Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 16417
02 juin 2026

Protéger la démocratie contre les perturbations causées par l'intelligence artificielle

Rapport[1]
Commission des questions politiques et de la démocratie
Rapporteure: Mme Deborah BERGAMINI, Italie, Groupe du Parti populaire européen

Sommaire **Page**

1. Renvoi en commission: Doc. 15978, Renvoi 4814 du 24 juin 2024.

A. Projet de résolution[2]

1. Le développement des technologies d'intelligence artificielle (IA) se poursuit à un rythme sans précédent, avec la promesse d'améliorer de nombreux aspects de la vie humaine et d'accélérer le développement social et économique. En effet, l'IA pourrait bien constituer la révolution la plus transformatrice de l'histoire de l'humanité. Cependant, les efforts déployés pour faire en sorte que les systèmes d'IA soient sûrs et régulés par des cadres de gouvernance démocratique sont loin de suivre le rythme de l'innovation.

2. L'Assemblée parlementaire est profondément préoccupée par l'impact potentiellement perturbateur de l'IA sur la démocratie en Europe et au-delà. En même temps, l'Assemblée reconnaît que cette technologie ne doit pas être diabolisée, mais qu'elle peut contribuer à faire évoluer les systèmes démocratiques, à condition que toutes les parties prenantes en saisissent les enjeux et prennent des mesures immédiates.

3. Avec un cadre de gouvernance approprié, l'IA peut être mise à profit pour renforcer les processus et les institutions démocratiques, comme souligné dans la feuille de route du Nouveau Pacte Démocratique pour l'Europe. L'IA peut faciliter la participation du public en permettant aux citoyens d'accéder à l'information, en expliquant les politiques complexes, en servant d'intermédiaire dans les délibérations et en identifiant des modèles et des positions communes au sein de grands groupes de personnes. Par ailleurs, elle pourrait aussi permettre à la classe politique et aux pouvoirs publics de recueillir des propositions et des informations concernant les aspirations des citoyens. En ce sens, l'IA peut être un outil puissant au service de la démocratie participative et délibérative.

4. L'IA peut promouvoir l'inclusion en éliminant les barrières socio-économiques et en offrant aux groupes défavorisés un meilleur accès aux services publics, à l'éducation et à l'emploi. En outre, l'IA peut renforcer la protection des droits humains, améliorer l'efficacité avec laquelle l'administration publique fournit des services aux citoyens, et détecter l'utilisation malveillante d'autres outils d'IA.

5. Dans ce contexte, l'Assemblée estime que l'Europe ne devrait pas se limiter à un rôle de régulateur, alors que les grandes avancées en matière d'IA interviennent principalement aux États-Unis et en Chine. Guidée par les valeurs de la démocratie, des droits humains et de l'État de droit, l'Europe devrait montrer la voie dans l'orientation du développement de nouvelles applications de l'IA, en mettant fortement l'accent sur leur dimension humaine. Les risques liés aux technologies d'IA doivent être identifiés, pris en compte et atténués de manière efficace. À cet égard, le Conseil de l'Europe a la responsabilité cruciale de veiller à ce que la relation entre les êtres humains et l'IA reste résolument axée sur le bien commun.

6. La technologie de l'IA repose sur de grands ensembles de données pour entraîner ses systèmes et produire des résultats. Des données personnelles sensibles, souvent collectées en portant atteinte au respect de la vie privée des citoyens, peuvent être exploitées par des individus, des entreprises ou des gouvernements malveillants à des fins telles que la surveillance de masse, la police prédictive, la notation des risques ou la notation sociale, ou encore la censure des opinions politiques. Cela a des effets dissuasifs sur la participation citoyenne.

7. Les ensembles de données utilisés pour entraîner les systèmes d'IA peuvent être pollués par des contenus de désinformation à caractère politique. Ils peuvent aussi contenir des biais, car ils peuvent refléter – voire amplifier – des inégalités déjà présentes dans nos sociétés dans les résultats produits. Lorsque l'IA sert à élaborer des politiques, ces biais peuvent conduire les responsables à prendre des décisions sans être bien informés ou donner lieu à des discriminations à l'égard de certains groupes, comme les femmes ou les minorités. En outre, les systèmes d'IA peuvent parfois «halluciner» et générer des informations incomplètes ou trompeuses.

8. Les données à caractère personnel peuvent être utilisées abusivement pour créer de fausses identités ou produire des contenus synthétiques tels que les hypertrucages (*deepfakes*) sous forme de textes, images, fichiers audio, ou vidéos, qui consistent essentiellement à usurper l'identité d'autrui dans le but de harceler, d'escroquer, de faire chanter ou de commettre d'autres fraudes.

9. Les *deepfakes* et autres contenus synthétiques peuvent aussi être utilisés pour propager de fausses informations, des discours de haine et des contenus qui divisent les opinions. Même avec des ressources limitées et en peu de temps, des campagnes de désinformation bien coordonnées peuvent être lancées à grande échelle pour perturber les débats politiques et les élections. Par le biais des «fermes à bots» et des «fermes de trolls», c'est-à-dire des réseaux créant des profils fictifs programmés pour diffuser

2. Projet de résolution adopté à l'unanimité par la commission le 20 mai 2026.

automatiquement de la désinformation, ces opérations peuvent toucher une large audience très rapidement, en contraste flagrant avec le temps et les ressources nécessaires pour «déconstruire» les récits de désinformation.

10. Des acteurs malveillants, y compris des agents étrangers, exploitent de plus en plus ces opportunités comme méthodes hybrides d'ingérence dans les processus et les institutions démocratiques en Europe. L'Assemblée se félicite par conséquent des travaux en cours du Comité d'experts sur la manipulation de l'information et l'ingérence menées depuis l'étranger, particulièrement en ce qui concerne l'étude de faisabilité sur l'élaboration éventuelle d'un instrument juridique sur la manipulation de l'information et de l'ingérence menées depuis l'étranger, y compris la désinformation.

11. De plus en plus de citoyens se tournent vers les plateformes de médias sociaux comme principale source d'information. En retour, les données recueillies auprès de ces citoyens sont également utilisées pour établir leur profil, identifier leurs préférences et les micro-cibler avec des contenus spécifiques, *in fine* dans le but de manipuler leurs opinions. Le microciblage contribue à la création de chambres d'écho, dans lesquelles les usagers sont exposés à un éventail limité d'idées et de croyances et n'ont pas la possibilité d'engager un dialogue politique constructif avec des personnes qui ont des opinions différentes. Les chatbots, qui sont des logiciels conçus pour simuler une conversation, peuvent aussi être programmés pour censurer des contenus spécifiques et donner des réponses biaisées, ce qui contribue d'autant à la manipulation des choix et des croyances des citoyens.

12. Le modèle commercial des grandes plateformes de médias sociaux vise à monétiser l'engagement des utilisateurs par le biais de la publicité. Dès lors, les algorithmes privilégient les contenus controversés et polarisants. Bien que la plupart de ces plateformes comportent des outils de vérification des faits et de modération, ces outils ne sont pas toujours très efficaces ou suffisamment rapides pour éviter la diffusion de contenus dangereux. En outre, des écosystèmes d'information pollués et les résultats biaisés produits par l'IA peuvent éroder la confiance des citoyens dans les médias traditionnels et dans les processus et institutions démocratiques, contribuant ainsi au recul démocratique.

13. Dans un proche avenir, davantage de responsabilités en matière de prise de décision pourraient être confiées aux systèmes d'IA. Outre le risque d'une mauvaise appréciation des capacités de l'IA, cela pourrait aussi abaisser les normes cognitives humaines et limiter la diversité des points de vue. De nouvelles évolutions pourraient même aboutir à la création d'une «super IA», qui surpasserait les capacités humaines et pourrait potentiellement développer une conscience propre et échapper à tout contrôle humain, avec des conséquences dramatiques.

14. Le contrôle de grands ensembles de données, des réseaux énergétiques, des capacités informatiques et des capacités humaines nécessaires pour développer et déployer les systèmes d'IA est devenu un atout géopolitique et stratégique crucial. Ce contrôle peut conduire à de dangereuses concentrations de pouvoir dans les mains de quelques acteurs privés, à la hausse des inégalités mondiales et à un accroissement des tensions entre États rivaux.

15. Compte tenu de ces considérations, l'Assemblée affirme qu'un contrôle démocratique doit être maintenu tout au long du cycle de vie des systèmes d'IA, du développement au déploiement, de façon à préserver la dignité humaine et à garantir la transparence et la responsabilité. Pour ce faire, il faut une collaboration entre toutes les parties prenantes, à commencer par les acteurs privés qui interviennent dans le domaine de l'IA, afin d'assurer que les systèmes d'IA soient véritablement centrés sur l'humain et autonomisent les êtres humains sans les remplacer.

16. À cette fin, l'Assemblée invite instamment les États membres et observateurs du Conseil de l'Europe à signer et ratifier la Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (STCE n° 225) afin qu'elle entre en vigueur rapidement, et encourage les États non membres dans le monde entier à adhérer à ce traité international, le premier de ce type dans ce domaine, dès qu'ils en auront la possibilité.

17. En outre, l'Assemblée appelle les États membres et observateurs du Conseil de l'Europe:

17.1. à engager une réflexion approfondie sur la nécessité de réglementer le développement et le déploiement de toutes les nouvelles technologies d'IA, y compris celles spécifiquement destinées à la sécurité nationale et à la défense, tout en éliminant les obstacles à l'innovation en Europe;

17.2. à prendre des mesures résolues face aux menaces d'ingérence étrangère et renforcer la résilience face à la désinformation et à la mésinformation, conformément à la Résolution 2593 (2025) et à la Recommandation 2292 (2025) de l'Assemblée; il faudrait notamment adopter des mesures spécifiques pour lutter contre l'utilisation abusive des outils d'IA pour propager des *deepfakes*, par

exemple en rendant obligatoires la vérification des contenus, le debunking (réfutation des contenus trompeurs) et l'ajout de systèmes de marquage numérique des contenus générés par l'IA sur les plateformes de réseaux sociaux;

17.3. à renforcer les critères de transparence, d'explicabilité, d'accessibilité et d'inclusivité requis par les technologies d'IA, y compris celles utilisées par le secteur public ou pour fournir des services publics, ainsi que les algorithmes et les outils de modération de contenu utilisés par les plateformes de médias sociaux;

17.4. à encourager l'utilisation de langues diverses dans le développement des technologies d'IA, afin de garantir leur diversité et leur représentativité;

17.5. à soutenir et promouvoir le développement d'environnements *open source*;

17.6. à veiller à ce que les développeurs d'IA, les fournisseurs et les plateformes de médias sociaux soient tenus responsables de tout préjudice causé par leurs services;

17.7. à mettre en place des mesures de réparation claires, efficaces et appropriées, facilement accessibles aux victimes de préjudices causés par l'IA;

17.8. à intégrer des procédures d'évaluation et d'atténuation des risques et des impacts tout au long du cycle de vie des systèmes d'IA, en mettant l'accent sur les droits humains, la démocratie et l'État de droit, par exemple en impliquant les institutions nationales des droits humains et en adoptant la Méthodologie pour l'évaluation des risques et des impacts des systèmes d'intelligence artificielle du point de vue des droits humains, de la démocratie et de l'État de droit (HUDERIA) du Conseil de l'Europe;

17.9. à renforcer l'éducation aux médias et à l'IA à tous les niveaux d'enseignement, y compris l'éducation informelle, pour tous les groupes d'âge (en mettant particulièrement l'accent sur les personnes âgées), afin de renforcer la capacité à déceler et déconstruire une fausse information (*pré-bunking*), les capacités de codage, l'éthique, la pensée critique et les connaissances générales sur le fonctionnement des technologies d'IA, de façon à garantir que personne n'est laissé pour compte dans la transition numérique;

17.10. à mobiliser des ressources suffisantes pour faire en sorte que la société civile et les citoyens participent à tous les débats autour des technologies d'IA et que l'ensemble des acteurs concernés, notamment les jeunes, prennent part à l'élaboration conjointe de nouvelles réglementations, normes et mécanismes de contrôle;

17.11. à lutter contre la discrimination et les préjugés à l'égard des femmes générés par l'IA, et à garantir l'égalité des chances entre les femmes et les hommes dans le développement, le déploiement et l'utilisation des technologies d'IA;

17.12. à consacrer des ressources à la prospective et à la recherche sur les multiples répercussions des nouvelles technologies d'IA sur la psychologie des individus ainsi que sur les écosystèmes informationnels, les institutions et les processus démocratiques, la production d'énergie, l'environnement et la société dans son ensemble, afin de pouvoir réagir chaque fois que nécessaire par le biais de la réglementation, du contrôle et d'autres mesures préventives ou d'atténuation;

17.13. à définir des cadres clairs pour leurs relations avec les grandes entreprises technologiques, afin que leur influence sur les sociétés démocratiques puisse être correctement contrôlée et réglementée chaque fois que nécessaire, notamment par le biais de lois antitrust appropriées visant à empêcher la formation d'oligopoles et la concentration du pouvoir;

17.14. à envisager de définir clairement des lignes rouges concernant le développement de certaines technologies, et un moratoire sur le développement de la super IA.

18. Pour exploiter pleinement les avantages potentiels de l'IA et renforcer la sécurité démocratique, l'Assemblée appelle par ailleurs les États membres et les États observateurs du Conseil de l'Europe:

18.1. à explorer toutes les utilisations possibles de l'IA pour renforcer la démocratie, notamment pour améliorer la prestation des services publics, renforcer la protection des droits humains et réduire toutes les formes de discrimination;

18.2. à encourager et à soutenir le développement d'approches innovantes pour stimuler l'engagement citoyen, notamment par le biais de consultations à grande échelle alimentées par l'IA sur des sujets difficiles, afin de renforcer la participation des citoyens aux processus d'élaboration des politiques et de prise de décision;

18.3. à encourager et à soutenir le développement d'outils basés sur l'IA pour détecter, enquêter et éliminer les contenus malveillants générés par l'IA et les cyberattaques.

19. Afin de renforcer la souveraineté numérique de l'Europe et de réduire la dépendance du continent à l'égard de prestataires externes, l'Assemblée appelle les États membres du Conseil de l'Europe:

19.1. à adopter de solides mesures de cybersécurité pour assurer la protection des algorithmes, modèles, applications, réseaux pertinents, ensembles de données et infrastructures essentielles de l'Europe contre les pirates informatiques malveillants;

19.2. à mettre l'accent sur l'éducation, le perfectionnement des compétences, l'attraction et la rétention des talents afin de former la prochaine génération de leaders et d'innovateurs qui connaîtront les dernières évolutions technologiques et sauront parvenir à un développement économique et social durable grâce à celles-ci;

19.3. à développer des espaces d'expérimentation («*sandbox*») paneuropéens structurés dans lesquels mettre à l'épreuve les nouvelles technologies et les nouveaux outils dans des environnements sécurisés et fermés, dans des cadres de gouvernance solides;

19.4. à identifier les domaines dans lesquels l'Europe dispose encore d'un avantage comparatif (par exemple l'informatique quantique, les technologies vertes ou le développement d'applications spécialisées) et en tirer parti en prévoyant des ressources et des incitations financières suffisantes, en simplifiant le cadre réglementaire et en renforçant les écosystèmes d'innovation (universités, centres de recherche, start-ups) et les infrastructures (centres de données, *clouds* souverains, calcul haute performance et production de puces);

19.5. à développer une innovation responsable, grâce à la participation de toutes les parties prenantes et au renforcement des partenariats public-privé, parallèlement à la réglementation;

19.6. à stimuler un changement culturel vers une plus grande tolérance à la prise de risques contrôlée.

20. Consciente du caractère global des défis soulevés par l'essor de l'IA, l'Assemblée appelle les États dans le monde entier à envisager de créer un organisme multilatéral dédié exclusivement à la supervision des technologies d'IA. Cet organisme pourrait définir un langage commun, des normes et un cadre réglementaire, en associant toutes les parties intéressées, et coordonner les diverses initiatives en cours lancées par différentes organisations multilatérales.

21. En outre, l'Assemblée invite les entreprises privées à coopérer de bonne foi avec les organisations multilatérales, les gouvernements nationaux et locaux, la société civile et les milieux universitaires pour garantir que le développement et le déploiement des technologies d'IA, dans tous les domaines, soient guidés par le respect des principes démocratiques, des droits humains et de l'État de droit.

22. L'Assemblée encourage également les parlements nationaux à accorder la priorité à l'IA dans leurs travaux. Cela devrait inclure non seulement la législation et la réglementation, mais aussi la promotion de débats généraux sur les usages de l'IA et le suivi des évolutions sociétales et des changements institutionnels pertinents. Une façon d'y parvenir serait de créer et d'institutionnaliser des commissions parlementaires sur l'IA.

23. Enfin, l'Assemblée décide de continuer à travailler sur cette question par le biais des rapports établis par ses différentes commissions et en organisant des événements spécifiques sur l'IA, et également en lien avec le Nouveau Pacte Démocratique pour l'Europe.

B. Exposé des motifs par M^me^ Deborah Bergamini, rapporteure[3]

1. Introduction

1. Les technologies numériques se sont développées plus rapidement que toute autre innovation dans l'histoire de l'humanité[4]. Le rythme des progrès est devenu si rapide que les tentatives nationales et internationales visant à réglementer leur utilisation, à exploiter leurs avantages et à atténuer les menaces qu'elles font peser sur la société risquent en permanence de devenir prématurément obsolètes.

2. Cela est particulièrement vrai dans le cas de l'intelligence artificielle (IA). L'utilisation de systèmes d'IA suscite des inquiétudes, notamment en raison de leur impact potentiellement négatif sur les libertés fondamentales et les processus et institutions démocratiques.

3. Les conséquences sont, entre autres, la violation de la vie privée des citoyens, l'utilisation de leurs données personnelles pour contrôler, contraindre, censurer ou punir leurs décisions et leur comportement, la diffusion de fausses informations et de désinformations pour influencer leurs opinions et leurs choix, et le risque de cyber-attaques sur des sites web et des bases de données publics sensibles.

4. Les implications sont également importantes pour la sécurité démocratique et la souveraineté des pays, car les outils d'IA peuvent devenir des armes efficaces entre les mains d'acteurs étrangers malveillants qui cherchent à déstabiliser les démocraties.

5. Toutefois, comme l'indique le rapport scientifique international sur la sécurité de l'IA avancée, «l'IA ne nous est pas imposée: ce sont les choix des individus qui déterminent son avenir. L'avenir de la technologie de l'IA à usage général est incertain, avec un large éventail de trajectoires qui semblent possibles même dans un avenir proche, comprenant à la fois des résultats très positifs et très négatifs. Cette incertitude peut évoquer le fatalisme et faire apparaître l'IA comme quelque chose qui nous arrive. Mais ce sont les décisions des sociétés et des gouvernements sur la manière de gérer cette incertitude qui détermineront la voie que nous emprunterons»[5].

6. L'Assemblée parlementaire doit évaluer ces préoccupations en analysant les abus potentiels des systèmes d'IA, leur impact sur la démocratie, les droits humains et l'État de droit, et la manière dont ils peuvent être atténués ou neutralisés.

7. En préparant ce rapport, la commission des questions politiques et de la démocratie a tenu plusieurs auditions au cours de l'année 2025:

– le 5 mars, avec la participation en ligne de M. Daniel Innerarity, titulaire de la chaire IA et démocratie à l'École de gouvernance transnationale, Institut universitaire européen (qui a également fait part de quelques réflexions supplémentaires sur les implications géopolitiques de l'IA, rédigées par lui-même et d'autres collègues de l'Institut universitaire européen);

– le 24 juin, avec la participation de M. Courtney Bowman, directeur de l'ingénierie en matière de confidentialité et de libertés civiles, Palantir, M^me^ Audrey Herblin-Stoop, vice-présidente et directrice des affaires publiques globales, Mistral AI (en ligne), M^me^ Julie Lavet, responsable des politiques et des partenariats pour l'Europe, OpenAI, et M. Ben Nimmo, enquêteur principal sur les menaces, OpenAI (en ligne);

– le 10 décembre, avec la participation de M^me^ Francesca Fanucci, conseillère juridique principale, Centre européen pour le droit des organisations à but non lucratif (ECNL), et représentante de la Conférence des ONG internationales du Conseil de l'Europe au Comité sur l'intelligence artificielle du Conseil de l'Europe.

8. La rapporteure tient à remercier tous les participants susmentionnés pour leurs contributions, ainsi que les membres de la commission pour leurs commentaires et leur soutien dans la préparation du présent rapport.

---

3. L'exposé des motifs est établi sous la responsabilité du rapporteur. Sa version originale anglaise a été traduite vers le français par un outil de traduction automatique.
4. www.un.org/fr/un75/impact-digital-technologies.
5. Gouvernement britannique, AI Action Summit, «International Scientific Report on the Safety of Advanced AI», janvier 2025.

2. Travaux antérieurs de l'Assemblée parlementaire

9. Le Conseil de l'Europe aborde l'impact des technologies de l'IA sur la vie humaine de manière globale et comme une priorité transversale. L'Assemblée contribue de manière importante à ces travaux. Elle dispose notamment d'une sous-commission sur l'intelligence artificielle et les droits de l'homme, et a adopté en octobre 2020 une série de résolutions et de recommandations sur le sujet[6]; parmi celles-ci, j'ai été rapporteure du rapport intitulé «Nécessité d'une gouvernance démocratique de l'intelligence artificielle»[7].

10. Dans une annexe commune à ces rapports, l'Assemblée a énoncé les principes éthiques qu'elle estime devoir être appliqués aux systèmes d'IA: transparence, justice et équité, responsabilité, sûreté et sécurité, respect de la vie privée.

11. Dans l'Avis 303 (2024), l'Assemblée se félicite également de la finalisation de la Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, et déclare qu'elle continuera à travailler sur les questions liées à l'IA.

12. Plus récemment, l'Assemblée a adopté la Résolution 2628 (2025) et la Recommandation 2300 (2025) «L'intelligence artificielle et la migration», ainsi que la Résolution 2654 (2026) «La protection du droit d'auteur dans l'environnement de l'intelligence artificielle».

13. En outre, l'Assemblée a coorganisé une conférence parlementaire sur l'intelligence artificielle avec le Parlement du Royaume-Uni, à Londres, les 15 et 16 décembre 2025. Cette conférence a été l'occasion d'échanger les meilleures pratiques et de définir le rôle des parlements dans la gouvernance de l'IA, et elle a permis de dégager plusieurs éléments pertinents pour le présent rapport[8].

14. Enfin, il convient également de mentionner que l'Assemblée parlementaire travaille actuellement sur plusieurs autres rapports pertinents concernant:

– «La transformation numérique: le rôle de l'OCDE dans l'évaluation de l'impact de l'intelligence artificielle sur l'avenir du travail»;

– «La nécessité de moderniser le droit international humanitaire» (qui prend également en compte l'utilisation de l'IA dans les conflits armés);

– «Utilisation de l'intelligence artificielle par les parlements: risques et opportunités»;

– «Sauvegarder les droits humains dans le cadre de l'utilisation de l'intelligence artificielle dans le secteur public»;

– «Préserver la créativité et l'éducation à l'ère de l'intelligence artificielle générative»;

– «Intelligence artificielle et égalité de genre: risques et défis».

15. Les travaux en cours de l'Assemblée soulignent l'importance qu'elle accorde à l'analyse de l'impact de l'IA à plusieurs niveaux dans les pays européens, dans le but d'identifier les domaines critiques et de définir des solutions à ce défi majeur. L'Assemblée continuera à accorder la priorité à cette question et à soutenir les efforts visant à faire face aux implications en constante évolution de l'IA.

3. Les menaces que l'intelligence artificielle fait peser sur la démocratie

16. 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 (STCE n° 225) définit un «système d'IA» comme «un système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influer sur des environnements physiques ou virtuels»[9]. En d'autres termes, les systèmes d'IA simulent des capacités cognitives et effectuent des tâches qui sont normalement associées aux humains: celles-ci comprennent l'analyse et le traitement de données, la résolution de problèmes, la prise de décision et, surtout, l'apprentissage.

---

6. https://pace.coe.int/fr/pages/artificial-intelligence.
7. Doc. 15150. Voir aussi Résolution 2341 (2020) et Recommandation 2181 (2020).
8. https://pace.coe.int/fr/pages/aiconferencelondon.
9. https://rm.coe.int/1680afae3d.

17. Les technologies d'IA actuelles sont définies comme des IA «étroites» ou «faibles»: elles peuvent effectuer des tâches spécifiques et limitées, selon certaines instructions, et le font souvent plus rapidement et plus efficacement que les humains. Il est possible que les développements futurs conduisent à une IA «générale» ou «forte», qui serait capable d'appliquer ce qu'elle a appris à différents contextes et d'égaler les capacités humaines. Il existe même la possibilité d'une «super IA», qui serait capable de surpasser les capacités humaines et pourrait potentiellement avoir sa propre «conscience».

18. L'idée d'un avenir dystopique dans lequel la démocratie pourrait être remplacée par l'«algocratie», ou le gouvernement par des algorithmes, par le biais d'une super IA consciente plutôt que par des représentants élus, n'est actuellement qu'une hypothèse. Cependant, compte tenu du rythme des progrès technologiques et de leurs multiples implications pour la géopolitique, les droits humains, la démocratie, l'économie et l'environnement, il est essentiel de surveiller les menaces et les perturbations très réelles que l'IA étroite fait déjà peser sur les pays démocratiques.

19. ChatGPT, un système d'IA «génératif», et l'un des chatbots d'IA le plus populaires[10] disponible au public aujourd'hui, partage le même point de vue. À la question «Pensez-vous que vous êtes une menace pour la démocratie?», le chatbot a donné la réponse suivante:

> *«En tant qu'IA, ma fonction première est d'aider et de fournir des informations, et non d'influencer la prise de décision ou d'entreprendre des actions qui pourraient menacer la démocratie. Cependant, la manière dont les systèmes d'IA sont utilisés peut certainement avoir des conséquences sur les processus démocratiques. L'IA peut être utilisée à mauvais escient par des individus ou des organisations pour manipuler l'opinion publique, diffuser des informations erronées ou porter atteinte à la vie privée. J'ai été conçu avec des lignes directrices éthiques pour promouvoir des interactions positives, la transparence et le respect de la vie privée. Mais les systèmes d'IA comme le mien ne sont éthiques et responsables que dans la mesure où les politiques, les cadres et les personnes qui les gouvernent le sont. La véritable menace pour la démocratie surviendrait si les systèmes d'IA étaient exploités de manière à miner la confiance, l'équité et la justice. C'est pourquoi il est important que la société établisse des réglementations et des garanties claires autour de l'IA afin de prévenir de tels risques.»*

20. Il est évidemment important de se demander comment cette réponse a été générée: Les chatbots IA sont des logiciels capables d'«interagir» avec le langage humain, utilisant des algorithmes sophistiqués pour traiter la demande qui leur est faite et produire des résultats basés sur leur accès à de très grandes bases de données. En d'autres termes, la réponse donnée par ChatGPT est basée sur des rapports, des articles, des déclarations et des publications de toutes sortes disponibles dans ses bases de données et sur Internet.

21. Cependant, la manière dont les algorithmes sont conçus peut grandement influencer la manière dont les résultats sont produits. Par exemple, dans la réponse fournie ci-dessus, ChatGPT déclare qu'il est «conçu avec des lignes directrices éthiques» – mais qui définit ces lignes directrices comme étant éthiques? Et qui veille à ce qu'elles soient respectées? Par conséquent, le manque de transparence de certains algorithmes, ainsi que le fait que l'autorégulation par les entreprises développant des systèmes d'IA ne semble pas suffisante, sont des questions supplémentaires qui doivent être évaluées.

22. Cela se reflète également dans l'opinion publique à l'égard de l'IA et de sa gouvernance: selon les données du Pew Research Centre, 34 % des adultes interrogés dans 25 pays se disent plus inquiets qu'enthousiastes face à l'utilisation croissante de l'IA[11]; selon l'enquête de l'Organisation de coopération et de développement économiques (OCDE) sur les déterminants de la confiance dans les institutions publiques, seuls 41 % des personnes interrogées dans 30 pays pensaient que leur gouvernement national était susceptible de réglementer de manière adéquate les nouvelles technologies, telles que l'IA et les applications numériques, et d'aider les entreprises et les citoyens à les utiliser de manière responsable[12]; et selon une étude de l'Institut Ada Lovelace, une très grande majorité des personnes interrogées au Royaume-Uni estime que la sécurité doit primer sur la rapidité et que la possibilité d'interdire l'IA pour des raisons éthiques est plus importante que les avantages concurrentiels[13].

---

10. Selon le dictionnaire de Cambridge, il s'agit d'un programme informatique conçu pour converser avec un être humain, généralement par l'intermédiaire de l'internet.
11. Pew Research Center, «How People Around the World View AI», 15 octobre 2025.
12. OCDE, Enquête de l'OCDE sur les déterminants de la confiance dans les institutions publiques – résultats 2024, juillet 2024.
13. Ada Lovelace Institute, "Mind the gap: reflections on 2025", 18 décembre 2025.

23. Selon l'université de Stanford, les capacités de l'IA dépassent désormais les critères de référence conçus pour les mesurer, surpassant les performances humaines établies. De plus, bien que les critères de référence pour une IA responsable (c'est-à-dire l'ensemble des pratiques et des mécanismes de gouvernance conçus pour garantir que les systèmes d'IA sont sûrs, équitables et bénéfiques, et qu'ils fonctionnent comme prévu) se multiplient, ils ne suivent pas le rythme des avancées et des déploiements de l'IA. L'université de Stanford a également signalé que les entreprises spécialisées dans l'IA sont devenues moins transparentes en 2025, ce qui renforce les inquiétudes quant aux méthodes de développement, d'entraînement, de test et de surveillance des systèmes[14].

3.1. Tout commence par les données

24. Les systèmes et outils d'IA reposent largement sur la capacité à collecter, stocker et analyser de grands ensembles de données, qui peuvent inclure des données à caractère personnel. Ces grands ensembles de données sont ensuite utilisés pour «entraîner» de nombreux types d'outils d'IA. Les grands modèles de langage, par exemple, sont des réseaux neuronaux fonctionnant de manière probabiliste, générant ainsi leurs résultats sur la base des modèles qu'ils identifient dans les ensembles de données.

25. L'utilisation abusive des systèmes d'IA par les gouvernements, les entreprises privées et d'autres entités pour accéder à des données à caractère personnel sans consentement est l'une des menaces les plus importantes, en raison de ses implications potentielles.

26. Les données à caractère personnel peuvent être utilisées à des fins de surveillance de masse par le biais de caméras vidéo publiques, de la localisation GPS des téléphones portables des citoyens ou de l'utilisation de leurs cartes de crédit[15]. Cette pratique est déjà largement répandue en Chine, à des fins d'évaluation des risques et de police prédictive, c'est-à-dire pour prévoir d'éventuels crimes et troubles futurs, sur la base de rapports de police antérieurs, de données de surveillance et d'activité sur les réseaux sociaux, ce qui a un effet dissuasif sur l'activisme de la société civile[16].

27. De plus, des acteurs malveillants peuvent utiliser des données personnelles pour créer de fausses identités à des fins frauduleuses et pour commettre des escroqueries. La technologie IA peut également être utilisée pour créer des deepfakes en clonant l'image ou la voix d'une personne afin de créer de fausses images, des fichiers audios ou des vidéos (également appelés «médias synthétiques»). Ceux-ci peuvent ensuite être utilisés pour faire chanter ou harceler des victimes, ou être diffusés à grande échelle et distribués par des robots sur les grandes plateformes de réseaux sociaux afin de propager de fausses informations. Parmi les exemples récents préoccupants, on peut citer les centaines de deepfakes sexuellement explicites ciblant les femmes générées par Grok, l'outil d'IA intégré à la plateforme de réseau social X[17].

28. Les ensembles de données peuvent être déséquilibrés et contenir des biais qui sont ensuite reproduits dans les résultats produits par les systèmes d'IA. Cela peut conduire à ou renforcer la discrimination, en particulier à l'égard des femmes et des minorités, lorsque les systèmes sont adoptés à des fins d'élaboration de politiques publiques[18]. Les algorithmes utilisés pour analyser les données et produire des résultats peuvent également être biaisés et conduire à des discriminations. En ce sens, les systèmes et outils d'IA sont rarement neutres; ils héritent souvent des biais des sociétés dans lesquelles ils sont construits et déployés.

29. En outre, les individus peuvent être affectés par des décisions algorithmiques potentiellement biaisées basées sur l'IA à leur insu. Cela porte atteinte à leur droit à un recours effectif, d'autant plus que ces systèmes fonctionnent souvent comme des «boîtes noires» et qu'il est alors presque impossible d'en attribuer la responsabilité.

30. Il est important de noter que, selon certaines estimations, le stock disponible de données de haute qualité pour l'entraînement des modèles d'IA pourrait être entièrement utilisé entre 2026 et 2032, ce qui soulève également des inquiétudes quant à la possibilité de faire évoluer les modèles et d'étendre leurs capacités.[19]

---

14. Université de Stanford, “The AI Index 2026 Annual Report”, avril 2026.
15. www.theregister.com/2024/09/16/oracle_ai_mass_surveillance_cloud/.
16. A. Cevallos, “How Autocrats Weaponize AI — And How to Fight Back” Journal of Democracy, mars 2025.
17. www.politico.eu/article/france-lawmaker-investigate-deepfakes-women-stripped-naked-grok-x/..
18. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/.
19. https://epoch.ai/blog/will-we-run-out-of-data-limits-of-llm-scaling-based-on-human-generated-data.

3.2. La désinformation et les médias

31. Le Rapport sur les risques mondiaux 2026 du Forum économique mondial classe la «désinformation et la mésinformation» comme le deuxième risque le plus grave à court terme, juste après la «confrontation géoéconomique»[20].

32. Si la désinformation et la mésinformation ne sont pas des phénomènes nouveaux, le développement et le déploiement accélérés des systèmes et outils d'IA contribuent certainement de manière importante à ce risque. L'IA peut être utilisée pour fabriquer de fausses informations et les diffuser à grande échelle avec des ressources et des compétences limitées, et ce très rapidement. Comme les fausses informations se propagent plus rapidement en ligne que la vérité[21] et compte tenu des coûts, des ressources et du temps nécessaires pour les démentir (souvent sans parvenir à les contrer efficacement), cela représente une autre menace majeure pour les démocraties.

33. Des acteurs étrangers malveillants mènent des campagnes de désinformation à grande échelle, comme le réseau russe «Portal Kombat» identifié par les autorités françaises en février 2024[22]. En inondant l'écosystème de l'information de milliers de fausses informations, de déclarations mensongères et de deepfakes, ces réseaux empoisonnent les ensembles de données sur lesquels sont entraînés les grands modèles de langage, influençant ainsi les résultats produits par ces modèles.

34. De même, les «fermes à bots» les «fermes de trolls» sont de plus en plus utilisées pour diffuser de fausses informations sur les réseaux sociaux, en créant des profils fictifs programmés pour diffuser automatiquement de la désinformation, des discours haineux et des contenus perturbateurs. Les plateformes, quant à elles, ne sont pas toujours efficaces pour modérer et supprimer les contenus mensongers – et dans certains cas, elles n'ont d'ailleurs pas intérêt à le faire: leurs algorithmes sont structurés de manière à donner la priorité aux contenus les plus engageants, ce qui leur permet de les monétiser. La plupart du temps, il s'agit précisément des contenus mensongers perturbateurs et clivants qui devraient être supprimés. Les plateformes peuvent donc exercer un pouvoir de contrôle très fort sur le discours politique, grâce à leurs capacités de modération des contenus.

35. D'autre part, la manipulation de l'information est également utilisée pour détourner l'attention des individus et susciter la méfiance envers les institutions, attisant ainsi des sentiments et des comportements antidémocratiques. Les technologies numériques et l'IA générative favorisent la prolifération et la fragmentation des réalités perçues, ce qui constitue une menace vitale: la démocratie ne peut survivre sans un certain degré de réalité partagée[23].

36. En outre, l'essor des plateformes de réseaux sociaux et le déploiement plus récent d'outils d'IA affectent également le modèle économique des médias traditionnels. Ces plateformes se nourrissent souvent de contenus sans aucune protection de la propriété intellectuelle, ce qui a de graves implications pour la diversité et la qualité de l'information[24]. Une estimation inquiétante suggère qu'en novembre 2024, le nombre d'articles générés par l'IA sur Internet était supérieur au nombre d'articles produits par des humains[25].

3.3. Persuasion politique et microciblage

37. La technologie de l'IA semble avoir dépassé la capacité des êtres humains à persuader les gens[26]. Les technologies numériques et les systèmes d'IA peuvent donc être utilisés pour influencer le comportement des citoyens, en particulier en ce qui concerne leurs attitudes politiques, avec des menaces croissantes apparaissant pendant les élections. Les informations, manipulations et ingérences étrangères (FIMI) constituent une menace importante pour les démocraties européennes.

38. Parmi les exemples récents, on peut citer le premier tour des élections présidentielles organisées en Roumanie le 24 novembre 2024, qui ont été annulées par la Cour constitutionnelle en raison des techniques de manipulation numérique sophistiquées qui auraient été déployées sur les grandes plateformes de médias sociaux (en particulier Tik-Tok), très probablement par une puissance étrangère[27]; et les élections législatives

---

20. Forum économique mondiale, "The Global Risks Report 2026", 14 janvier 2026.
21. S. Vosoughi, D. Roy, S. Aral, "The spread of true and false news online", Science, Vol 359, Issue 6380, 9 mars 2018.
22. VIGINUM, "PORTAL KOMBAT: un réseau structuré et coordonné de propagande prorusse", février 2024.
23. M. Scharfbillig, S. Lewandowsky, S. Altay, M. van Alstyne, A. Kozyreva, et al., "Fractured reality – How democracy can win the global struggle over the information space", Publications Office of the European Union, Luxembourg, 2026.
24. Anya Schiffrin, "AI slop and the battle for truth — why platform dominance threatens quality information", Daily Maverick, 30 June 2025.
25. https://graphite.io/five-percent/more-articles-are-now-created-by-ai-than-humans.
26. www.technologyreview.com/2025/05/19/1116779/ai-can-do-a-better-job-of-persuading-people-than-we-do/.

moldaves qui se sont tenues le 28 septembre 2025, au cours desquelles la Russie a mené une campagne de désinformation massive, dépensant pour cela l'équivalent de plus de 1 % du PIB de la République de Moldova[28].

39. Les systèmes et outils d'IA peuvent être utilisés pour micro-cibler précisément certains groupes de citoyens à des fins marketing, mais aussi pour influencer leurs opinions et leurs choix politiques. Cela peut passer par une restriction de leur accès à certaines sources d'information tout en amplifiant leur exposition à d'autres, grâce à un profilage psychologique des utilisateurs, qui reçoivent alors des messages et des contenus hautement personnalisés. Une influence rémunérée peut également être intégrée dans les résultats générés par l'IA, d'une manière qui ne permet pas de la distinguer d'un contenu neutre.

40. Le microciblage contribue à la création de chambres d'écho, dans lesquelles les citoyens ne sont pas exposés à une diversité d'opinions et sont incapables d'engager un dialogue politique avec ceux qui pensent différemment. Au contraire, ils sont des récepteurs passifs d'informations et d'idées qui renforcent leurs propres convictions.

41. Les chatbots, en particulier, peuvent être très efficaces dans la persuasion politique. Une étude récente menée au Canada et aux États-Unis a montré comment ils pouvaient être utilisés pour persuader les gens de changer leur orientation de vote[29]. De même, avant les élections législatives du 29 octobre 2025, l'autorité néerlandaise chargée de la protection des données a averti que les chatbots basés sur l'IA n'étaient pas fiables et manifestement biaisés lorsqu'ils donnaient des conseils de vote[30].

42. Dans un nombre croissant de pays, on utilise également des «softfakes», des images synthétiques créées pour rendre les candidats politiques plus attrayants. Bien qu'elles soient souvent créées par les candidats eux-mêmes (ou leurs équipes), leur utilisation dans les campagnes électorales soulève néanmoins des questions éthiques[31].

43. Enfin, l'IA peut également être utilisée pour censurer certains contenus spécifiques. Le chatbot chinois DeepSeek (dont les performances globales sont comparables à celles de ChatGPT et d'autres chatbots fabriqués aux États-Unis, mais qui coûte nettement moins cher)[32], censure ou biaise les réponses aux questions liées au gouvernement chinois, démontrant ainsi clairement comment ces outils peuvent être utilisés pour influencer les utilisateurs[33].

3.4. Autres menaces

44. Les menaces décrites ci-dessus peuvent avoir un effet néfaste supplémentaire sur la démocratie, en raison du déploiement accru des systèmes et outils d'IA, car elles renforcent la méfiance des citoyens à l'égard des médias, des institutions publiques et de l'intégrité des processus démocratiques. Non seulement les citoyens risquent d'être trompés par des contenus mensongers, mais ils peuvent également devenir plus cyniques. Une lassitude vis-à-vis de l'actualité peut apparaître, et les gens peuvent être amenés à se fier davantage aux réseaux sociaux qu'aux médias traditionnels (ce qui est déjà le cas pour la plupart des jeunes Européens)[34], voire à ne plus croire aucune source d'information. Cela alimente encore davantage la polarisation et les troubles sociaux, contribuant ainsi au recul de la démocratie.

45. Les «hallucinations» de l'IA constituent une menace supplémentaire, car elles génèrent des résultats contenant des informations fausses ou trompeuses. Celles-ci peuvent renforcer la discrimination et propager la désinformation, polluant davantage les ensembles de données et l'écosystème informationnel. Elles peuvent également avoir des conséquences diffamatoires pour les individus: dans un cas récent, en Norvège, un homme a demandé à ChatGPT des informations le concernant et a reçu en réponse une fausse affirmation selon laquelle il aurait assassiné ses deux fils[35].

---

27. VIGINUM, "Manipulation d'algorithmes et instrumentalisation d'influenceurs: enseignements de l'élection présidentielle en Roumanie & risques pour la France" février 2025.
28. Statement of the Delegation to the EU-Moldova Parliamentary Association Committee of the European Parliament, 29 September 2025.
29. www.cbc.ca/news/politics/canada-elections-artificial-intelligence-9.7021876.
30. www.theguardian.com/world/2025/oct/21/ai-chatbots-unreliable-biased-advice-voters-dutch-watchdog.
31. www.nature.com/articles/d41586-024-00995-9.
32. www.bbc.com/news/articles/c5yv5976z9po.
33. www.theguardian.com/technology/2025/jan/28/we-tried-out-deepseek-it-works-well-until-we-asked-it-about-tiananmen-square-and-taiwan.
34. https://fr.euronews.com/my-europe/2025/02/19/les-reseaux-sociaux-sont-desormais-la-principale-source-dinformation-des-jeunes-europeens.

46. En outre, il existe un risque que l'utilisation excessive des outils d'IA puisse réduire la capacité des individus à penser de manière critique et à innover, en fixant des normes moins élevées et en limitant la diversité des points de vue. Les citoyens pourraient utiliser l'IA pour poser des questions à leurs représentants élus, qui pourraient également utiliser l'IA pour fournir leurs réponses. De même, les étudiants pourraient utiliser l'IA pour produire leurs travaux, et les enseignants pourraient ensuite utiliser l'IA pour les corriger.

47. Si une IA incompétente se voit confier des responsabilités décisionnelles, sur la base d'un optimisme technologique injustifié ou d'une mauvaise appréciation des capacités réelles de l'IA, il existe un risque supplémentaire d'«élévation de l'incompétence», qui pourrait avoir des conséquences catastrophiques.

48. L'utilisation d'outils d'IA peut également conduire à la solitude et à l'érosion des compétences sociales, en particulier lorsque les utilisateurs anthropomorphisent l'outil et l'utilisent comme un substitut synthétique aux relations réelles, y compris les relations amoureuses[36].

49. La propriété des ensembles de données, associée au contrôle des systèmes d'IA et des technologies informatiques les plus puissants, peut conduire à une concentration dangereuse du pouvoir entre les mains des entreprises technologiques privées, en particulier en l'absence d'une surveillance adéquate[37].

50. En outre, les différents niveaux d'accès à la technologie et aux compétences nécessaires pour l'utiliser pleinement peuvent conduire à des inégalités accrues entre les citoyens. Les femmes, les personnes âgées et les groupes marginalisés ayant un accès limité à l'éducation peuvent être les plus vulnérables. S'il est trop tôt pour prévoir les effets nets de l'IA sur le marché du travail, il est possible que certains groupes soient laissés pour compte dans la transition numérique: ceux qui perdront leur emploi en raison de l'automatisation croissante des tâches pourraient se sentir davantage marginalisés et enclins à l'extrémisme politique.

51. Enfin, la demande croissante en services d'IA et les besoins connexes en capacités de stockage de données et de calcul toujours plus importantes peuvent avoir un impact considérable sur la production d'énergie et l'environnement, notamment en ce qui concerne les émissions de CO2 et la consommation d'eau.

4. Comment l'intelligence artificielle peut-elle renforcer la démocratie?

52. L'IA ne doit cependant pas être diabolisée, car elle peut également renforcer les processus démocratiques, à condition d'être correctement développée, déployée, et contrôlée. Bien qu'il existe des risques, l'IA offre également des opportunités. Avec une gouvernance, des normes et des règles appropriées, ces opportunités pourraient compenser les menaces, transformant l'IA en un formidable outil pour renforcer les institutions et les processus démocratiques, les rendant plus résilients et prêts à relever les défis de l'avenir. Il est encore temps de faire en sorte que ce changement se produise.

53. L'utilisation la plus évidente des systèmes d'IA en politique est le renforcement de la participation publique. L'IA pourrait notamment permettre aux citoyens d'accéder à des informations spécifiques, analyser et expliquer des politiques par ailleurs techniquement compliquées, servir de médiateur et résumer des discussions, identifier des modèles et des positions communes au sein de grands groupes de personnes participant à des consultations et à des processus délibératifs, et faciliter leur interaction avec leurs représentants élus ou les autorités publiques[38]. En ce sens, l'IA pourrait, dans un avenir proche, être utilisée pour faciliter les consultations internationales et identifier des solutions communes aux problèmes mondiaux[39].

54. De même, l'IA pourrait également être utilisée par les représentants élus et les autorités publiques pour recueillir des commentaires, des propositions et des informations sur les besoins et les souhaits des citoyens de leur communauté. Ceci soutiendrait les processus d'élaboration des politiques et de prise de décision en les rendant plus ciblés et plus efficaces.

---

35. https://www.theguardian.com/technology/2025/mar/21/norwegian-files-complaint-after-chatgpt-falsely-said-he-had-murdered-his-children.
36. E. Andoh, "AI chatbots and digital companions are reshaping emotional connection", American Psychological Association, Monitor on Psychology 2026, Vol. 57 No. 01, 1 January 2026.
37. www.brookings.edu/articles/how-public-ai-can-strengthen-democracy/.
38. www.imf.org/fr/Publications/fandd/issues/2023/12/POV-Fostering-more-inclusive-democracy-with-AI-Landemore.
39. www.lemonde.fr/idees/article/2025/02/07/l-intelligence-artificielle-permet-d-inventer-de-nouveaux-processus-democratiques_6536494_3232.html.

55. De plus, les outils d'IA peuvent avoir un impact positif sur l'inclusion, car ils pourraient offrir à des personnes de tous horizons, et en particulier aux groupes défavorisés, un meilleur accès aux services publics, à l'éducation et aux opportunités d'emploi, ce qui permettrait d'uniformiser les règles du jeu et d'éliminer les obstacles.

56. L'IA pourrait donc encourager les citoyens à participer davantage à la sphère publique, les rapprochant ainsi des responsables politiques qui prennent les décisions affectant leur vie. Cela pourrait, à son tour, inverser la tendance à l'abstention, car les citoyens retrouveraient confiance dans les institutions en sentant que leur voix est entendue et prise en compte.

57. L'IA peut également être utilisée pour renforcer la protection des droits humains (par exemple en luttant contre la traite des êtres humains)[40] ou pour automatiser et accélérer certaines procédures administratives publiques, augmentant ainsi la productivité, la réactivité, la responsabilité[41] et, par conséquent, améliorant la satisfaction des citoyens à l'égard du travail et des performances de leurs gouvernements locaux et nationaux.

58. Plusieurs parlements européens, dont l'Assemblée, testent déjà des outils d'IA pour améliorer leur fonctionnement interne. En septembre 2025, l'Albanie a lancé Diella, une «ministre IA» chargée des marchés publics, dans le but de rendre le processus transparent et incorruptible[42].

59. Enfin, la technologie de l'IA pourrait être utilisée pour surveiller et identifier les tentatives d'influence des citoyens au moyen de l'IA elle-même, par exemple en identifiant le contenu généré par l'IA, et en général pour assurer un contrôle démocratique plus fort sur le développement, l'essai et l'application des systèmes et des outils d'IA.

5. Implications géopolitiques

60. La course au développement et au contrôle de la technologie de l'IA, de son infrastructure et des ressources associées déterminera l'évolution des relations géopolitiques à l'échelle mondiale dans les années à venir.

61. La première implication concerne la «souveraineté numérique» des pays. La propriété et le contrôle des ensembles de données et des centres de données, des capacités de cloud computing (y compris l'informatique quantique), des compétences humaines, des pôles de recherche et de développement en IA et des réseaux énergétiques suffisants deviendront des atouts de plus en plus précieux pour la sécurité nationale et les relations entre États: les pays qui exerceront ce contrôle pourront manipuler et «fermer» de manière sélective les services d'IA utilisés par les pays qui en sont dépourvus, comme un instrument de politique étrangère.

62. La deuxième implication concerne le conflit entre des visions concurrentes de la société et des régimes politiques, qui influencent également différents «modèles» de développement de l'IA. Les États-Unis restent à la pointe de la recherche et du développement en matière d'IA, grâce à leur modèle caractérisé par un écosystème d'innovation fondé sur le libre marché et la concurrence, dans lequel opèrent leurs géants technologiques. La Chine, quant à elle, rattrape son retard grâce à son système de planification centralisée par un parti unique, et elle est en train de façonner un modèle dans lequel la forte présence du gouvernement central dans la vie des citoyens se reflète dans le développement et le déploiement de systèmes et d'outils d'IA.

63. À son tour, l'UE est critiquée d'être à la traîne en raison de l'importance qu'elle accorde à la réglementation, sur la base de l'argument fallacieux selon lequel la réglementation est un obstacle à l'innovation. Il est important de noter qu'il s'agit là d'une fausse dichotomie: une réglementation appropriée peut faciliter le développement technologique en offrant aux innovateurs un environnement sûr et prévisible. Les véritables défis de l'Europe résident peut-être dans la fragmentation de ses marchés financiers, l'absence d'un marché numérique unique, des lois punitives en matière de faillite et une aversion accrue pour le risque, qui contribuent tous à réduire les incitations à la création d'un écosystème d'innovation, en particulier pour les start-ups [43].

---

40. www.coe.int/fr/web/anti-human-trafficking/-/high-level-conference-in-malta-puts-ai-at-the-centre-of-anti-trafficking-strategies.
41. OCDE Gouverner avec l'intelligence artificielle: État des lieux et perspectives pour les fonctions essentielles de l'État, OCDE Publishing Paris, 2025.
42. www.politico.eu/article/albania-apppoints-worlds-first-virtual-minister-edi-rama-diella/.

64. Le «modèle de l'UE» met toutefois particulièrement l'accent sur les droits numériques et s'efforce de projeter un leadership normatif à l'échelle mondiale, afin de façonner les normes réglementaires internationales (ce que l'on appelle «l'effet Bruxelles»).

65. La pertinence de l'IA en tant qu'atout géopolitique réside donc dans sa capacité à remodeler les relations de pouvoir, les normes internationales et l'existence même de la démocratie. Elle représente également un domaine de concurrence idéologique, les régimes autoritaires et les pays démocratiques se disputant la prévalence de leurs systèmes d'IA, qui intégreront à leur tour différents ensembles de valeurs.

66. De plus, la concentration du contrôle des technologies d'IA entre les mains d'un petit nombre de géants technologiques, qui disposent de ressources financières supérieures à celles de nombreux États, est préoccupante pour deux raisons. Premièrement, le déséquilibre des pouvoirs entre les entreprises privées et les pays disposant de moins de ressources est important et a des implications géopolitiques. Deuxièmement, la nature transnationale de ces entreprises rend plus difficile la garantie de leur responsabilité.

67. Un exemple récent est le cas du modèle de cybersécurité Mythos d'Anthropic, dont la diffusion a été limitée à un certain nombre d'entreprises et d'organisations technologiques: alors que ce modèle semble surpasser les humains dans l'identification des vulnérabilités cybernétiques, les entreprises et même les organismes gouvernementaux qui n'y ont pas accès se retrouvent désavantagés. Une préoccupation supplémentaire est soulevée par le fait qu'une telle technologie, entre les mains d'un acteur malveillant, peut également devenir une menace.

68. En outre, certains observateurs indiquent que la commercialisation rapide des produits afin d'assurer un retour rapide sur les investissements actuels représente un risque majeur pour 2026. Cela pourrait conduire certaines entreprises à déployer des outils d'IA qui n'ont pas encore été correctement testés[44].

69. Enfin, il convient de noter qu'un pays capable de mettre au point une IA générale ou une super-IA représenterait une menace sans précédent pour ses rivaux. Cela pourrait finalement conduire à la mise en place de cadres de dissuasion de type «Mutual Assured AI Malfunction» (similaires au cadre de dissuasion «Mutual Assured Destruction» qui a assuré la stabilité pendant l'ère nucléaire)[45]. Pire encore, une super-IA pourrait être impossible à contrôler, avec des conséquences difficiles à imaginer à ce stade. Une solution possible pourrait être de suivre le modèle des traités nucléaires[46].

70. En septembre 2025, l'initiative «AI Red Lines» a été lancée, mettant en garde contre le fait qu'il pourrait devenir de plus en plus difficile d'exercer un contrôle humain significatif sur des systèmes d'IA non réglementés dans les années à venir, et exhortant les gouvernements à «parvenir à un accord politique international sur des lignes rouges pour l'IA – en veillant à ce qu'elles soient opérationnelles, avec des mécanismes d'application robustes – d'ici la fin de l'année 2026»[47].

71. De même, une déclaration sur la superintelligence a été publiée en octobre 2025, recueillant les signatures de centaines de personnalités publiques, appelant «à l'interdiction du développement de la superintelligence, qui ne sera levée qu'après un large consensus scientifique sur sa mise en œuvre sûre et contrôlée, et une forte adhésion du public»[48].

6. Efforts internationaux actuels

72. Bien que les progrès technologiques aient un impact mondial, les réglementations qui les régissent dépassent rarement les frontières nationales. Cela souligne la nécessité de renforcer la coopération internationale entre les différentes parties prenantes.

---

43. A. Bradford, "The False Choice Between Digital Regulation and Innovation" (7 March, 2024). Northwestern University Law Review, Vol. 118, Issue 2, 6 octobre, 2024
44. Eurasia Group, Top Risks 2026.
45. https://time.com/7265056/nuclear-level-risk-of-superintelligent-ai/.
46. www.ft.com/content/767d1feb-2c6a-4385-b091-5c0fc564b4ee.
47. https://red-lines.ai/#call.
48. https://superintelligence-statement.org/fr.

6.1. Conseil de l'Europe

73. Le Conseil de l'Europe contribue à cet effort international de différentes manières. Sa Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit a été ouverte à la signature à Vilnius le 5 septembre 2024 et représente le tout premier traité international juridiquement contraignant dans le domaine de l'IA[49].

74. L'article 4 de la Convention-cadre stipule que les parties signataires adoptent ou maintiennent «des mesures pour veiller à ce que les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle soient cohérentes avec les obligations de protection des droits de l'homme». L'article 5 prévoit que «chaque Partie adopte ou maintient des mesures visant à garantir que les systèmes d'intelligence artificielle ne sont pas utilisés pour porter atteinte à l'intégrité, à l'indépendance et à l'efficacité des institutions et processus démocratiques» et «qui visent à protéger ses processus démocratiques au cours des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle, y compris l'accès équitable et la participation des personnes au débat public, ainsi que leur capacité à se forger librement une opinion».

75. En outre, en novembre 2024, le Comité sur l'intelligence artificielle (CAI) créé par le Comité des ministres du Conseil de l'Europe a adopté la Méthodologie pour l'évaluation des risques et des impacts des systèmes d'intelligence artificielle du point de vue des droits humains, de la démocratie et de l'État de droit (méthodologie HUDERIA)[50], un document d'orientation non contraignant juridiquement destiné à être utilisé par les acteurs publics et privés. Depuis le 1er janvier 2026, les travaux du CAI sont poursuivis par le Comité directeur pour les technologies numériques nouvelles et émergentes (CDNET), nouvellement créé, qui succède au CAI.

76. En novembre 2025, le Comité directeur pour les droits humains a adopté le Manuel sur les droits humains et l'intelligence artificielle, conçu pour aider les responsables gouvernementaux et les responsables politiques des États membres du Conseil de l'Europe à appliquer la Convention européenne des droits de l'homme (STE n° 5), la Charte sociale européenne (révisée) (STE n° 163) et d'autres normes en matière de droits de l'homme à l'utilisation de l'IA[51].

77. En avril 2026, le Comité des ministres du Conseil de l'Europe a adopté la Recommandation CM/Rec(2026)4 sur la sécurité et l'autonomisation en ligne des utilisateurs et des créateurs de contenu, appelant à davantage de transparence, de responsabilité et de contrôle concernant la manière dont les plateformes hébergeant du contenu généré par les utilisateurs conçoivent leurs interfaces et leurs algorithmes, et évaluent et gèrent les risques qu'elles font peser sur les droits humains des utilisateurs et les processus démocratiques[52].

78. Dans l'ensemble, l'IA est considérée comme une question prioritaire transversale par l'Organisation; parmi les autres travaux pertinents, on peut citer la note d'orientation sur les implications de l'intelligence artificielle générative sur la liberté d'expression, adoptée en décembre 2025 par le Comité directeur du Conseil de l'Europe sur les médias et la société de l'information[53].

79. Le Comité d'experts sur la manipulation de l'information et l'ingérence menées depuis l'étranger (PC-FIMI) créé en tant que sous-comité du Comité européen pour les problèmes criminels, a préparé une étude de faisabilité sur l'élaboration éventuelle d'un instrument juridique relatif à la manipulation de l'information et l'ingérence menées depuis l'étranger, y compris la désinformation, présentée lors de la session ministérielle du Comité des ministres à Chişinău (République de Moldova) les 14-15 mai 2026[54].

80. Par ailleurs, le Comité directeur sur la démocratie finalise actuellement un projet d'étude sur les avantages et les risques de l'utilisation de l'intelligence artificielle générative dans le débat public relatif au processus démocratique et sur la maîtrise de l'IA pour la vie démocratique.

81. Le Conseil de l'Europe accorde une attention particulière à la participation des jeunes et de leurs organisations à la gouvernance de l'IA. En avril 2025, il a organisé une réunion consultative qui a abouti à une feuille de route sur l'intelligence artificielle, la politique de la jeunesse et le travail avec les jeunes[55].

---

49. www.coe.int/fr/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
50. www.coe.int/fr/web/portal/-/huderia-new-tool-to-assess-the-impact-of-ai-systems-on-human-rights.
51. www.coe.int/fr/web/cddh-handbook-on-ai-and-hr.
52. https://search.coe.int/cm?i=09125948802b41e8.
53. https://rm.coe.int/cdmsi-2025-15rev-note-dorientation-sur-les-implications-de-lintelligen/488029df81.
54. www.coe.int/fr/web/cdpc/-/the-council-of-europe-s-committee-on-crime-problems-cdpc-holds-its-88th-plenary-meeting-in-strasbourg.
55. www.coe.int/en/web/youth/2026-workshop-ai-and-internet-governance.

82. Le Conseil de l'Europe a également lancé en 2025 le Nouveau pacte démocratique pour l'Europe, afin de promouvoir les solutions efficaces et de trouver de nouvelles réponses au recul de la démocratie sur le continent[56]. L'IA sera au cœur de cet effort, en particulier en ce qui concerne son pilier 3 «Innover pour la démocratie», qui vise à mettre les technologies numériques – y compris l'IA – au service du bien commun, tout en combattant leurs usages abusifs et leurs effets néfastes. Le présent rapport et les autres rapports pertinents actuellement en cours d'élaboration par l'Assemblée apporteront une contribution essentielle.

6.2. Nations Unies

83. Les Nations Unies ont intégré un pacte numérique mondial dans le Pacte pour l'avenir adopté en septembre 2024[57], dans lequel les États membres se sont fixé pour objectif de réduire toutes les fractures numériques et de renforcer la gouvernance internationale de l'IA pour le bien de l'humanité.

84. Dans le cadre du Pacte, les États membres ont également décidé de créer un groupe scientifique international indépendant et multidisciplinaire sur l'intelligence artificielle[58] et de lancer un dialogue mondial sur la gouvernance de l'intelligence artificielle. La première session du dialogue mondial des Nations unies se tiendra en juillet 2026[59].

85. En outre, le Secrétaire Général des Nations Unies a mis en garde, dans un message public, contre les dangers d'une IA non contrôlée pour la démocratie, et a appelé à ce que l'IA serve l'humanité de manière équitable et sûre[60].

86. Différentes agences et entités des Nations Unies travaillent sur l'IA sous différents angles. L'UNESCO[61] s'attaque aux questions liées à l'éthique de l'IA, à l'IA dans l'éducation, à l'égalité des genres et au renforcement des capacités des gouvernements et du pouvoir judiciaire. Elle a également publié un rapport consacré à «l'intelligence artificielle et la démocratie»[62]. L'ONU Femmes accorde également une attention particulière à la dimension de genre dans le domaine de l'IA et a lancé l'année dernière une école dédiée à l'IA qui permet aux participants d'apprendre, de construire et de régir une IA sûre et inclusive sur le plan du genre[63].

6.3. Le G7 et l'Organisation de coopération et de développement économiques (OCDE)

87. Le G7 suit de près les développements en matière d'IA; en particulier, dans le cadre du processus du G7 sur l'IA à Hiroshima, il a élaboré en 2023 des principes directeurs et un code de conduite à l'intention des acteurs de l'IA[64].

88. L'OCDE travaille également de manière intensive sur les questions liées à l'IA; la portée de ses travaux, en particulier en ce qui concerne l'impact de l'IA sur le marché du travail, sera révisée en profondeur dans un rapport spécifique actuellement en cours d'élaboration par l'Assemblée. Il convient toutefois de mentionner que le Conseil de l'OCDE a adopté en 2019 (et modifié en 2024) une recommandation sur l'intelligence artificielle[65]. En outre, l'OCDE coopère avec le Partenariat mondial sur l'IA[66].

6.4. Union européenne (UE)

89. L'UE a pris plusieurs initiatives pertinentes. En 2025, elle a adopté un plan d'action pour le continent de l'IA, visant à développer des technologies d'IA fiables afin de renforcer la compétitivité de l'Europe tout en préservant et en faisant progresser les valeurs démocratiques[67].

---

56. www.coe.int/fr/web/new-democratic-pact-for-europe/home.
57. UN, Pacte numérique mondial, 2024.
58. /www.un.org/independent-international-scientific-panel-ai/en.
59. www.un.org/global-dialogue-ai-governance/en.
60. https://news.un.org/en/story/2024/09/1154316.
61. www.unesco.org/fr/artificial-intelligence.
62. www.unesco.org/en/articles/artificial-intelligence-and-democracy.
63. https://asiapacific.unwomen.org/en/partnerships/ai-school.
64. www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html.
65. https://legalinstruments.oecd.org/fr/instruments/oecd-legal-0449.
66. https://oecd.ai/fr/.
67. https://digital-strategy.ec.europa.eu/fr/policies/european-approach-artificial-intelligence.

90. En 2024, elle a adopté le règlement (UE) 2024/1689 établissant des règles harmonisées en matière d'intelligence artificielle (législation sur l'IA)[68], qui définit une approche fondée sur les risques pour les développeurs et les déployeurs d'IA concernant des utilisations spécifiques de l'IA, en définissant quatre niveaux de risques pour les systèmes d'IA: inacceptable, élevé, limité et minimal. En particulier, la législation sur l'IA interdit les systèmes d'IA visant à établir des notations sociales, à profiler des individus afin de prédire leur risque de commettre un crime, ou à exploiter les vulnérabilités des personnes pour fausser leur comportement.

91. En outre, l'UE a adopté en 2022 le règlement (UE) 2022/2065 relatif à un marché unique des services numériques (législation sur les services numériques), qui introduit des règles pour les services en ligne utilisés par les citoyens européens dans leur vie quotidienne, notamment les places de marché, les réseaux sociaux, les boutiques d'applications et les plateformes de voyage et d'hébergement en ligne[69].

92. Enfin, l'UE a également lancé en novembre 2025 l'initiative «Bouclier européen de la démocratie», qui comprend une série de mesures concrètes visant à renforcer, protéger et promouvoir des démocraties solides et résilientes dans toute l'UE[70].

6.5. Autres initiatives

93. Parmi les autres initiatives pertinentes, citons le Sommet sur la sécurité de l'IA, qui s'est tenu à Bletchley (Royaume-Uni) en novembre 2023[71], le Sommet d'action sur l'IA de Paris, qui s'est tenu en février 2025[72], et le Sommet sur l'impact de l'IA, qui s'est tenu à New Delhi en février 2026[73].

94. En novembre 2024, les instituts de sécurité de l'IA et les organismes mandatés par les gouvernements chargés de faciliter la sécurité et l'évaluation de l'IA de la Commission européenne, de la France, du Royaume-Uni ainsi que du Canada, du Japon et des États-Unis, entre autres pays, ont lancé le Réseau international des instituts de sécurité de l'IA. L'objectif est de faciliter une compréhension technique commune des risques liés à la sécurité de l'IA et des mesures d'atténuation, et d'encourager une compréhension générale et une approche de la sécurité de l'IA à l'échelle mondiale[74].

95. En outre, l'Organisation internationale de normalisation (ISO) a créé en 2017 le sous-comité de normalisation «ISO/IEC JTC1/SC 42 Intelligence artificielle», axé sur l'ensemble de l'écosystème de l'IA, afin de permettre le déploiement et l'adoption à grande échelle de l'IA dans un grand nombre de domaines[75].

96. Enfin, il convient également de mentionner la cartographie des initiatives d'intérêt public utilisant l'IA pour soutenir la gouvernance démocratique en ligne, préparée par l'organisation civique de technologie Make.org[76].

7. Conclusions

97. En 1955, Isaac Asimov a publié la nouvelle «Franchise», qui imaginait un avenir dans lequel les États-Unis étaient devenus une «démocratie électronique». Dans cet avenir, un superordinateur sélectionnait une seule personne pour représenter l'ensemble de l'électorat et répondre à une série de questions. La machine utilisait ensuite ces réponses pour déterminer les résultats des élections. «Les ordinateurs sont devenus de plus en plus grands, de sorte qu'ils ont réussi à estimer, d'après un nombre de votes de plus en plus restreint, quel serait le résultat de l'élection. Et puis, en fin de compte, on a fabriqué Multivac, qui est capable de le déterminer d'après un seul votant». Bien que ce scénario inquiétant semble actuellement relever du domaine de la science-fiction, il convient de noter qu'en septembre 2025, un nouveau parti politique japonais a désigné l'IA comme son leader[77].

---

68. https://digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai.
69. https://digital-strategy.ec.europa.eu/fr/policies/digital-services-act.
70. https://ec.europa.eu/commission/presscorner/detail/fr/ip_25_2660.
71. https://www.gov.uk/government/topical-events/ai-safety-summit-2023.
72. https://www.elysee.fr/sommet-pour-l-action-sur-l-ia.
73. https://www.mea.gov.in/bilateral-documents.htm?dtl/40809v.
74. https://digital-strategy.ec.europa.eu/fr/news/first-meeting-international-network-ai-safety-institutes.
75. https://jtc1info.org/technology/subcommittees/ai/.
76. https://docs.google.com/document/u/0/d/1h5CwhLn6-et5Wvy08_DvfFxqVaDsDBfs8IhU-zO5MhU/mobilebasic?pli=1.
77. https://www.japantimes.co.jp/news/2025/09/16/japan/ai-leader-path-to-rebirth-party/.

98. Parallèlement, les dernières avancées en matière de technologie numérique et d'IA constituent une menace très réelle pour les institutions et les processus démocratiques, et exigent une action immédiate de la part des États membres et observateurs du Conseil de l'Europe.

99. Bien que la transition numérique puisse apporter de nombreux avantages à l'humanité, les risques pour la démocratie ne peuvent être sous-estimés. Le Conseil de l'Europe fait figure de pionnier: sa Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit est le tout premier traité juridiquement contraignant dans ce domaine.

100. Cela n'est toutefois pas suffisant. Les États membres et observateurs doivent adopter des mesures visant à garantir le maintien d'un contrôle démocratique tout au long du cycle de vie de tous les systèmes d'IA, du développement au déploiement, afin de préserver la dignité humaine, la transparence et la responsabilité. Cela doit se faire en collaboration avec toutes les parties prenantes concernées, à commencer par les acteurs privés opérant dans le domaine de l'IA, afin de garantir que les systèmes d'IA soient véritablement centrés sur l'humain et qu'ils autonomisent les humains sans les remplacer.

101. Les initiatives visant à lutter contre l'ingérence étrangère et à renforcer la résilience face à la désinformation devraient être prioritaires.

102. Les développeurs et les fournisseurs d'IA, ainsi que les plateformes de réseaux sociaux, devraient être tenus responsables de tout préjudice causé par leurs services, et les victimes devraient avoir accès à des voies de recours.

103. Il est tout aussi important de consacrer des ressources suffisantes à l'éducation aux médias et à l'IA, et d'associer toutes les parties prenantes concernées à l'élaboration de nouvelles normes et réglementations.

104. Les États membres devraient s'efforcer de définir des cadres clairs pour leurs relations avec les grandes entreprises technologiques, tout en prenant des mesures pour renforcer la souveraineté numérique européenne.

105. Un organisme multilatéral dédié exclusivement à la supervision des technologies d'IA pourrait être créé, afin de définir un langage commun, des normes et un cadre réglementaire, en associant toutes les parties prenantes concernées.

106. En fin de compte, il est important de reconnaître que les technologies d'IA peuvent également constituer un outil puissant pour renforcer la sécurité démocratique en Europe. Les États membres doivent être prêts à saisir cette opportunité et à profiter des avantages qui en découlent, tout en veillant à ce que des cadres de gouvernance appropriés soient en place.