masse pour protéger la sécurité nationale et d'autres intérêts nationaux essentiels contre des menaces extérieures graves, la marge d'appréciation accordée aux États doit être plus étroite[265]. Pour les interceptions de masse, un ensemble de critères plus large que les six exigences (voir paragraphe [x] ci-dessus) s'applique pour déterminer si l'État a agi dans le cadre de sa marge d'appréciation.[266]

140. Des violations de l'article 8 relatives à la surveillance secrète ont été identifiées dans des affaires impliquant des militants des droits humains[267], des membres d'organisations non gouvernementales,[268] des avocats,[269] des journalistes[270]. En ce qui concerne les journalistes, les mesures de surveillance ciblée visant à découvrir leurs sources journalistiques peuvent également porter atteinte à leur droit à la liberté d'expression (article 10 de la CEDH), en l'absence de garanties adéquates dans la loi ou d'une exigence impérieuse d'intérêt public justifiant de telles mesures dans le cas concret. Le droit des journalistes de protéger leurs sources fait partie de la liberté de « recevoir et de communiquer des informations et des idées sans ingérence d'autorités publiques » protégée par l'article 10 et constitue l'une de ses garanties importantes.

141. En ce qui concerne la collecte de données personnelles (biométriques) au moyen de la technologie de reconnaissance faciale, des mesures de sécurité minimales concernant la durée, le stockage, l'utilisation et la destruction des données personnelles sont nécessaires pour assurer des garanties appropriées. Si la nécessité d'utiliser les technologies modernes dans le cadre des efforts déployés par les États pour lutter contre la criminalité, et en particulier contre la criminalité organisée et le terrorisme, est incontestable[271] dans l'affaire *Glukhin c. Russie*, l'utilisation par les autorités de la technologie de reconnaissance faciale pour enquêter sur le requérant a violé son droit au respect de la vie privée (article 8) et à la liberté d'expression (article 10). Bien que les mesures policières soient fondées sur le droit national, il n'existe pas de garanties adéquates et effectives contre les abus. En outre, les données à caractère personnel traitées contenaient des informations sur la participation du requérant à une manifestation pacifique et révélaient donc ses opinions politiques. Les données à caractère personnel révélant des opinions politiques entrent dans la catégorie particulière des données sensibles bénéficiant d'un niveau de protection accru[272]. Dans le cadre de la mise en œuvre de la technologie de reconnaissance faciale, il est essentiel de disposer de règles détaillées régissant la portée et l'application des mesures, ainsi que de solides garanties contre le risque d'abus et d'arbitraire. Le besoin de garanties est d'autant plus grand lorsque la technologie de reconnaissance faciale est utilisée en direct[273]. Outre les préoccupations liées à l'article 8, l'utilisation d'une technologie de reconnaissance faciale très intrusive pour identifier et arrêter

---

[263] *Szabó et Vissy c. Hongrie*, No. 37138/14, 12 janvier 2016
[264] *Zoltán Varga et 2 autres c. Slovaquie*, No. 58361/12, 20 juillet 2021, §§ 155-163.
[265] Ibid, § 347.
[266] En examinant le respect des principes de légalité et de nécessité, la Cour vérifie si le cadre juridique national définit clairement : (1) les motifs d'autorisation ; (2) les circonstances de l'interception individuelle ; (3) les procédures d'autorisation ; (4) la sélection, l'examen et l'utilisation du matériel d'interception ; (5) les garanties relatives au partage des données ; (6) les limites à la durée de l'interception, au stockage des données et à l'effacement ; (7) les mécanismes de contrôle indépendants et les pouvoirs d'exécution ; et (8) les procédures de contrôle *a posteriori* et les voies de recours en cas de non-respect des règles. Voir *Big Brother Watch et autres*, § 336.
[267] *Shimovolos c. Russie*, No. 30194/09, 21 juin 2011.
[268] *Association "21 décembre 1989" et autres c. Roumanie*, No. 33810/07, 24 mai 2011.
[269] *Vasil Vasilev c. Bulgarie*, No. 7610/15, 16 novembre 2021.
[270] *Azer Ahmadov c. Azerbaïdjan*, No. 3409/10, 22 juillet 2021.
[271] *Glukhin c. Russie*, No. 12317/16, 4 juillet 2023, § 85.
[272] Ibid, § 76 et 86.
[273] Ibid, § 82.

les participants à des actions de protestation pacifiques pourrait avoir un effet dissuasif sur les droits à la liberté d'expression (article 10 de la CEDH) et à la liberté de réunion (article 11 de la CEDH)[274].

142. Les lignes directrices sur la reconnaissance faciale du Conseil de l'Europe[275] fournissent un ensemble de mesures de référence que les gouvernements, les développeurs de reconnaissance faciale, les fabricants, les fournisseurs de services et les entités utilisant des technologies de reconnaissance faciale devraient suivre et appliquer pour s'assurer qu'elles ne portent pas atteinte aux droits humains. Il souligne que l'utilisation de la reconnaissance faciale doit avoir une base légale, conformément à l'article 6 de la Convention 108+. Des garanties spéciales devraient être établies dans le droit national, afin de s'assurer que toute utilisation est proportionnée à l'objectif légitime poursuivi. La nécessité et la proportionnalité de la reconnaissance faciale doivent être soigneusement évaluées et un cadre juridique doit définir ses différentes applications. Cela inclut des critères tels que le but de l'utilisation, la fiabilité de l'algorithme, la conservation des données, l'auditabilité, la traçabilité et les garanties. L'utilisation de la reconnaissance faciale pour déterminer des attributs tels que la couleur de la peau, la religion, le sexe, l'appartenance ethnique ou la santé devrait être interdite, à moins que des garanties juridiques appropriées n'existent pour prévenir la discrimination. Des règles spécifiques devraient être établies pour l'utilisation par les forces de l'ordre, limitant le traitement des données biométriques dans des environnements contrôlés et non contrôlés à des fins strictement nécessaires et proportionnées.

143. Les technologies de surveillance pilotées par des systèmes d'IA, y compris la surveillance biométrique et le suivi du comportement, peuvent également être utilisées pour renforcer la sécurité des prisons. Placer une personne sous surveillance vidéo permanente en prison - ce qui implique déjà une limitation considérable de la vie privée - doit être considéré comme une ingérence grave dans le droit au respect de la vie privée, en tant qu'élément de la notion de « vie privée » (article 8 de la CEDH)[276]. La Recommandation CM/Rec(2024)5 relative aux aspects éthiques et organisationnels de l'utilisation de l'intelligence artificielle et des technologies numériques associées par les services pénitentiaires et de probation souligne que l'utilisation de ces systèmes pour maintenir la sûreté, la sécurité et le bon ordre doit être strictement nécessaire, proportionnée à l'objectif poursuivi et éviter tout effet négatif sur la vie privée et le bien-être des délinquants et du personnel. L'utilisation de systèmes d'intelligence artificielle dans le cadre de la surveillance doit être proportionnée à l'objectif poursuivi et n'être utilisée qu'en cas de stricte nécessité. L'approche centrée sur l'être humain doit rester un élément clé de la prise de décision en matière de gestion des délinquants, d'évaluation des risques, de réadaptation et de réinsertion. L'utilisation des systèmes d'IA ne doit en aucun cas causer des dommages ou des souffrances physiques ou mentales intentionnels à une personne.

144. Les technologies de surveillance basées sur les systèmes d'IA, notamment la reconnaissance faciale et l'identification biométrique à distance, posent de nouveaux défis en matière de protection des droits humains. Ces technologies augmentent considérablement la portée, la vitesse et l'échelle de la surveillance, y compris les interceptions en masse, ce qui accroît les risques, par exemple, de collecte massive de données, d'atteintes graves à la vie privée ou de profilage. Dans le même temps, les systèmes d'IA peuvent être opaques, biaisés ou sujets à des erreurs. C'est pourquoi le respect des articles 8, 10 et 11 peut nécessiter, au-delà des garanties traditionnelles, des mesures supplémentaires adaptées aux questions de partialité algorithmique, de transparence, d'explicabilité et d'interprétabilité, et de responsabilité. La surveillance fondée sur des systèmes d'IA devrait être fondée sur une législation accessible et prévisible, poursuivre un but légitime et inclure un contrôle solide, y compris une protection judiciaire le cas échéant, afin de protéger le droit au respect de la vie privée (article 8), la liberté d'expression (article 10) et la liberté de réunion et d'association (article 11). Les technologies de reconnaissance faciale, en particulier les systèmes en temps réel, nécessitent des garanties renforcées contre les abus et les effets dissuasifs sur la liberté d'expression et de réunion. Les États membres devraient prévoir des règles claires, un contrôle indépendant et des voies de recours efficaces pour empêcher les pratiques de

[274] Ibid, § 88.
[275] Adoptée par le Comité consultatif de la Convention 108 en 2021.
[276] *Vasilică Mocanu c. Roumanie*, No. 43545/13, 6 décembre 2016, § 36.

surveillance arbitraires ou illégales qui risquent de violer les droits humains et les principes de la dignité humaine et de l'autonomie personnelle. Le cas échéant, cela devrait inclure des interdictions explicites de l'utilisation de systèmes d'intelligence artificielle pour des mesures de surveillance[277].

Non-discrimination et égalité

145. L'application des systèmes d'IA au maintien de l'ordre et à la sécurité publique soulève également des inquiétudes quant aux biais algorithmiques conduisant à des discriminations (article 14). Par exemple, les systèmes de reconnaissance faciale se sont avérés biaisés dans plusieurs cas, entraînant l'identification erronée de suspects et, dans certains cas, l'incarcération injustifiée de personnes innocentes[278]. Les États devraient faire preuve de prudence en ce qui concerne l'identification, l'évaluation, la prévention et l'atténuation des risques de discrimination découlant de l'utilisation, par exemple, des technologies de reconnaissance faciale ou des systèmes d'identification biométrique à distance dans les secteurs du maintien de l'ordre et de la sécurité. Les États peuvent évaluer si de nouvelles réglementations sont nécessaires ou si des mesures spécifiques, y compris des interdictions explicites, doivent être mises en œuvre pour prévenir la discrimination[279].

146. Dans le contexte des services pénitentiaires et de probation, la Recommandation CM/Rec(2024)5 souligne que des garanties doivent être mises en place pour prévenir la discrimination, assurer l'équité procédurale et défendre la dignité humaine, afin que la gestion des prisons par l'IA reste compatible avec les droits fondamentaux et l'État de droit. Lors du développement de l'IA et des technologies numériques connexes en vue d'accroître la précision et l'objectivité de l'évaluation des risques, il convient de relever les défis des biais algorithmiques ainsi que de la qualité et de la représentativité des données. La sensibilité à toutes les formes de diversité, y compris à la perspective de genre et au multiculturalisme, devrait inspirer la conception et l'utilisation des outils d'évaluation des risques afin d'éviter toute discrimination. Lorsque ces outils sont utilisés pour personnaliser les plans de traitement et de réinsertion, il convient de veiller à éviter les préjugés. L'utilisation de ces outils ne devrait pas remplacer les contacts humains réguliers entre les professionnels et les délinquants, y compris, le cas échéant, le travail avec leurs familles et leurs enfants.

Droit à un recours effectif

147. L'application de systèmes d'intelligence artificielle au maintien de l'ordre et à la sécurité publique soulève des préoccupations quant au droit à un recours effectif (article 13) [HYPERLIEN].

Pour en savoir plus

- Rapport de l'APCE | Doc. 15156 | 01 octobre 2020, La justice par algorithme - le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale
- La Convention européenne des droits de l'homme et la police (2015) (en anglais uniquement)
- Fiche d'information de la CEDH - Surveillance de masse
- Fiche d'information sur la CEDH - Protection des données à caractère personnel
- Fiche d'information sur la CEDH - Nouvelles technologies
- CEDH, Guide sur la jurisprudence dans le terrorisme
- Sécurité nationale et jurisprudence européenne, Rapport préparé par la Division des recherches de la Cour, 2013
- Recommandation CM/Rec(2021)8 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

[277] Loi européenne sur l'IA, préambule (33).
[278] Étude CDADI/GEC (2023), pp. 22-23. D'autres exemples figurent dans la « Justice par algorithme - Le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale », paragraphe 7.
[279] Voir également la loi européenne sur l'IA, préambule (33).

- EUROPOL (2023) Report, AI and policing: The benefits and challenges of artificial intelligence for law enforcement (en anglais uniquement)
- European Parliament Study (2020) “Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights” (en anglais uniquement)
- Résolution du Conseil des droits de l'homme des Nations unies sur la liberté d'opinion et d'expression, UN Doc A/HRC/RES/50/15 (8 juillet 2022)
- Résolution du Conseil des droits de l'homme des Nations unies sur la promotion, la protection et la jouissance des droits de l'homme sur l'internet, UN Doc A/HRC/RES/47/16 (7 juillet 2021)

3.3.5 Immigration et contrôle des frontières

148. Ce secteur comprend les activités liées au contrôle des frontières, aux conditions et modalités d'entrée et de sortie du territoire de l'État, y compris la délivrance de visas, l'expulsion et la reconduite à la frontière, l'asile et le statut de réfugié et l'adaptation du statut, les services de traduction/interprétation, la production de transcriptions, la collecte et l'évaluation des preuves.

Principaux cas d'utilisation de l'IA

149. L'IA est de plus en plus utilisée à tous les stades du contrôle de l'immigration et des frontières, avec un déploiement plus important dans les phases de pré-départ et d'arrivée, tandis que son rôle dans la phase de retour reste limité en comparaison.

- *Systèmes d'identification et de vérification* : Contrôles d'identité assistés par l'IA et utilisant la biométrie (par exemple, identification automatisée des empreintes digitales, balayage de l'iris, reconnaissance faciale), y compris l'identification des demandeurs d'asile sans preuve documentaire de leur identité.
- *Analyse prédictive et systèmes d'évaluation des risques* : outils de prévision et d'alerte précoce dans le contexte du contrôle de l'immigration et des frontières.
- *Systèmes de surveillance alimentés par l'IA* : camps de réfugiés, installations d'hébergement de migrants et surveillance et contrôle des frontières à l'aide de caméras alimentées par l'IA, de la reconnaissance faciale et de drones alimentés par l'IA ; évaluations des risques assistées par l'IA.
- *Prise de décision et automatisation assistées par l'IA* : Vérification et traitement des demandes d'asile assistés par l'IA (par exemple, reconnaissance faciale, vocale et dialectale, translittération des noms et analyse des données des téléphones portables) ; IA générative pour aider les agents chargés des dossiers à synthétiser et à analyser de grandes quantités de documents ; systèmes d'IA qui fournissent des informations sur les formalités d'immigration à accomplir et sur les conditions de vie et de travail auxquelles les demandeurs peuvent s'attendre dans le pays de destination.

Droits humains et principes pertinents[280]

150. La CEDH ne garantit pas le droit d'entrer, de s'installer ou de résider dans un pays spécifique[281]. Toutefois, les non-nationaux se trouvant sur le territoire ou soumis à la juridiction extraterritoriale d'un État partie bénéficieront de la protection de la CEDH. Les États ont le droit de contrôler l'entrée des non-ressortissants sur leur territoire[282]. En exerçant le contrôle de leurs frontières, les États membres doivent agir en conformité avec les normes de la CEDH. La jurisprudence n'impose que certaines limites au droit des États de refouler une personne à leurs frontières, par exemple lorsque cela équivaudrait à un *refoulement*[283].

151. La CSE n'accorde pas non plus aux ressortissants étrangers un droit d'entrée ou une liberté de circulation sur les territoires des autres parties. Le CSER a affirmé que les protections de la CSE peuvent être étendues aux

[280] Outre la CEDH et la CSE, le Conseil de l'Europe a adopté d'autres instruments juridiques relatifs à l'immigration. Voir https://www.coe.int/fr/web/migration-and-refugees/council-of-europe-reference-documents-and-resources1

[281] *Jeunesse c. Pays-Bas*, No. 12738/10, 3 octobre 2014, § 103 ; *Maslov c. Autriche* [GC], No. 1638/03, § 68, CEDH 2008 ; *Üner c. Pays-Bas* [GC], No. 46410/99, § 54, CEDH 2006-XII ; *Boujlifa c. France*, No. 25404/94, 21 octobre 1997, § 42, Recueil 1997-VI ; *Abdulaziz, Cabales et Balkandali c. Royaume-Uni*, No. 9214/80, § 9473/8, CEDH 2006-XII. *France*, no 25404/94, 21 octobre 1997, § 42, Recueil 1997-VI ; *Abdulaziz, Cabales et Balkandali c. Royaume-Uni*, nos 9214/80, 9473/81 et 9474/81, 28 mai 1985, § 67, série A no 94.

[282] *Abdulaziz, Cabales et Balkandali c. Royaume-Uni*, App No. 9214/80, 9473/81, 9474/81, 28 mai 1985, § 67.

[283] *F.G. c. Suède* [GC], no. 43611/11, 23 mars 2016, § 117.

ressortissants étrangers d'États non parties[284], dans la mesure où les parties ont déjà garanti des droits identiques ou indissociables en vertu des traités relatifs aux droits humains, en particulier la CEDH. Toutefois, elle a noté que de telles obligations ne relèvent généralement pas de ses fonctions de contrôle. La CSE oblige les États parties à adopter des politiques d'immigration flexibles, à assouplir les réglementations en matière d'emploi[285] et à faciliter le regroupement familial[286].

152. L'utilisation de systèmes d'IA pour le contrôle de l'immigration et des frontières peut soulever des questions au regard de l'article 8 (respect de la vie privée et familiale), de l'article 14 (non-discrimination) et de l'article 13 (recours effectif) de la Convention européenne des droits de l'homme.

Droit à la vie privée et à la protection des données

153. Les États membres sont tenus de respecter les droits prévus à l'article 8 pour les non-ressortissants qui se trouvent dans la juridiction de l'État. Bien que la protection offerte par l'article 8 ne soit pas absolue, toute restriction doit reposer sur une base juridique claire assortie de garanties appropriées ; elle doit être nécessaire et proportionnée à un objectif légitime et ne doit pas être discriminatoire. Si la surveillance peut être nécessaire pour garantir la sécurité nationale et d'autres objectifs légitimes, les mesures ne doivent pas porter atteinte de manière disproportionnée aux droits individuels[287]. La Convention 108(+) autorise également des exceptions, par exemple pour la sécurité nationale et la sécurité publique, mais exige des garanties strictes pour s'assurer que toutes les exceptions restent nécessaires et proportionnées et sont soumises à un examen et à un contrôle indépendants et efficaces dans le cadre de la législation nationale de la partie concernée[288].

154. L'utilisation de systèmes d'IA pour la gestion des frontières, tels que les drones équipés d'IA, la reconnaissance faciale et l'analyse prédictive utilisant des données personnelles, pourrait entraîner une surveillance excessive des personnes grâce à la technologie[289]. La protection de l'article 8 s'étend aux données à caractère personnel, y compris les données électroniques[290] et les données biométriques[291]. La conservation générale et indiscriminée des données biométriques a été jugée incompatible avec le droit au respect de la vie privée[292]. Les données biométriques sont considérées comme des données sensibles[293] et peuvent révéler des caractéristiques personnelles supplémentaires, telles que l'origine ethnique, l'état de santé ou le handicap. Par conséquent, une protection spéciale est nécessaire pour éviter toute utilisation abusive susceptible d'entraîner une discrimination. Les systèmes d'identification et de vérification basés sur les empreintes digitales, les scans

[284] Conclusions 2004, Déclaration d'interprétation.
[285] CSE, article 18§1-3.
[286] CSE, article 19, paragraphe 6.
[287] *Glukhin c. Russie*, § 90 ; CDH, Rapport "Impact des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris les manifestations pacifiques" (2020) Doc ONU A/HRC/44/24 ; AGNU n(11) para 1.
[288] Ibid.
[289] CDH, Rapport "Impact de l'utilisation de services militaires et de sécurité privés dans la gestion de l'immigration et des frontières sur la protection des droits de tous les migrants" (2020) UN Doc A/HRC/45/9 ; AGNU, Rapport "Formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée" (2020) UN Doc A/75/590 ;
[290] *S. et Marper c. Royaume-Uni* App. No. 30562/04 et 30566/04 (Cour européenne des droits de l'homme, 4 décembre 2008)
[291] Voir entre autres *Van der Velden c. Pays-Bas* (déc.), No. 29514/05, 7 décembre 2006 ; *Schmidt c. Allemagne* (déc.), No. 32352/02, 5 janvier 2006 ; *S. et Marper c. Royaume-Uni* [GC], Nos. 30562/04 et 30566/04, 4 décembre 2008 ; *Canonne c. France* (déc.), No. 22037/13, 2 juin 2015 ; *Gaughran c. Royaume-Uni*, No. 45245/15, 13 février 2020 ; *Dragan Petrović c. Serbie*, No. 75229/10, 14 avril 2020 ; *McVeigh, O'Neill et Evans c. Royaume-Uni*, Nos. 8022/77, 8025/77 et 8027/77, décision de la Commission du 18 mars 1981 ; *Allan c. Royaume-Uni*, No. 48539/99, 5 novembre 2002 ; *Doerga c. Pays-Bas*, No. 50210/99, 27 avril 2004 ; *Vetter c. France*, No. 59842/00, 31 mai 2005 ; *Wisse c. France*, No. 71611/01, 20 décembre 2005.
[292] *S. et Marper contre le Royaume-Uni*, § 125.
[293] Convention 108+, article 8.

de l'iris et la reconnaissance faciale présentent des risques, en particulier lorsque les données biométriques sont collectées, stockées ou utilisées sans garanties suffisantes.

155. Les systèmes d'IA peuvent générer des erreurs, en particulier lors du contrôle des données relatives aux voyageurs ordinaires à des fins de sécurité, par exemple pour détecter des terroristes ou des criminels présumés. Ces systèmes traitent de vastes ensembles de données provenant de sources multiples (police, services de renseignement, autorités frontalières), souvent à l'insu des personnes concernées[294] et comprennent souvent des bases de données interopérables qui partagent les empreintes digitales et les données biométriques entre les services de police et de contrôle des frontières. Dans de telles circonstances, le contrôle et la possibilité de contester l'inclusion injustifiée sur et de demander une rectification pourraient être entravés. L'inscription injustifiée sur les listes de surveillance du terrorisme a de graves répercussions sur les droits humains de la personne concernée.[295] Selon les mesures spécifiques déclenchées par un signalement provenant d'une liste de surveillance (par exemple, interdiction de voyager, refus d'entrée ou de séjour, interrogatoire, surveillance ou même arrestation), cela peut avoir une incidence sur un large éventail de droits, notamment la liberté de circulation, le respect de la vie privée, le droit à la liberté et le droit à un procès équitable. Elle peut également avoir une incidence directe ou indirecte sur toute une série de droits civils, politiques, économiques, sociaux et culturels des membres de la famille, y compris les enfants, et des associés des personnes inscrites sur la liste. Afin d'éviter l'identification erronée de voyageurs comme suspects ou comme personnes représentant une menace liée au terrorisme, la pertinence des résultats individuels des évaluations automatiques devrait être soigneusement examinée par une personne de manière non automatisée[296]. Les agents qui procèdent à cet examen devraient être correctement formés et sensibilisés aux risques de partialité et aux conséquences d'une identification erronée des risques pour les personnes concernées.

156. La création et la maintenance des systèmes d'IA utilisés à de telles fins doivent être fondées sur une législation qui prévoit des garanties efficaces contre les abus[297], y compris des délais de conservation des données et une protection particulière des données sensibles telles que les informations sur les opinions politiques d'une personne[298], et la possibilité réelle de demander la suppression des données[299] et la rectification des données erronées[300].

Non-discrimination et égalité

157. Les décisions fondées sur des informations provenant de systèmes d'IA peuvent donner lieu à une discrimination illégale, y compris une discrimination indirecte et intersectionnelle, en raison des préjugés des systèmes d'IA. En outre, les technologies telles que les systèmes de reconnaissance faciale qui utilisent des données biométriques ont été décrites comme intrinsèquement faillibles, car elles reposent inévitablement sur des probabilités statistiques et sont sujettes à l'inexactitude et aux erreurs[301]. Bien que cette question ne soit pas

---

[294] 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 (en anglais uniquement)/

[295] *Nada c. Suisse* [GC], No. 10593/08, CEDH 2012.

[296] Comité consultatif de la Convention 108 du Conseil de l'Europe, "Avis sur les implications du traitement des dossiers passagers pour la protection des données", Strasbourg, 19 août 2016, p. 8.

[297] *Shimovolos c. Russie*, No. 30194/09, 21 juin 2011, concernant l'enregistrement d'un militant des droits de l'homme dans une "base de données de surveillance" qui suivait ses déplacements en train et en avion.

[298] *Catt c. Royaume-Uni*, No. 43514/15, 24 janvier 2019, concernant la collecte et la conservation de données sur un militant de longue date dans une base de données de la police sur les " extrémistes nationaux ".

[299] *Brunet c. France*, requête No. 21010/10, 18 septembre 2014.

[300] *Khelili c. Suisse*, No. 16188/07, 18 octobre 2011.

[301] Les niveaux d'inexactitude des algorithmes de reconnaissance biométrique des visages dépendent fortement du sexe, de la couleur de la peau et de l'âge. Des études ont montré que les algorithmes de reconnaissance faciale existants avaient plus de difficultés à reconnaître les visages féminins et produisaient plus de faux rejets et de fausses acceptations pour les visages féminins. Ils produisaient des résultats plus précis pour les visages clairs que pour les visages foncés et avaient le taux d'erreur le plus élevé sur les visages féminins foncés. Voir 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 octobre 2021.

exclusivement liée à la migration, les conséquences pour les droits des migrants et des réfugiés peuvent être importantes. Si des systèmes d'IA basés sur des technologies de reconnaissance faciale sont utilisés pour l'identification et la vérification de l'identité avant le départ ou à l'arrivée aux frontières, certaines personnes peuvent être plus exposées à des inexactitudes et à des erreurs d'identification en raison de leurs caractéristiques protégées. Les outils de prise de décision assistée par ordinateur qui analysent le visage, la parole, la reconnaissance dialectale, la translittération du nom ou les données du téléphone portable dans les systèmes de visa et d'autorisation de voyage pourraient révéler par inadvertance des caractéristiques protégées, augmentant ainsi le risque d'évaluations biaisées et de traitement inégal, et leur utilisation abusive pourrait conduire à un profilage discriminatoire. Si ces erreurs ne sont pas corrigées, des personnes mal identifiées peuvent se voir refuser l'entrée sur le territoire, ce qui entraîne des décisions discriminatoires susceptibles d'avoir un impact sur le droit à la liberté de circulation (article 2 du protocole n° 4). Toute mesure restreignant le droit à la liberté de circulation doit poursuivre l'un des buts légitimes[302] visés au paragraphe 3 de l'article 2 du Protocole n° 4 et établir un juste équilibre entre l'intérêt public et les droits de l'individu[303].

Droit à un recours effectif

158. La nature « boîte noire » des systèmes d'IA peut réduire la transparence, laissant les individus dans l'ignorance de la manière dont l'IA a influencé les décisions les concernant, telles que les refus de visa, les évaluations du statut de réfugié ou les mesures d'éloignement. Les biais liés à l'automatisation aggravent ces problèmes. Par exemple, l'existence d'une classification automatisée ou d'un score de risque peut affecter de manière significative les décisions des agents chargés des dossiers concernant les visas et les permis de séjour ou les demandes d'asile[304].

159. Si les décisions relatives à l'immigration et aux questions connexes, telles que l'entrée, le séjour et l'éloignement des étrangers, ne relèvent pas du champ d'application de l'article 6 de la CEDH (droit à un procès équitable) car elles ne concernent pas les « droits et obligations de caractère civil »[305], l'article 13 de la CEDH (droit à un recours effectif) s'applique à ces questions. Par exemple, la jurisprudence concernant les éloignements au titre de l'article 13, lorsqu'elle est examinée conjointement avec l'article 3 (interdiction de la torture) de la CEDH, établit que les personnes faisant l'objet d'une mesure d'éloignement doivent recevoir des informations suffisantes pour garantir un accès adéquat aux procédures pertinentes et à l'aide juridique disponible, ainsi que des informations susceptibles de les aider à étayer leurs plaintes[306]. La transparence et la responsabilité dans le contexte du contrôle de l'immigration et des frontières basé sur le système AI sont donc nécessaires pour permettre aux personnes d'exercer leur droit à un recours effectif.

Pour en savoir plus

- COE, La protection des migrants au titre de la Convention européenne des droits de l'homme et de la Charte sociale européenne (2013)

[302] Il s'agit de la sécurité nationale ou de la sûreté publique, du maintien de l'ordre public, de la prévention des infractions pénales, de la protection de la santé ou de la morale, ou de la protection des droits et libertés d'autrui.
[303] *De Tommaso c. Italie* [GC], No. 43395/09, 23 février 2017, § 104 ; *Pagerie c. France*, No. 24203/16, 12 janvier 2023, § 171 ; *Battista c. Italie*, No. 43978/09, 2 décembre 2014, § 37 ; *Khlyustov c. Russie*, No. 28975/05, 11 juillet 2013, § 64 ; *Labita c. Italie* [GC], No. 26772/95, 6 avril 2000, §§ 194-195.
[304] Voir Automatiser la prise de décision en matière de politique migratoire : navigation (en anglais uniquement)
[305] *Maaouia c. France*, No. 39652/98, 5 octobre 2000, § 40 ; *Mamatkulov et Askarov c. Turquie* [GC], Nos. 46827/99 et 46951/99, 4 février 2005, §§ 82-83 ; *M.N. et autres c. Belgique* (déc.), No. 3599/18, 5 mars 2020, § 137.
[306] *D. c. Bulgarie*, No. 29447/17, 20 juillet 2021, § 116 ; *Hirsi Jamaa et autres c. Italie* [GC], No. 27765/09, 23 février 2012, § 204 ; *M.S.S. c. Belgique et Grèce* [GC], No. 30696/09, 21 janvier 2011, §§ 304-309.

- OSCE, Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 5 octobre 2021. (en anglais uniquement)
- CEDH, Guide de la jurisprudence - Immigration
- FRA, Handbook on European law relating to asylum, borders and immigration - Edition 2020
- (en anglais uniquement)
- Parlement européen, Intelligence artificielle aux frontières de l'UE, Aperçu des applications et des questions clés (2021)
- Frontex, Artificial Intelligence-Based Capabilities for the European Border and Coast Guard, Final Report (2021) (en anglais uniquement)
- EMN-OECD Inform https://www.oecd.org/migration/mig/EMN-OECD-INFORM-FEB-2022-The-use-of-Digitalisation-and-AI-in-Migration-Management.pdf (en anglais uniquement)
- 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 (en anglais uniquement)
- Amnesty International, The Digital Border: Migration, Technology and Inequality (2023) (en anglais uniquement)

3.3.6 Travail et emploi

160. Ce secteur comprend les activités liées à l'emploi, aux ressources humaines et à la gestion du travail, y compris, mais sans s'y limiter, des questions telles que le recrutement, l'accès à l'emploi, la gestion des performances et les politiques relatives aux travailleurs.

Principaux cas d'utilisation de l'IA

161. Sur le lieu de travail, les systèmes d'IA sont utilisés pour automatiser ou faciliter les décisions des ressources humaines en matière de recrutement et d'évaluation des candidats, pour automatiser des tâches traditionnellement effectuées par des travailleurs et pour soutenir les fonctions managériales par le biais d'analyses et d'algorithmes pilotés par l'IA - ce que l'on appelle communément la « gestion algorithmique ». Il s'agit notamment de :

- *Recrutement et embauche* : L'IA est utilisée pour la création de descriptions d'emploi optimisées et leur diffusion sur les réseaux sociaux et les plateformes d'emploi, ainsi que pour la mise en relation entre les emplois et les demandeurs d'emploi, l'automatisation de la sélection des CV, la notation des candidats et les évaluations prédictives, ainsi que la conduite d'entretiens initiaux via des 'chatbots' ou des outils vidéo automatisés.
- *Automatisation des tâches et productivité* : Systèmes d'IA utilisés par les travailleurs pour automatiser les tâches de routine telles que la saisie ou la recherche de données.
- *Gestion du lieu de travail* : L'IA optimise la planification, contrôle la productivité et améliore l'automatisation des flux de travail.
- *Bien-être des employés* : Les outils alimentés par l'IA analysent le sentiment au travail, la satisfaction et l'engagement des employés, détectent les risques d'épuisement professionnel et personnalisent les programmes de soutien aux employés.
- *Gestion des performances* : Les systèmes d'IA utilisés pour suivre et analyser les performances des employés, en utilisant les données pour identifier les points forts, les faiblesses et les domaines potentiels d'amélioration.

Droits humains et principes pertinents

162. La CEDH a été interprétée à travers le droit au respect de la vie privée (article 8 de la CEDH), la non-discrimination (article 14 et protocole n° 12 de la CEDH), la liberté d'expression (article 10 de la CEDH) et la liberté d'association (article 11 de la CEDH) pour englober certains droits liés au travail et à l'emploi tels que le droit à la négociation collective[307] ou le droit de grève[308] et pour reconnaître la valeur particulière de certains droits au travail tels que la protection de la vie privée sur le lieu de travail[309] ou la santé au travail[310]. La CSE comprend un large éventail de droits du travail, tant individuels que collectifs[311].

[307] *Demir et Baykara c. Turquie*, No. 34503/97, 12 novembre 2008.
[308] *Ognevenko c. Russie*, No. 44873/09, 20 novembre 2018, § 73.
[309] *López Ribalda et autres c. Espagne* [GC], Nos. 1874/13 et 8567/13, 17 novembre 2019.
[310] *Meier c. Suisse*, No. 10109/14, 9 février 2016.
[311] Le droit de travailler, le droit à des conditions de travail justes, à des conditions de travail sûres et saines, à une rémunération équitable, à l'égalité des chances et à l'égalité de traitement en matière d'emploi et de profession sans discrimination fondée sur le sexe, le droit à la protection en cas de licenciement et à la protection des droits des travailleurs en cas d'insolvabilité de leur employeur, à la dignité au travail, le droit des travailleurs ayant des responsabilités familiales à l'égalité des chances et à l'égalité de traitement ; et le droit collectif : le droit de s'organiser et de négocier collectivement, le droit à l'information et à la consultation - également dans les procédures de licenciement collectif - et de participer à la détermination et à l'amélioration des conditions de travail et de l'environnement de travail, la protection des représentants des travailleurs dans l'entreprise et les facilités qui doivent leur être accordées.

163. L'utilisation des systèmes d'IA peut avoir des conséquences considérables sur le travail et l'emploi, couvrant de nombreuses catégories de professions (y compris celles qui ont été relativement protégées des vagues précédentes d'automatisation), d'employeurs et de travailleurs. L'utilisation de systèmes d'IA pourrait entraver l'accès au travail, augmenter l'intensité du travail, renforcer ou exacerber les déséquilibres de pouvoir entre employeurs et travailleurs, réduire l'implication humaine dans les décisions d'embauche, d'évaluation et de licenciement, et porter atteinte aux principes fondamentaux et aux droits au travail. Les défis liés à l'IA sont particulièrement présents dans les nouvelles formes d'emploi telles que les plateformes ou le « gig work », une forme de travail temporaire[312].

Droit à la vie privée et à la protection des données

164. L'article 8 protège le droit au respect de la vie privée sur le lieu de travail, ce qui englobe la confidentialité de la correspondance[313], l'utilisation du courrier électronique[314], la protection des données[315], l'accès aux données[316], la réputation professionnelle[317], et fournit des motifs de protection en cas de licenciements abusifs[318].

165. Toute ingérence dans la vie privée doit être légale, poursuivre un but légitime, être nécessaire et proportionnelle[319]. Cela s'applique à la fois à l'obligation négative de l'État de ne pas interférer avec les droits à la vie privée des employés (par exemple dans les affaires portées devant les tribunaux par des fonctionnaires) et à ses obligations positives de garantir le droit à la vie privée dans les relations entre parties privées[320]. Les États disposent d'une large marge d'appréciation pour évaluer la nécessité d'établir un cadre juridique régissant les conditions dans lesquelles un employeur peut réglementer les communications électroniques ou autres de nature non professionnelle de ses employés sur le lieu de travail[321]. Toutefois, les autorités nationales devraient veiller à ce que l'introduction par un employeur de mesures de surveillance de la correspondance et d'autres communications, quelles que soient l'étendue et la durée de ces mesures, s'accompagne de garanties adéquates et suffisantes contre les abus[322]. À la lumière des développements rapides dans ce domaine, des facteurs pertinents ont été identifiés pour la proportionnalité, ainsi que des garanties procédurales contre l'arbitraire[323]. Les autorités nationales devraient veiller à ce qu'un employé dont les communications ont été surveillées ait accès à un recours devant une instance judiciaire[324].

---

[312] Le travail via une plateforme est une forme d'emploi dans laquelle des organisations ou des individus utilisent une plateforme en ligne pour accéder à d'autres organisations ou individus afin de résoudre des problèmes spécifiques ou de fournir des services spécifiques en échange d'un paiement. L'économie des plateformes numériques (ou « gig economy ») s'est développée de manière exponentielle pendant et après la pandémie de Covid-19.

[313] ***Bărbulescu c. Roumanie*** [GC], No. 61496/08, 5 septembre 201

[314] *Copland c. Royaume-Uni*, No. 62617/00, 3 avril 2007.

[315] *Surikov c. Ukraine*, No. 42788/06, 26 janvier 2017.

[316] *Yonchev c. Bulgarie*, No. 12504/09, 7 décembre 2017.

[317] *S.W. c. Royaume-Uni*, No. 87/18, 22 juin 2021

[318] *Ülya Ebru Demirel c. Turquie*, No. 30733/08, 19 juin 2018 ; *Denisov c. Ukraine* [GC], No. 76639/11, 25 septembre 2018.

[319] *Peev c. Bulgarie*, No. 64209/01, 26 juillet 2007 ; *Radu c. Moldova*, No. 50073/07, 15 avril 2014.

[320] *Köpke c. Allemagne (déc.)*, No. 420/07, 5 octobre 2010 (irrecevable) ; ***Bărbulescu c. Roumanie*** [GC] § 118 « D'un point de vue normatif, le droit du travail ménage une marge de négociation pour les parties au contrat de travail. Ainsi, il revient en général aux parties elles-mêmes de déterminer une partie importante du contenu de leurs relations. Il ressort d'ailleurs des éléments de droit comparé dont dispose la Cour qu'il n'existe pas de consensus européen en la matière. En effet, peu d'États membres ont encadré de manière explicite la question de l'exercice par les employés de leur droit au respect de leur vie privée et de leur correspondance sur leur lieu de travail ».

[321] *Barbulescu c. Roumanie* [GC], § 119.

[322] Ibid. § 120.

[323] Ibid. § 121. Les facteurs pertinents sont les suivants (i) si l'employé a été clairement informé à l'avance de la surveillance ; (ii) l'étendue et le caractère intrusif de la surveillance ; (iii) si l'employeur avait des raisons légitimes de surveiller les communications, en particulier d'accéder à leur contenu ; (iv) s'il existait des solutions moins intrusives ; (v) les conséquences pour l'employé et la manière dont les résultats de la surveillance ont été utilisés ; et (vi) si des garanties adéquates ont été mises en place pour protéger la vie privée de l'employé.

[324] Ibid, § 122.

166. En ce qui concerne la légalité, les politiques de l'employeur peuvent constituer une protection suffisante de la vie privée en l'absence de législation nationale pertinente[325]. Pour qu'il en soit ainsi, dans les cas concernant les obligations positives de l'État en vertu de l'article 8, le droit à la vie privée de l'individu doit être effectivement protégé et correctement mis en balance avec les droits de l'employeur par les tribunaux nationaux. Il s'agit notamment des cas de licenciement d'employés pour non-respect de leurs obligations, révélés par la vidéosurveillance, de la surveillance par[326] des messages privés envoyés à partir d'un compte de messagerie d'entreprise[327], et de l'accès de l'employeur aux fichiers des employés sur un ordinateur[328].

167. Pour la CSE, le droit de travailler librement inclut la protection contre les intrusions injustifiées dans la vie privée (article 1, paragraphe 2)[329]. L'ingérence dans la vie privée peut prendre diverses formes, notamment la collecte de données par l'employeur (par le biais de la vidéosurveillance[330] ou de la vérification des courriels des employés[331]), leur stockage, leur partage et leur utilisation pour prendre des décisions en matière d'emploi. Les employés doivent être protégés contre de telles ingérences, en particulier lorsqu'elles se produisent par le biais de la communication électronique et du traitement des données[332]. Les articles 1§2 et 26 (protection contre le harcèlement) protègent globalement contre les intrusions inutiles sur le lieu de travail, mais les violations de la vie privée des salariés peuvent également enfreindre l'article 3 (santé des travailleurs, y compris santé mentale), l'article 5 (affiliation syndicale), l'article 6 (négociation collective), l'article 11 (santé mentale), l'article 20 (discrimination fondée sur le sexe) et l'article 24 (licenciement injustifié)[333]. La question de la vie privée au travail peut également être réglementée par des conventions collectives[334]. En outre, l'article 3 (droit à un lieu de travail sûr et sain) s'applique aux secteurs public et privé, tant aux salariés qu'aux indépendants[335]. En ce qui concerne l'application de ce droit, l'introduction de nouvelles technologies peut générer, accroître et déplacer des facteurs de risque pour la santé et la sécurité des travailleurs. En particulier, les nouvelles technologies, les contraintes organisationnelles et les exigences psychologiques favorisent le développement de facteurs de risque psychosociaux, conduisant au stress, à l'agression, à la violence et au harcèlement liés au travail[336]. Les États parties à la CSE (ou à la Charte sociale européenne révisée) doivent revoir la prévention des risques professionnels au niveau national et au niveau de l'entreprise, en consultation avec les partenaires sociaux (article 3, paragraphe 1)[337]. En vertu de l'article 3§2, ils devraient adopter des réglementations en matière de santé et de sécurité alignées sur les normes scientifiques et internationales,[338] en veillant à ce que les responsabilités de l'employeur et les droits et devoirs du travailleur soient clairement définis.

168. La plupart des systèmes d'IA développés ou déployés dans un contexte d'emploi traiteront les données à caractère personnel des candidats et des employés. Leur utilisation peut présenter des risques importants en matière de protection des données et de la vie privée, en particulier dans le cadre du recrutement et du suivi des travailleurs. Ces risques comprennent un manque de transparence, la non-prise en compte de la nécessité et de la proportionnalité, une surveillance humaine inadéquate, une formation insuffisante à la prise de décisions à haut

---

[325] *Wretlund c. Suède,* No. 46210/99, décision du 9 mars 2004 (irrecevable).
[326] *Köpke c. Allemagne*, No. 420/07, décision du 5 octobre 2010 (irrecevable) ; *López Ribalda et autres c. Espagne* [GC], No. 1874/13 et 8567/13, 17 octobre 2019.
[327] *Barbulescu c. Roumanie* [GC].
[328] *Libert c. France, No. 588/13, 22 février 2018.*
[329] Conclusions 2012, Déclaration d'interprétation de l'article 1§2.
[330] Conclusions 2020, Géorgie.
[331] Conclusions XXI-1, Islande.
[332] Conclusions 2012, Déclaration d'interprétation de l'article 1§2.
[333] Conclusions 2012, Déclaration d'interprétation de l'article 1§2.
[334] Conclusions 2016, Belgique.
[335] Conclusions II (1971), Déclaration d'interprétation de l'article 3 ; Conclusions 2013, Déclaration d'interprétation de l'article 3§3.
[336] Conclusions 2013, Déclaration d'interprétation sur l'article 3.
[337] Conclusions 2003, Déclaration d'interprétation sur l'article 3§1 ; voir en particulier Conclusions 2003, Bulgarie ; Déclaration sur la Covid-19 et les droits sociaux adoptée le 24 mars 2021.
[338] *Fondation Marangopoulos pour les droits de l'homme (FMDH) c. Grèce*, réclamation No. 30/2005, décision sur le bien-fondé du 6 décembre 2006, §224.

risque, l'absence de base juridique valable, la perte de contrôle individuel sur les données à caractère personnel, des difficultés à exercer les droits relatifs aux données, des garanties inadéquates ou une mauvaise sécurité des données. La collecte disproportionnée ou non autorisée de données à caractère personnel pour prendre des décisions uniquement automatisées ou assistées par l'IA sur les performances des employés, la répartition du travail ou d'autres questions liées à l'emploi, qui peuvent porter atteinte aux droits des travailleurs, constitue une préoccupation majeure. Cela est particulièrement problématique lorsque les systèmes d'IA sont utilisés à des fins de surveillance excessive du lieu de travail, de détection des émotions, de micro-gestion ou de contrôle des travailleurs à distance, ce qui peut entraîner des atteintes à la vie privée, à l'autonomie et à la dignité humaine. Les États devraient veiller à ce que les cadres juridiques régissant la protection de la vie privée sur le lieu de travail dans le contexte des systèmes d'IA protègent les employés d'une surveillance disproportionnée, d'une collecte de données intrusive et de licenciements abusifs.

Non-discrimination et égalité

169. La Cour a examiné des affaires liées au travail en vertu de l'article 14 et du protocole n° 12 de la CEDH, en rapport avec des allégations de discrimination fondée sur le sexe, la religion[339] ou l'orientation sexuelle[340], y compris des affaires d'accès au travail, de licenciement abusif ou de suspension du travail[341]. Dans le contexte de l'emploi et de la discrimination, « lorsqu'une différence de traitement est fondée sur le sexe, la marge d'appréciation accordée à l'État est étroite et, dans de telles situations, le principe de proportionnalité n'exige pas seulement que la mesure choisie soit en général adaptée à la réalisation de l'objectif poursuivi, mais il doit également être démontré qu'elle était nécessaire dans les circonstances »[342]. La promotion de l'égalité entre les hommes et les femmes est aujourd'hui un objectif majeur dans les États membres du Conseil de l'Europe et des raisons très sérieuses devraient être avancées pour qu'une telle différence de traitement puisse être considérée comme compatible avec la CEDH[343].

170. Les DESC ont pris en compte la non-discrimination et l'égalité en ce qui concerne l'accès à l'emploi (article 1§2)[344], des conditions de travail équitables (article 2), une rémunération décente (article 4), l'égalité de rémunération entre les hommes et les femmes (article 4§3)[345], l'accès à l'égalité des chances en matière d'emploi (article 20), les femmes salariées en ce qui concerne la maternité (article 8) et les travailleurs ayant des responsabilités familiales (article 27)[346]. Pour se conformer pleinement à l'article 1, paragraphe 2[347], à l'article 4, paragraphe 3[348], et à l'article 20[349], les États parties doivent mettre en œuvre des mesures juridiques garantissant l'application effective de l'interdiction de la discrimination. Les recours effectifs comprennent des procédures judiciaires et administratives pour traiter les plaintes pour discrimination, garantissant l'accès à la réintégration, à l'indemnisation et à des sanctions exécutoires, les inspections du travail jouant un rôle clé dans l'application de

339 *Thlimmenos c. Grèce* [GC], No. 34369/97, 6 avril 2000.
340 *Oleynik c. Russie*, No. 4086/18, affaire communiquée.
341 *Thlimmenos c. Grèce* [GC], No. 34369/97, 6 avril 2000 ; *Lombardi Vallauri c. Italie*, 20 octobre 2009 *; Emel Boyraz c. Turquie*, No. 61960/08, 2 décembre 2014 ; *Eweida et autres c. Royaume-Uni*, No. 48420/10, 15 janvier 2013 ; *Markin c. Russie* [GC], No. 30078/06, 22 mars 2012 ; *Saumier c. France*, No. 74734/14, 12 janvier 2017.
342 *Emel Boyraz c. Turquie,* No. 61960/08, 2 décembre 2014, § 51 (en anglais uniquement, traduction libre).
343 Ibid.
344 *Syndicat national des professions du tourisme c. France*, réclamation No. 6/1999, décision sur le fond du 10 octobre 2000, §24 ; Conclusions XVI-1 (2002), Islande.
345 Conclusions XII-5 (1997), Déclaration d'interprétation de l'article 1 du protocole additionnel.
346 Conclusions 2005, Suède ; Conclusions 2005, Estonie.
347 Conclusions XVI-1 (2003), Islande.
348 *University Women of Europe (UWE) c. Belgique*, réclamation No. 124/2016, décision sur le fond du 6 décembre 2019, §115.
349 Conclusions 2020, Albanie.

ces mesures[350]. Ces recours doivent être adéquats, proportionnés et dissuasifs pour garantir une protection efficace contre la discrimination[351].

171. Les systèmes d'IA sont de plus en plus utilisés dans les procédures de sélection pour déterminer l'accès à l'emploi[352]. Les processus de recrutement peuvent être affectés négativement par l'utilisation de systèmes d'IA, par exemple dans les cas où le recours à l'apprentissage automatique pour l'identification des candidats a abouti à des résultats discriminatoires, ou lorsque des systèmes de reconnaissance faciale et d'analyse des émotions basés sur l'IA ont donné lieu à une discrimination raciale[353]. À ce titre, les systèmes d'IA utilisés pour le recrutement et la sélection des candidats devraient être objectifs, neutres et exempts de préjugés, y compris de préjugés sexistes. Dans un contexte plus large, les États devraient veiller à ce que l'utilisation de systèmes d'IA sur le lieu de travail ne reproduise pas ou n'amplifie pas les schémas d'inégalité existants et promeuve l'égalité, y compris l'égalité entre les hommes et les femmes, la diversité et l'inclusion. En particulier, cela pourrait consister en un audit régulier des résultats de l'utilisation des systèmes d'IA dans les procédures de recrutement, de promotion et autres ; l'implication des employés et de leurs organisations représentatives dans les politiques ou les choix concernant l'utilisation de l'IA dans la prise de décision sur le lieu de travail ; le suivi de l'impact de l'introduction des systèmes d'IA dans le lieu de travail sur l'égalité des sexes et la diversité au sein de la main-d'œuvre ; et la formation et la sensibilisation de la main-d'œuvre aux préjugés sur les données, aux stéréotypes et aux risques de discrimination lors de l'utilisation des systèmes d'IA.

Transparence et responsabilité

172. L'utilisation de l'IA dans le domaine du travail et de l'emploi pose des problèmes de transparence et de responsabilité, en particulier dans le contexte de l'embauche, de la détermination des salaires[354], de la surveillance du lieu de travail et des processus décisionnels. Par exemple, en raison du problème de la boîte noire des systèmes d'IA, la fixation des salaires et l'attribution des tâches dans les plateformes et le gig work peuvent laisser les travailleurs sans explications sur les fluctuations de salaire ou la disponibilité de l'emploi. Les mécanismes de responsabilisation sont tout aussi essentiels pour éviter que l'utilisation de l'IA sur le lieu de travail ne porte atteinte aux droits du travail. Les employeurs et les décideurs politiques devraient mettre en œuvre des réglementations claires, en veillant à ce que les systèmes d'IA s'alignent sur les normes d'équité, de non-discrimination et de protection des travailleurs. Les détenteurs de droits doivent pouvoir disposer de recours efficaces.

Liberté d'expression ; liberté de réunion et d'association

173. L'article 10 de la CEDH (liberté d'expression) s'applique dans le contexte des relations de travail, y compris lorsque celles-ci sont régies par les règles du droit privé[355]. Il peut en résulter des obligations négatives et positives pour l'État. Dans la sphère privée, la responsabilité des autorités serait engagée si les faits reprochés résultaient d'un manquement de leur part à assurer aux requérants la jouissance de l'article 10 de la CEDH[356]. L'article 11 de la CEDH (liberté de réunion et d'association) protège à la fois les travailleurs et les syndicats. Un employé ou un travailleur doit être libre d'adhérer ou non à un syndicat sans être sanctionné ou découragé[357].

---

[350] Conclusions 2020, Chypre.
[351] Conclusions XVIII-I (2006), Autriche.
[352] Résolution 2343 (2020) Prévenir les discriminations résultant de l'utilisation de l'intelligence artificielle, paragraphe 1. Voir également la Recommandation CM/Rec(2020)1 sur les impacts des systèmes algorithmiques sur les droits de l'homme, paragraphe 8.
[353] Étude CDADI/GEC (2023), pp. 19-21.
[354] En vertu de l'article 4§3, les États parties doivent assurer la transparence des rémunérations et permettre les comparaisons d'emploi. Voir *University Women of Europe (UWE) c. Belgique*, réclamation No. 124/2016, décision sur le bien-fondé du 6 décembre 2019, §§115, 154 et conclusions 2020, Albanie.
[355] *Herbai c. Hongrie*, No. 11608/15, 9 juillet 2019, § 37 ; *Fuentes Bobo c. Espagne*, No. 39293/98, 29 février 2000, § 38.
[356] *Herbai c. Hongrie*, § 37.
[357] *Associated Society of Locomotive Engineers and Firemen (ASLEF) c. Royaume-Uni,* No. 11002/05, 27 février 2007, § 39.

Compte tenu du caractère sensible des questions sociales et politiques liées à la recherche d'un juste équilibre entre les intérêts respectifs des travailleurs et des employeurs, et du degré élevé de divergence entre les systèmes nationaux dans ce domaine, les États disposent d'une large marge d'appréciation quant à la manière d'assurer la liberté syndicale et la protection des intérêts professionnels des membres des syndicats[358].

174. La CSE protège la liberté d'association en tant que droit d'organisation en vertu de l'article 5, garantissant aux travailleurs le droit de former des syndicats et des organisations d'employeurs et de s'y affilier sans autorisation préalable[359]. L'article 28 de la CSE complète ces protections en sauvegardant l'indépendance des syndicats et en garantissant la protection des représentants des travailleurs[360], y compris la protection contre le licenciement ou tout traitement de représailles[361] tel que le refus d'avantages sociaux, de formation, de promotions ou les licenciements discriminatoires[362].

175. La surveillance du lieu de travail par l'IA peut avoir des conséquences négatives sur la liberté d'expression et la syndicalisation[363]. L'utilisation abusive de la surveillance basée sur les systèmes d'IA peut constituer une menace pour la liberté d'expression et la liberté d'association des employés en ayant potentiellement un effet dissuasif sur leurs droits d'avoir des opinions, de recevoir et de transmettre des informations et des idées, de s'organiser, d'organiser des réunions de travailleurs et de communiquer de manière confidentielle. La surveillance des communications, des interactions et des mouvements peut aider les employeurs à réprimer les activités syndicales en entravant les réunions ou en décourageant les employés de s'exprimer. L'absence de protection des salariés contre la discrimination exercée par l'employeur en raison de leurs activités syndicales peut avoir un effet dissuasif et décourager d'autres personnes d'adhérer à ce syndicat, ce qui pourrait conduire à sa disparition[364].

176. Pour éviter que la surveillance des lieux de travail par les systèmes d'IA n'ait un effet dissuasif, les États devraient mettre en place des garanties strictes assurant la transparence, la responsabilité et le respect des articles 10 et 11 de la CEDH et des articles 5 et 28 de la CSE. Les employeurs doivent justifier les mesures de surveillance comme étant nécessaires et proportionnées, avec des limites claires pour éviter les abus antisyndicaux.

Pour en savoir plus

- CEDH, Fiche d'information – Surveillance au travail
- CEDH, Fiche d'information – Droit en matière syndicale
- CEDH, Fiche d'information - Droits relatifs au travail
- OECD, Employment Outlook 2023, Artificial Intelligence and the Labour Market (2023) (en anglais uniquement)
- OECD, Using AI to Support People with Disability in the Labour Market: Opportunities and Challenges (2023) (en anglais uniquement)

[358] *Sindicatul "Păstorul cel Bun" c. Roumanie* [GC], No. 2330/09, 9 juillet 2013, § 133.
[359] Conclusions 2010, Géorgie ; Conclusions I (1969), Déclaration d'interprétation de l'article 5.
[360] Conclusions 2003, Bulgarie.
[361] Conclusions 2018, Fédération de Russie.
[362] Conclusions 2018, Azerbaïdjan.
[363] En avril 2022, Amazon a mis fin au développement de son application de chat interne 'Shout-Out' disponible sur les appareils IoT des employés (par exemple, smartphones, tablettes). Certains développeurs ont divulgué le modèle d'IA qui aurait surveillé les communications des employés. L'IA aurait bloqué une variété de termes en corrélation avec la critique des conditions de travail et des activités syndicales d'Amazon, tels que 'Slave labour', 'Representation', 'Union', 'Unite/Unity' et bien d'autres. Voir : https://theintercept.com/2022/04/04/amazon-union-living-wage-restrooms-chat-app/
[364] *Wilson, National Union of Journalists et autres c. Royaume-Uni*, No. 30668/96 et 2 autres, § 47, CEDH 2002-V ; *Danilenkov et autres c. Russie*, No. 67336/01, § 135, CEDH 2009 (extraits) ; et *Trade Union of the Police in the Slovak Republic et autres c. Slovaquie*, No. 11828/08, §§ 60-61, 25 septembre 2012.

- OECD, Using AI in the Workplace: Opportunities, Risks and Policy Responses (2024) (en anglais uniquement)
- ILO, Generative AI and Jobs: A global analysis of potential effects on job quantity and quality (en anglais uniquement)
- ILO, Digital transformation in employment policies (2025) (en anglais uniquement)
- ILO, The Algorithmic Management of work and its implications in different contexts (2022) (en anglais uniquement)

3.3.7 L'éducation

177. Ce secteur comprend les activités liées à l'accès à l'apprentissage, à l'évaluation des élèves, à l'orientation et à la formation professionnelles, à l'apprentissage tout au long de la vie et aux résultats de l'éducation.

Principaux cas d'utilisation de l'IA[365]

178. Dans le domaine de l'éducation, les systèmes d'IA sont utilisés pour améliorer l'apprentissage, soutenir les fonctions administratives et aider les enseignants grâce à l'analyse et à l'automatisation basées sur l'IA. Les cas d'utilisation sont les suivants :

- *Soutien à l'apprenant* : Les systèmes de tutorat pilotés par l'IA fournissent un enseignement personnalisé, les outils d'apprentissage adaptatif s'ajustent aux progrès individuels et les 'chatbots' offrent une assistance aux étudiants 24 heures sur 24 et 7 jours sur 7, y compris pour l'apprentissage tout au long de la vie.
- *Évaluation et retour d'information* : L'IA automatise l'évaluation des écrits, génère des analyses de performance en temps réel, utilise des modèles d'apprentissage ouverts pour aider les étudiants à suivre leurs progrès et aide à détecter le plagiat dans les travaux des étudiants en analysant les bases de données à la recherche de similitudes avec le contenu existant. La surveillance par l'IA évalue le comportement, l'environnement et les mouvements d'une personne qui passe un examen.
- *Administration de l'enseignement* : L'IA optimise les processus d'admission, automatise les emplois du temps et gère les systèmes d'apprentissage afin de rationaliser les opérations institutionnelles.
- *Soutien aux enseignants* : L'IA sélectionne des supports d'apprentissage à partir de sources en ligne et crée des contenus d'apprentissage adaptatifs et des manuels dynamiques. Elle fournit des analyses en temps réel en classe grâce à des tableaux de bord permettant d'analyser les données relatives aux performances, à l'assiduité, à la participation et à l'engagement des élèves, et aide à la planification des cours et à la gestion du temps.
- *Analyse de l'apprentissage et allocation des ressources* : L'IA analyse l'engagement des étudiants, prédit les résultats de l'apprentissage et informe sur la distribution des ressources afin d'améliorer l'efficacité de l'enseignement.
- *Reconnaissance de la parole et traitement du langage* **:** Les outils de reconnaissance vocale et de traitement du langage basés sur l'IA peuvent aider les étudiants handicapés en convertissant la parole en texte ou en fournissant une traduction et une transcription en temps réel.

Droits humains et principes pertinents

179. L'article 2 du protocole n° 1 de la CEDH garantit le droit à l'éducation. Le droit à l'éducation n'est pas absolu. Il existe des limitations acceptées, sachant que le droit d'accès à l'éducation « appelle, par sa nature même, une réglementation de la part de l'État »[366]. Par conséquent, les autorités nationales jouissent d'une certaine marge d'appréciation. Toutefois, les restrictions ne doivent pas porter atteinte à l'essence du droit ou le rendre ineffectif ; elles doivent être prévisibles pour les intéressés et poursuivre un but légitime[367]. Bien qu'il n'existe pas de liste exhaustive des "buts légitimes" qui peuvent être poursuivis en limitant la jouissance du droit

[365] Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022), pp.15-23 ; voir aussi UNESCO, Artificial Intelligence and Education : Guidance for Policy Makers (2021) , pp. 13-19
[366] *Affaire relative à certains aspects du régime linguistique de l'enseignement en Belgique (au principal)*, No. 1474/62, rapport de la Commission du 23 juillet 1968, § 5 de la partie « En droit » (l'affaire de « linguistique belge ») ; *Golder c. Royaume-Uni*, No. 4451/70, 21 février 1975, § 38 ; *Fayed c. Royaume-Uni*, No. 17101/90, 21 septembre 1994, § 65.
[367] *Leyla Şahin c. Turquie* [GC], No. 44774/98, 10 novembre 2005, § 154.

à l'éducation[368], toute limitation doit maintenir un équilibre proportionné entre les moyens employés et le but recherché.[369] L'État a des responsabilités concernant les écoles publiques et privées[370].

180. L'article 2 du Protocole n° 1 doit être interprété en harmonie avec les autres règles du droit international dont la CEDH fait partie,[371] y compris la Convention des Nations unies relative aux droits de l'enfant, et la CSE[372]. Les États doivent respecter et remplir les obligations et les engagements prévus par les normes existantes du Conseil de l'Europe et des Nations unies en matière de droits de l'enfant.

181. En ce qui concerne l'ESC, les États parties sont, en vertu de la partie II, article 17§2,[373] tenus - soit directement, soit en partenariat avec des organisations publiques et privées - de mettre en œuvre des mesures qui assurent un enseignement primaire et secondaire gratuit à tous les individus de moins de 18 ans (à moins que la majorité ne soit atteinte plus tôt en vertu de la loi applicable à l'enfant)[374]. L'article 17 exige des États parties qu'ils mettent en place et maintiennent un système éducatif qui soit à la fois accessible et efficace[375]. Si les acteurs privés peuvent apporter leur contribution, leur participation ne doit pas nuire à la qualité ou à l'accessibilité de l'enseignement public[376]. Les États parties doivent assurer une formation professionnelle efficace en promouvant des programmes techniques et professionnels pour tous[377]. En vertu de l'article 17, l'égalité des chances en matière d'éducation doit être garantie pour tous les enfants, en particulier pour les groupes vulnérables[378].

Droit à la vie privée et à la protection des données

182. L'utilisation de systèmes d'IA à des fins éducatives peut conduire au traitement de données à caractère personnel, par exemple, d'enfants, d'étudiants universitaires, de personnes handicapées, de personnes en formation professionnelle, d'apprenants tout au long de la vie, d'éducateurs ou de parents par divers acteurs, notamment les gouvernements nationaux, les établissements d'enseignement publics et privés, les entreprises commerciales telles que les fournisseurs de produits ou de services, les développeurs de logiciels et les particuliers tels que les enseignants, les tuteurs légaux et les camarades de classe. Le traitement des données à caractère personnel d'un enfant dans un établissement d'enseignement est particulièrement complexe en raison du cadre dans lequel il s'inscrit, ce qui peut avoir une incidence sur la nature librement consentie du consentement. En particulier, en règle générale, les enfants ne peuvent pas conclure de contrats[379]. L'utilisation de systèmes d'intelligence artificielle dans le contexte éducatif doit donc être examinée au regard de l'article 8 de la CEDH, lu en combinaison avec l'article 2 du protocole n° 1.

183. Le document CM/Rec(2018)7, qui fournit des "Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique", reconnaît que les données à caractère personnel peuvent être traitées au profit des enfants, mais souligne que les États devraient prendre des mesures pour veiller à ce que les données à caractère personnel des enfants soient traitées de manière loyale, licite, précise et sécurisée, à des fins spécifiques et avec le consentement libre, explicite, éclairé et univoque des

[368] Contrairement aux articles 8, 9, 10 et 11 de la CEDH.
[369] *Leyla Şahin c. Turquie* [GC], No. 44774/98, 10 novembre 2005, § 154 et s.
[370] *Kjeldsen, Busk Madsen et Pedersen c. Danemark*, Nos. 5095/71, 5920/72 et 5926/72, 7 décembre 1976.
[371] *Catan et autres c. République de Moldova et Russie* [GC], 2012, § 136
[372] *Timishev c. Russie*, Nos. 55762/00 et 55974/00, 13 décembre 2005, § 64 ; *Çam c. Turquie*, No. 51500/08, 23 février 2016, § 53 ; *Ponomaryovi c. Bulgarie*, No. 5335/05, 21 juin 2011, §§ 34-35.
[373] De la CSER.
[374] Sans préjudice d'autres dispositions spécifiques prévues par la CSE, notamment l'article 7. Voir l'annexe à la Charte sociale européenne (révisée) - Série des traités européens - No. 163.
[375] Conclusions 2003, Bulgarie.
[376] Conclusions 2019, Déclaration d'interprétation sur l'article 17§2 - Participation du secteur privé à l'éducation.
[377] Conclusions I (1969), Déclaration d'interprétation de l'article 10§1.
[378] *Mental Disability Advocacy Center (MDAC) c. Bulgarie*, réclamation No. 41/2007, décision sur le bien-fondé du 3 juin 2008, §34, citant les Conclusions 2003, Bulgarie.
[379] Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022), p. 71 (en anglais uniquement)

enfants et/ou de leurs parents, soignants ou représentants légaux, ou conformément à une autre base légitime prévue par la loi. Le principe de minimisation des données doit être respecté, ce qui signifie que le traitement des données à caractère personnel doit être adéquat, pertinent et non excessif au regard des finalités pour lesquelles elles sont traitées

184. Les États devraient veiller à ce que le traitement de catégories particulières de données, considérées comme sensibles, ne soit autorisé dans tous les cas que lorsque des garanties appropriées sont inscrites dans la loi. Le profilage des enfants, c'est-à-dire toute forme de traitement automatisé de données à caractère personnel consistant à appliquer un « profil » à un enfant, notamment pour prendre des décisions le concernant ou pour analyser ou prédire ses préférences personnelles, son comportement et ses attitudes, devrait être interdit par la loi. Dans des circonstances exceptionnelles, les États peuvent lever cette restriction lorsque cela est dans l'intérêt supérieur de l'enfant ou s'il existe un intérêt public supérieur, à condition que des garanties appropriées soient prévues par la loi. Les outils éducatifs basés sur des systèmes d'IA, tels que l'analyse en temps réel des salles de classe et le suivi de l'engagement des étudiants ou l'IA de contrôle qui surveille les étudiants par reconnaissance faciale et suivi comportemental, peuvent interférer avec le droit au respect de la vie privée. Les personnes ne doivent pas être soumises à des ingérences arbitraires ou illégales dans leur vie privée. Toute ingérence doit être conforme à la loi, poursuivre un objectif légitime, être nécessaire dans une société démocratique et être proportionnée à l'objectif légitime poursuivi. Les mesures de surveillance ou d'interception, en particulier, doivent respecter ces conditions et faire l'objet d'un contrôle efficace, indépendant et impartial[380].

Non-discrimination et égalité

185. L'accès à l'éducation devrait être assuré sur une base d'égalité et avec des chances égales, à tous les niveaux de l'éducation[381]. Cela devrait inclure la prise en compte des risques liés à la non-discrimination et à l'égalité pour tous les individus dans les contextes éducatifs, en veillant à ce que les systèmes d'IA dans l'éducation ne renforcent pas les préjugés qui peuvent conduire à des résultats discriminatoires ou créer des obstacles à l'accès. En raison de leur stade de développement, les enfants ont des besoins et des droits spécifiques qui les distinguent des adultes. Il est donc nécessaire de mettre en place des réglementations axées sur les enfants dans le cadre de l'acquisition et de l'utilisation des technologies éducatives, y compris les systèmes d'intelligence artificielle[382]. Dans toutes les actions concernant les enfants, qu'elles soient entreprises par des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale[383].

186. Compte tenu de l'importance croissante des nouvelles technologies, un certain nombre de documents du Conseil de l'Europe ont été adoptés dans ce domaine, qui invitent les États à veiller à ce que les enfants aient accès à l'environnement numérique d'une manière inclusive et en tenant compte du développement des capacités des enfants et de la situation particulière des enfants en situation de vulnérabilité[384]. Cela devrait également s'appliquer aux situations dans lesquelles des systèmes d'intelligence artificielle sont impliqués. S'il convient de s'efforcer de respecter, de protéger et de réaliser droits de chaque enfant dans un cadre éducatif, des mesures ciblées peuvent être nécessaires pour répondre à des besoins spécifiques, en reconnaissant que les systèmes

[380] CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique

[381] Recommandation CM/Rec(2007)17 du Comité des Ministres aux Etats membres sur les normes et mécanismes d'égalité entre les femmes et les hommes, paragraphes 24-25.

[382] Preparatory study for the development of a legal instrument on regulating the use of artificial intelligence systems in education, Revised draft (mars 2024) (en anglais uniquement), Unité de transformation numérique du département de l'éducation, Conseil de l'Europe.

[383] Convention des Nations unies relative aux droits de l'enfant (adoptée le 20 novembre 1989, entrée en vigueur le 2 septembre 1990), UNGA Res 44/25, article 3

[384] CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 4 juillet 2018.

d'IA ont le potentiel à la fois d'accroître la vulnérabilité des enfants et de les autonomiser, de les protéger et de les soutenir[385].

187. En l'absence de garanties appropriées, les systèmes d'IA peuvent être susceptibles de reproduire et d'amplifier les inégalités structurelles existantes. Dans le contexte de l'article 14 de la CEDH, les obligations positives des États pourraient inclure des mesures visant à corriger les « inégalités de fait »[386]. L'action positive, ou les mesures temporaires spéciales, peuvent comprendre des mesures visant à prévenir ou à compenser les désavantages subis par les groupes exposés à la discrimination et à l'intolérance et à faciliter leur pleine participation dans tous les domaines de la vie[387]. Les États membres devraient veiller à ce que les établissements d'enseignement utilisent les systèmes d'IA de manière inclusive[388]. Les États devraient également s'efforcer de renforcer l'utilisation des technologies de l'information et de la communication par les filles et de promouvoir l'égalité des chances et des résultats pour tous les enfants[389]. En outre, des systèmes tels que la reconnaissance faciale, utilisée dans le cadre d'un système d'IA de surveillance conçu pour contrôler le comportement des étudiants pendant les examens en ligne, peuvent présenter des préjugés et conduire à une discrimination intersectionnelle, notamment fondée sur la race et le sexe[390]. En vertu de la CEDH, toute différence de traitement doit poursuivre un but légitime et être proportionnée[391]. Il convient donc d'accorder une attention particulière à l'utilisation des systèmes d'IA dans les procédures de sélection et d'examen, afin d'éviter les résultats discriminatoires.

188. En outre, un accès limité aux systèmes et outils d'IA peut empêcher des individus ou des groupes de bénéficier des avantages qu'ils peuvent offrir, ce qui entraîne des désavantages dans divers secteurs, y compris l'éducation. La maîtrise de l'IA, qui peut être considérée comme une extension ou une spécialisation de la maîtrise du numérique, devrait être incluse dans le programme d'enseignement de base dès le plus jeune âge, en tenant compte du développement des capacités des enfants[392]. Cela comprend les compétences techniques, les compétences en matière de création de contenu et la compréhension critique des risques et des opportunités en ligne. Les efforts devraient se concentrer sur les écoles, les organisations axées sur les enfants et les parents, afin de garantir un environnement numérique sûr et inclusif. Les politiques d'éducation numérique ne doivent pas désavantager les enfants qui manquent de ressources à la maison ou qui vivent dans des institutions. Un soutien particulier doit être apporté aux enfants dont l'accès au numérique est limité ou inexistant, y compris ceux issus de milieux socio-économiques défavorisés et les enfants handicapés. Les États devraient également s'efforcer de réduire la fracture numérique et le fossé entre les sexes dans le domaine de la technologie, en garantissant l'égalité des chances pour tous les enfants, quel que soit leur milieu, et en accordant une attention particulière

[385] Lignes directrices du Conseil de l'Europe sur la protection des données des enfants dans un cadre éducatif (2020), Comité sur la Convention 108, T-PD(2019)06BISrev5, paragraphe 5.4
[386] Guide sur l'article 14 de la Convention européenne des droits de l'homme et sur l'article 1 du Protocole 12, p. 20.
[387] Voir également la Recommandation de politique générale No. 2 révisée de l'ECRI sur les organismes de de promotion de l'égalité chargées de lutter contre le racisme et l'intolérance au niveau national, paragraphe 60, et la Recommandation de politique générale No. 7 révisée de l'ECRI sur la législation nationale pour lutter contre le racisme et la discrimination raciale, paragraphe 5.
[388] Recommandation CM/Rec(2019)1 sur la prévention et la lutte contre le sexisme, en particulier II.G. « Établissements d'enseignement ».
[389] CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 4 juillet 2018, para. 46
[390] Étude CDADI/GEC (2023), p. 24.
[391] Par exemple, les modifications d'un système d'accès à l'université qui ont conduit à une différence de traitement ont emporté violation de l'article 14, combiné avec l'article 2 du Protocole No. 1, alors qu'elles visaient à améliorer rapidement la qualité de l'enseignement supérieur. L'application imprévisible du nouveau système, conjuguée à l'absence de mesures correctives, a rendu sa mise en œuvre disproportionnée par rapport à ce but - voir *Altınay c. Turquie*, No. 37222/04, 9 juillet 2013, § 60.
[392] Recommandation CM/Rec(2019)10 visant à développer et à promouvoir l'éducation à la citoyenneté numérique, 21 novembre 2019 ; Recommandation CM/Rec(2016)2 sur l'Internet des citoyens, 10 février 2016.

aux filles, en ce qui concerne l'accès aux outils numériques, y compris les systèmes d'intelligence artificielle, et les avantages qu'ils en tirent[393].

Transparence et responsabilité

189. Le manque d'explicabilité et d'interprétabilité des systèmes d'IA (le « problème de la boîte noire ») présente des risques dans le contexte de l'éducation. Si un système d'IA fait des recommandations sur le parcours d'apprentissage d'un enfant ou fournit des recommandations qui peuvent avoir des conséquences à long terme sur le développement de l'enfant, les enseignants et les parents doivent être en mesure de comprendre le raisonnement qui sous-tend ses décisions, y compris les paramètres utilisés, et avoir la possibilité de les annuler si nécessaire. De même, les systèmes d'IA utilisés pour les admissions ou les examens pourraient avoir des conséquences importantes sur les possibilités d'éducation et les perspectives d'avenir des titulaires de droits. L'opacité de l'IA peut également rendre difficile l'obtention d'un consentement véritablement éclairé ou la contestation de ses décisions et résultats[394]. Le consentement doit être donné librement sans ambiguïté et pouvoir être refusé sans préjudice[395]. Des niveaux de transparence suffisants doivent être garantis.

190. Les États membres devraient également veiller à la mise en œuvre effective des obligations qui leur incombent en vertu de l'article 13 de la CEDH, à savoir garantir aux enfants et aux autres détenteurs de droits le droit à un recours effectif lorsque leurs droits humains et leurs libertés fondamentales ont été violés par l'utilisation de systèmes d'intelligence artificielle dans le contexte éducatif.

191. Pour les enfants, cela implique la mise à disposition de moyens disponibles, connus, accessibles, abordables et adaptés aux enfants, par lesquels les enfants, ainsi que leurs parents ou représentants légaux, peuvent déposer des plaintes et demander réparation. Les recours effectifs peuvent comprendre, en fonction de la violation en question, une enquête, une explication, une réponse, une correction, une procédure, le retrait immédiat du contenu illicite, des excuses, une réintégration, une reconnexion et une indemnisation[396]. Les États devraient également veiller à ce que, dans tous les cas, l'accès aux tribunaux ou le contrôle judiciaire des recours administratifs et autres procédures soient disponibles, conformément aux principes énoncés dans les Lignes directrices du Comité des Ministres du Conseil de l'Europe sur une justice adaptée aux enfants (2010).

Entreprises et droits humains

192. Le rôle du secteur privé dans l'éducation se développe, que ce soit par le biais d'écoles privées ou de l'acquisition de systèmes d'enseignement et de gestion scolaire basés sur l'IA auprès d'entreprises privées. Les États doivent veiller à ce que les entreprises et autres partenaires clés assument leurs responsabilités en matière de droits humains et soient tenus de rendre des comptes en cas d'abus. Les entreprises ont la responsabilité de respecter les droits humains, y compris les droits de l'enfant, comme l'affirment les Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations unies et la Recommandation CM/Rec(2016)3 du Comité des ministres aux États membres sur les droits de l'homme et les entreprises[397]. En vertu de la CEDH, les États ne peuvent s'exonérer de leur responsabilité en déléguant leurs obligations à des organismes privés ou à des particuliers. Cela inclut l'enseignement dispensé par les écoles privées et leur personnel, dont les actes peuvent engager la responsabilité de l'État[398].

---

[393] CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 4 juillet 2018, §§ 41-46.
[394] Ibid, p. 52.
[395] Lignes directrices sur la protection des données personnelles des enfants dans un cadre éducatif (2020), Comité du Conseil de l'Europe sur la Convention 108, T-PD(2019)06BISrev5.
[396] CM/Rec(2018)7, § 67.
[397] Voir section VI
[398] *Costello-Roberts c. Royaume-Uni*, No. 13134/87, 25 mars 1993, § 27.

193. La Recommandation CM/Rec(2018)7 du Comité des ministres recommande aux États d'exiger des entreprises commerciales et des autres parties prenantes concernées qu'elles s'acquittent de leur responsabilité de respecter les droits de l'enfant dans l'environnement numérique et de les encourager à soutenir et à promouvoir ces droits. Les États devraient promouvoir et inciter les entreprises commerciales à mettre en œuvre la sécurité dès la conception, la protection de la vie privée dès la conception et la protection de la vie privée par défaut en tant que principes directeurs pour les caractéristiques et fonctionnalités des produits et services adressés aux enfants ou utilisés par eux.

194. Les États devraient prendre des mesures appropriées pour protéger les enfants contre les violations des droits humains commises par les entreprises dans l'environnement numérique et pour veiller à ce que les enfants aient accès à un recours effectif. Il s'agit notamment de mettre en œuvre des politiques et des mesures visant à encourager les entreprises à mettre en place leurs propres mécanismes de recours et de réclamation, conformément aux critères d'efficacité définis dans les principes directeurs des Nations unies, tout en veillant à ce que ces mécanismes n'entravent pas l'accès de l'enfant aux mécanismes judiciaires ou non judiciaires de l'État. Les États devraient également encourager les entreprises à fournir des informations accessibles, adaptées à l'âge et disponibles dans la langue de l'enfant sur la manière de déposer des plaintes et de demander réparation par le biais de mécanismes de recours et de réclamation. En outre, les entreprises commerciales devraient être tenues de mettre à disposition, sur leur plateforme ou au sein de leur service, des moyens facilement accessibles permettant à toute personne, et en particulier aux enfants, de signaler tout matériel ou activité qui les inquiète, en veillant à ce que les signalements reçus soient traités de manière efficace et dans des délais raisonnables[399]. Il devrait y avoir des moyens accessibles et efficaces de signaler les préjugés, les erreurs ou les préoccupations concernant les systèmes éducatifs pilotés par l'IA qui pourraient avoir un impact sur les titulaires de droits.

Pour en savoir plus

- CEDH, Guide sur l'article 2 du Protocole n° 1 - Droit à l'instruction
- Conseil de l'Europe, Réglementer l'utilisation des systèmes d'IA dans l'éducation (en anglais uniquement)
- Conseil de l'Europe, The state of artificial intelligence and education across Europe – Results of a survey of Council of Europe member states (2024) (en anglais uniquement)
-
- Conseil de l'Europe, 1st Working Conference "Artificial Intelligence and education: A critical view through the lens of human rights, democracy and the rule of law" - Conference highlights (2022) (en anglais uniquement)
- Conseil de l'Europe, Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022) (en anglais uniquement)
- Regulating artificial intelligence in the education domain: a general approach (2024: Ilkka TUOMI) (en anglais uniquement)
- Towards a European review framework for AI EdTech systems (2024: Beth HAVINGA) (en anglais uniquement)
- UNESCO, Beijing Consensus on Artificial Intelligence and Education (2019) (en anglais uniquement)
- UNESCO, Artificial Intelligence and Education: Guidance for Policy Makers (2021) (en anglais uniquement)
- (UN) Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment (2021) (en anglais uniquement)

[399] CM/Rec(2018)7, § 71.