

Résolution 2662 (2026)¹

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

Assemblée parlementaire

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

1. *Discussion par l'Assemblée* le 24 juin 2026 (23^e et 24^e séances) (voir [Doc. 16417](#), rapport de la commission des questions politiques et de la démocratie, rapporteure: Mme Deborah Bergamini). *Texte adopté par l'Assemblée* le 24 juin 2026 (24^e séance).

Version provisoire sous réserve de révision éditoriale.



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 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 (*pre-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;

17.15. à veiller à ce qu'il n'y ait pas d'écart de protection entre les approches de réglementation de l'IA et les approches de réglementation des plateformes en ligne en ce qui concerne l'intégration croissante des outils d'IA générative dans les plateformes de médias sociaux et les moteurs de recherche, ainsi que l'utilisation de plus en plus répandue, de fait, des outils d'IA générative en tant que moteurs de recherche.

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;

18.4. à garantir la mise en œuvre cohérente et effective de la Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit en renforçant les efforts de coordination entre les États signataires.

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 reconnaître que la mise en place de technologies et d'infrastructures européennes stratégiques en matière d'IA est essentielle pour la sécurité démocratique et l'autonomie du continent, et prendre des mesures concrètes pour éviter toute dépendance technologique unilatérale vis-à-vis de prestataires étrangers ou privés, tout en garantissant un accès sûr et équitable, en particulier pour les petits États membres, les instituts de recherche d'intérêt public et les petites et moyennes entreprises;

19.6. 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;

19.7. 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.