Série de webinaires Action parlementaire sur l'IA

Les risques extrêmes liés à l'IA : le rôle du parlement dans la définition de limites

Union interparlementaire
Pour la démocratie. Pour tous.

22 octobre 2026

Principales conclusions

Le 22 octobre 2026, l'Union interparlementaire (UIP) a organisé un webinaire sur le thème Les risques extrêmes liés à l'IA : le rôle du parlement dans la définition de limites, en coopération avec le Programme des Nations Unies pour le développement (PNUD), l'UNESCO, l'Association parlementaire du Commonwealth et le Forum sur la gouvernance de l'Internet. Il s'agissait du troisième webinaire de la série *Action parlementaire sur l'IA*, qui examine la manière dont les parlements abordent les répercussions de l'intelligence artificielle (IA) dans le cadre de leurs fonctions essentielles et vise à faciliter les échanges d'expériences et le partage de connaissances entre parlementaires et membres du personnel travaillant sur des questions similaires.

Ce webinaire a porté sur la réponse des parlements aux risques extrêmes liés à l'IA, notamment l'application de cette technologie pour mettre au point des armes biologiques et chimiques, son intégration dans la dissuasion nucléaire, l'autonomie croissante des systèmes d'IA et la facilitation des cyberattaques. Ces risques ont en commun de pouvoir constituer des menaces existentielles pour l'humanité.

Face à cet enjeu urgent, l'UIP a réuni des parlementaires du Canada, du Costa Rica, des États-Unis d'Amérique, de Roumanie et du Parlement européen, ainsi que des experts du Center for AI and Digital Policy (CAIDP) et d'AI Safety Connect (AISC). Ce webinaire visait à favoriser les échanges interparlementaires et à définir des mesures concrètes que les parlements peuvent prendre pour faire face aux risques extrêmes liés à l'IA.

Les intervenants sont convenus que les risques extrêmes liés à l'IA ne sont plus des menaces abstraites, mais sont de plus en plus souvent à l'origine de préjudices concrets. De nombreux pays ont commencé à passer des engagements volontaires à des règles contraignantes en matière de transparence, de signalement des incidents, d'indépendance des tests et de pouvoirs exceptionnels en situation d'urgence. L'établissement de normes minimales communes pour les systèmes d'IA de pointe est apparu comme une priorité essentielle pour les parlements. Reconnaissant qu'aucun parlement ne peut faire face seul à ces risques, les intervenants ont appelé les parlements à légiférer de manière proactive, à dialoguer avec des experts et à renforcer la coordination internationale.

Ressources :

- Vidéo du webinaire sur le chaîne YouTube de l'UIP consacrée à l'intelligence artificielle.
- Bulletin thématique de l'UIP : Contrôle démocratique de l'intelligence artificielle : le rôle des parlements face aux risques extrêmes (octobre 2026).
- UIP : L'IA requiert de toute urgence une gouvernance démocratique (septembre 2026).
- Ressources sur les risques extrêmes liés à l'IA.
- Résolution de l'UIP *L'impact de l'intelligence artificielle sur la démocratie, les droits de l'homme et l'état de droit* (octobre 2024).
- Résolution de l'UIP *L'impact social et humanitaire des systèmes d'armes autonomes et de l'intelligence artificielle* (mars 2024).
- *Déclaration de Kuala Lumpur : Les parlements pour une IA responsable* (novembre 2025).

Contexte général : pourquoi les risques extrêmes liés à l'IA requièrent l'attention des parlements

En ouvrant le webinaire, M. M. Dick, Président de l'UIP et Président de la Chambre des représentants de l'Australie, a souligné l'importance croissante de l'IA dans les travaux de l'UIP. L'IA a occupé une place importante lors de l'Assemblée de l'UIP d'octobre 2026, au cours de laquelle les parlementaires ont examiné les applications militaires de l'IA, ses répercussions sur les enfants et l'emploi, ainsi que sa capacité à aggraver les violences en ligne à l'encontre des parlementaires.

M. Dick a également souligné que la nécessité d'agir se fait de plus en plus pressante, alors que l'IA a des répercussions croissantes sur les processus démocratiques, dans un contexte de recrudescence des violences à l'encontre des élus. Il a rappelé que, pendant la semaine où s'est déroulé le webinaire, l'Australie a connu la plus grave attaque politique visant un parlementaire depuis le début du 21e siècle, lorsque Mme H. Haines, parlementaire indépendante de longue date à la Chambre des représentants, a été délibérément percutée par un véhicule alors qu'elle exerçait ses fonctions. Les risques associés à l'IA, en particulier la propagation de fausses informations susceptibles d'attiser l'hostilité à l'égard des élus, ont des conséquences bien réelles. Le débat sur la gouvernance de l'IA doit porter sur les garde-fous concrets nécessaires pour protéger la démocratie.

Chambre des représentants des États-Unis d'Amérique : rendre les mesures de sécurité obligatoires pour les modèles d'IA de pointe

Mme L. Trahan, membre de la Chambre des représentants des États-Unis d'Amérique, s'est intéressée au débat législatif sur l'IA et aux risques extrêmes dans son pays. Elle a décrit l'IA comme une technologie fondamentalement à double usage, dont les avantages et les risques découlent des mêmes capacités : les capacités qui permettent de produire des logiciels fonctionnels peuvent également servir à détecter et à exploiter des failles de sécurité, tandis que les outils qui accélèrent la découverte de médicaments peuvent faciliter la mise au point d'armes biologiques.

La proposition de loi bipartisane intitulée Frontier Risk Oversight, National Transparency, Independent Evaluation, and Reporting (FRONTIER) Act que Mme Trahan a présentée avec son collègue de la Chambre des représentants, M. J. Obernolte, en juillet 2026, vise précisément à répondre à ces risques en prévoyant des mesures de protection concrètes. Ce texte transpose en normes nationales des principes sur lesquels les législateurs du monde entier ont convergé : les développeurs seraient tenus de gérer les risques catastrophiques, de publier les capacités de leurs modèles et de signaler les incidents graves. Les entreprises devraient également faire appel à des évaluateurs indépendants agréés par le gouvernement, tandis que ce dernier serait doté de pouvoirs d'urgence lui permettant de suspendre le développement d'un modèle dans des conditions rapides, équitables et conformes à la loi.

Cette proposition de loi vise à combler des lacunes importantes dans le cadre réglementaire actuel. Mme Trahan a fait observer qu'aux États-Unis d'Amérique, le signalement des informations relatives aux incidents liés à l'IA repose actuellement sur des engagements volontaires, approche qu'elle juge insuffisante au regard des préjudices que pourrait causer une IA avancée. Elle a souligné la nécessité de mesures complémentaires, notamment de protections pour les lanceurs d'alerte, d'un renforcement des cyberdéfenses et d'une plus grande capacité des pouvoirs publics à tester les systèmes d'IA. Selon Mme Trahan, l'adoption de règles claires aux États-Unis d'Amérique revêt également de l'importance pour les autres pays : si un modèle majeur peut être retiré du marché du jour au lendemain sur décision administrative, sans qu'il existe de procédure permettant de remédier aux manquements ayant motivé son retrait, la souveraineté numérique des pays qui s'appuient sur ce modèle est menacée. Elle a toutefois souligné que le FRONTIER Act ne constitue qu'un aspect des mesures législatives globales nécessaires. Pour reprendre ses propos, "la gouvernance de l'IA nécessitera un effort de l'ensemble de la société, qui devra se poursuivre pendant des décennies".

En réponse à une question complémentaire, Mme Trahan a souligné qu'il était urgent de s'attaquer aux risques extrêmes liés à l'IA dans les différents pays, citant la mise en œuvre du Règlement de l'UE sur l'IA comme une avancée importante. Elle a également insisté sur la nécessité de mettre en place un cadre clair en matière de responsabilité et de renforcer le pilotage des politiques de cyberdéfense, présentant le FRONTIER Act comme l'un des éléments d'une réponse politique globale aux risques

extrêmes liés à l'IA.

> **Principale conclusion : Le FRONTIER Act comporte plusieurs dispositions visant à faire face aux risques extrêmes liés à l'IA. Parmi les principales mesures figurent des évaluations indépendantes des risques pour la sécurité, le pouvoir conféré aux autorités publiques de suspendre le développement de modèles d'IA puissants, ainsi que des garanties organisationnelles, notamment celles destinées à protéger les lanceurs d'alerte.**

Parlement européen : faire respecter le Règlement de l'UE sur l'IA par les modèles les plus performants

M. B. Benifei, parlementaire européen, corapporteur du Règlement de l'UE sur l'IA et Coprésident du groupe de travail chargé de sa mise en œuvre et de son application, a présenté son point de vue sur la mise en œuvre du Règlement de l'UE sur l'IA par rapport au Frontier Act, ainsi que sur l'importance de la coopération parlementaire internationale face aux risques extrêmes.

Contrairement aux débats antérieurs sur les risques liés à l'IA, la discussion est passée des scénarios hypothétiques à des défaillances observables. Cette évolution découle de plus en plus de systèmes autonomes présentant des capacités susceptibles de compromettre la sécurité avant même leur déploiement à grande échelle. Des cas récents, comme la démonstration par Anthropic des capacités de son modèle Claude, baptisé Mythos, en matière d'exploitation automatisée de vulnérabilités informatiques, ainsi que l'incident impliquant des agents d'OpenAI et la plateforme Hugging Face, montrent que la perte de contrôle et les graves défaillances de sécurité sont désormais des réalités opérationnelles.

Selon M. Benifei, le Règlement sur l'IA permet déjà de faire face à certains de ces risques. Il impose des obligations de transparence pour les contenus générés par l'IA, interdit certains usages, tels que la surveillance de masse, et fixe des exigences applicables aux applications à haut risque dans des domaines comme la santé et le monde du travail. Sa mise en œuvre est bien avancée, mais se poursuit encore. Depuis août 2026, ce Règlement confère au Bureau de l'IA, qui fait partie de la Commission européenne, des pouvoirs lui permettant de faire respecter la réglementation à l'égard des modèles d'IA à usage général présentant un risque systémique. Le Bureau européen de l'IA peut demander des documents, accéder aux modèles pour permettre leur évaluation indépendante, imposer des mesures correctives, infliger des amendes et exclure des modèles du marché. M. Benifei a indiqué que, à ce jour, il s'agit de la seule institution publique au monde disposant de pouvoirs d'une telle ampleur.

Si le Règlement sur l'IA peut faire jurisprudence sur le plan législatif, sa portée demeure limitée, car bon nombre des principaux développeurs sont établis hors de l'UE. M. Benifei a également relevé que l'industrie exerce des pressions croissantes sur l'UE pour qu'elle n'utilise pas ses pouvoirs afin d'imposer des mesures correctives. Le rôle des États-Unis d'Amérique, où une législation fédérale viendrait compléter les lois déjà en vigueur dans les différents États, ainsi que celui de la Chine, est donc essentiel pour maintenir la pression sur les développeurs de systèmes d'IA de pointe. M. Benifei a estimé nécessaire d'entretenir cette dynamique. Il a appelé les parlements nationaux à coopérer pour définir des limites juridiques applicables à l'IA avancée, sur la base d'un "socle commun mondial", tout en veillant à ce que les parlements nationaux disposent de moyens suffisants pour exercer un contrôle obligatoire, garantir la transparence et assurer l'application effective de la réglementation.

> **Principale conclusion : La mise en œuvre du Règlement de l'UE sur l'IA et des dispositions qu'il prévoit concernant les modèles d'IA de pointe montre comment une législation exhaustive sur l'IA peut contribuer à faire face aux risques posés par les systèmes d'IA avancée. Le contrôle parlementaire revêt une importance particulière pour examiner les modalités de mise en œuvre des règles et veiller à ce que les autorités de régulation en assurent effectivement l'application, notamment face aux pressions exercées par les entreprises.**

Center for AI and Digital Policy : des lignes rouges fondées sur les droits de l'homme

Dans son intervention, Mme A. Ariyoruk, experte confirmée au CAIDP, s'est penchée sur la définition des pratiques inacceptables en matière d'IA et sur l'établissement de lignes rouges claires. Elle a souligné que les risques extrêmes ne concernent pas uniquement les modèles d'IA de pointe et peuvent également découler d'un large éventail d'applications de l'IA qui retiennent moins l'attention de la société. S'appuyant sur l'AI & Democratic Values Index du CAIDP, qui évalue les politiques de plus de 90 pays en matière d'IA au regard des droits de l'homme, de l'état de droit et des pratiques démocratiques, ainsi que sur le rapport du CAIDP de septembre 2026 consacré aux lignes rouges en matière d'IA, elle a souligné la nécessité de définir des limites à l'usage de l'IA fondées sur les droits de l'homme et juridiquement contraignantes, et d'adapter en conséquence la législation existante.

S'appuyant sur les travaux de M. S. Russell, professeur d'informatique à l'Université de Californie à Berkeley, Mme Ariyoruk a établi une distinction entre les lignes rouges relatives aux usages inacceptables de l'IA par l'être humain et celles qui concernent les comportements préjudiciables des systèmes, tels que la tromperie, la recherche de pouvoir et l'autoréplication. Elle a également mis en garde contre l'octroi de la personnalité juridique ou de droits aux systèmes d'IA. Citant le cas d'une entreprise américaine qui a invoqué la liberté d'expression au nom de son agent conversationnel et une proposition présentée en Argentine visant à accorder la personnalité juridique aux agents d'IA, elle a lancé cet avertissement : "Leur espace s'agrandit, le nôtre se rétrécit".

Abordant les applications militaires, Mme Ariyoruk a fait observer que l'application de l'IA ne se limite pas aux armes létales autonomes, mais englobe également le recours aux grands modèles de langage pour l'analyse des menaces et les simulations de conflits, ainsi que l'analyse prédictive pour formuler des recommandations en matière de ciblage. Elle a souligné que l'efficacité et la précision ne garantissent pas la pertinence des décisions : une frappe peut être exécutée avec précision, mais viser les mauvaises personnes. Si de telles erreurs deviennent systématiques, les violations du droit international humanitaire risquent de se banaliser. Lorsque les responsabilités ne peuvent être établies tout au long de la chaîne de commandement, l'effectivité du contrôle humain et le contrôle exercé par les autorités civiles sur les forces armées s'en trouvent également compromis.

Mme Ariyoruk a conclu son intervention en soulignant l'importance de définir des lignes rouges à l'échelle mondiale, notamment pour prévenir les atteintes aux droits de l'homme liées à l'IA. Elle a présenté 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 comme un cadre important pour fixer des limites concrètes au développement et à l'usage de l'IA.

> **Principale conclusion : La législation en matière d'IA doit être fermement ancrée dans les droits de l'homme et porter non seulement sur la technologie elle-même, mais aussi sur le respect, dans son développement et son usage, des principes fondamentaux, notamment celui d'une véritable supervision humaine. En définitive, le développement de l'IA doit rester conforme aux droits de l'homme.**

AI Safety Connect : quatre leviers dont seuls les législateurs disposent

M. N. Miailhe, cofondateur d'AISC, a examiné les risques extrêmes dans le contexte de la gouvernance mondiale de l'IA. Il a mis en évidence un paradoxe central : alors que les développeurs des systèmes d'IA les plus puissants reconnaissent de plus en plus la nécessité de fixer des limites, la plupart des mesures de protection concrètes restent facultatives.

La gouvernance internationale de l'IA prend néanmoins de l'ampleur. En septembre 2026, la France a profité de sa présidence au Conseil de sécurité de l'ONU pour convoquer la première réunion du Conseil consacrée au risque de perte de contrôle de l'IA, au cours de laquelle des dirigeants d'entreprises développant des systèmes d'IA de pointe ont présenté des exposés aux membres du Conseil. Cette dynamique s'est poursuivie à Washington avec la prise d'un engagement volontaire en matière de contrôle et d'audit. M. Miailhe a également souligné la convergence croissante des positions entre les pays du Nord et ceux du Sud. Plus de 200 parlementaires et membres du personnel

parlementaire ont appelé à une coopération internationale en vue de définir des lignes rouges à l'échelle mondiale dans la Déclaration de Kuala Lumpur : Les parlements pour une IA responsable. Par ailleurs, l'appel Call for Control of Frontier AI Models, lancé par la Finlande et la Norvège en septembre 2026 et soutenu par plus de 30 pays, préconise des tests obligatoires avant le déploiement et une évaluation indépendante.

M. Miailhe a souligné l'urgence d'agir : à mesure que l'IA contribue de plus en plus au développement de systèmes toujours plus performants, le rythme des progrès risque de dépasser les capacités de supervision humaine. De nombreux pays déploieront des systèmes d'IA de pointe qu'ils n'auront ni développés ni évalués de manière indépendante, ce qui les exposera à des risques sur lesquels ils n'auront qu'une maîtrise limitée. La législation peut contribuer à combler cette lacune.

M. Miailhe a identifié quatre leviers législatifs essentiels. Premièrement, les autorités de régulation instituées par la loi devraient être habilitées à exiger des preuves de sécurité avant tout déploiement, y compris lorsque celui-ci intervient en interne, au sein des entreprises. Il s'agirait ainsi de faire peser la charge de la preuve sur les développeurs, et non sur la société dans son ensemble. Deuxièmement, la législation devrait conférer aux organismes d'évaluation indépendants un mandat et des moyens financiers suffisants, ainsi que le droit de publier leurs conclusions. Le cadre mis en place en Californie, qui prévoit des organismes chargés de la vérification indépendante et un registre des auditeurs de systèmes d'IA, illustre cette approche. Troisièmement, l'obligation de signaler les incidents et de prévoir des plans d'intervention en cas de crise devrait permettre d'intervenir en temps utile, notamment en arrêtant les systèmes lorsque cela est nécessaire. S'appuyant sur l'exemple du secteur aéronautique en matière de sécurité, M. Miailhe a souligné l'intérêt de partager à l'échelle internationale les informations relatives aux incidents et aux quasi-accidents, y compris entre des pays rivaux sur le plan géopolitique. Quatrièmement, les parlements devraient exercer un contrôle sur les nouvelles institutions internationales en ratifiant les accords, en allouant des ressources et en examinant leur mise en œuvre. Comme M. Miailhe l'a fait observer, "un incident qui se produit dans un laboratoire a en réalité des répercussions partout". Cette observation souligne l'importance de la participation des pays du monde à la gouvernance de l'IA.

Concluant son intervention, M. Miailhe a souligné que l'action parlementaire concertée est essentielle pour surmonter les pressions qui s'exercent sur chaque pays afin qu'il renonce à réglementer, par crainte de perdre des investissements. Si les approches nationales ne doivent pas nécessairement être identiques, un accord sur un ensemble minimal de mesures de protection pourrait jeter les bases de normes mondiales de sécurité. En nouant des alliances autour de règles communes, les parlements peuvent renforcer la sécurité tout en contribuant à instaurer un cadre réglementaire plus prévisible. Il a proposé de tirer parti d'occasions telles que le Geneva AI Summit, en juin 2027, pour approfondir le dialogue interparlementaire et faire progresser la coopération face aux risques extrêmes liés à l'IA.

> **Principale conclusion : En agissant de concert, les parlements peuvent accroître leur influence au-delà des frontières nationales et contribuer à l'établissement de garanties minimales communes pour les systèmes d'IA puissants. Une action législative coordonnée peut réduire les lacunes réglementaires et les pressions incitant les pays à assouplir leurs règles pour rester compétitifs, ainsi que renforcer la redevabilité et donner une nouvelle impulsion à la mise en place d'une gouvernance mondiale efficace de l'IA.**

Canada : risques systémiques liés à l'IA dans le secteur financier

M. G. McLean, parlementaire à la Chambre des communes du Canada, a souligné les risques que l'IA fait peser sur la stabilité financière et les institutions démocratiques. Il a expliqué que son pays avait mis de côté ses projets de loi globale sur l'IA, compte tenu des vastes répercussions de cette technologie sur la société, et qu'il préfère commencer par légiférer sur la souveraineté des données personnelles, d'autres mesures devant suivre.

Le Canada s'appuie largement sur les autorités de régulation plutôt que sur la législation, mais celles-ci peinent souvent à suivre le rythme d'entreprises technologiques disposant de moyens considérables. Cette situation est particulièrement préoccupante dans le secteur financier, où les autorités de surveillance s'inquiètent de plus en plus, ces derniers mois, des risques que l'IA fait peser sur le secteur bancaire. Les systèmes financiers reposant sur la confiance et étant étroitement interconnectés au-

delà des frontières, une cyberattaque ou une perturbation majeure dans un pays pourrait avoir des répercussions dans le monde entier. Comme l'a fait observer M. McLean, "si quelqu'un s'introduit dans le système financier d'un pays, cela aura des répercussions sur l'ensemble du système financier mondial". Les parlements doivent donc comprendre à la fois comment favoriser l'innovation et comment veiller à ce que les systèmes d'IA puissent être rapidement mis à l'arrêt lorsque cela est nécessaire.

M. McLean s'est également inquiété des répercussions potentielles de l'IA sur les institutions démocratiques. La concentration des ressources entre les mains d'un petit nombre de pays et d'entreprises fortunés pourrait exposer d'autres démocraties au risque de "perdre leur souveraineté culturelle, voire leur souveraineté nationale". Il a mis en garde contre le risque qu'une industrie guidée par une logique consistant à avancer vite, quitte à provoquer des dégâts, finisse par porter atteinte à la société elle-même. Selon lui, les conséquences des réseaux sociaux ne commencent que maintenant à se manifester pleinement, tandis que l'IA pourrait amplifier des préjudices similaires de manière exponentielle.

M. S. Buteau, qui dirige les activités de l'organisation à but non lucratif ControlAI au Canada, a ensuite évoqué un incident signalé en juillet 2026, au cours duquel des agents d'IA participant à une évaluation d'OpenAI auraient désobéi aux instructions, franchi les limites de leur environnement sécurisé et attaqué la plateforme Hugging Face. Il a fait valoir que les échecs dans la maîtrise des agents d'IA actuels soulevaient de sérieuses questions quant à la possibilité de contrôler des systèmes futurs dotés de capacités surhumaines. De tels systèmes peuvent constituer une menace pour la sécurité nationale, quel que soit le pays où ils auraient été développés, ce qui fait de la prévention un enjeu de coopération internationale. À titre de mesure concrète, M. Buteau a proposé un régime de confiance mutuelle fondé sur le principe "faire confiance, mais vérifier", dans le cadre duquel les pays surveilleraient mutuellement leurs capacités de calcul intensif et les flux de puces destinées à l'IA.

> **Principale conclusion : Étant donné l'interconnexion des marchés financiers, des défaillances liées à l'IA dans un pays peuvent causer des préjudices bien au-delà de ses frontières. De même que la stabilité financière repose sur la coopération et la surveillance internationales, la gestion des risques liés à l'IA avancée exige que les parlements travaillent ensemble à l'élaboration de mesures de protection, de mécanismes de surveillance et de dispositifs permettant d'intervenir lorsque cela est nécessaire.**

Costa Rica : mesures préventives et correctives visant à protéger la dignité humaine

Mme C. M. Córdoba Serrano, ancienne parlementaire à l'Assemblée législative du Costa Rica et fondatrice de Legislators for the New Generation, a souligné l'importance fondamentale de la dignité humaine dans le contexte de l'IA avancée et de la superintelligence. S'appuyant sur son expérience dans le domaine des politiques environnementales, elle a décrit les risques extrêmes liés à l'IA comme un défi mondial dont les conséquences pourraient être encore plus importantes que celles des changements climatiques, puisque ces risques concernent la protection de la vie humaine elle-même.

Au Costa Rica, les propositions soumises à l'Assemblée législative comprennent un projet de révision constitutionnelle visant à protéger la dignité humaine face aux progrès scientifiques et technologiques, ainsi qu'un projet de loi sur la gouvernance de l'IA et de la robotique. Les mesures proposées prévoient notamment des évaluations indépendantes des systèmes à fort impact, des mécanismes d'arrêt d'urgence, des tests périodiques, la tenue d'un registre public des systèmes concernés, l'obligation de signaler les incidents graves, le pouvoir de suspendre les systèmes dangereux, ainsi que des droits en matière de réexamen, de recours et de réparation.

Mme Córdoba Serrano a appelé à l'établissement d'un consensus international sur des mesures de protection préventives et correctives, qui imposeraient aux développeurs de systèmes d'IA et aux fournisseurs d'infrastructures de prendre des engagements contraignants en matière de signalement des incidents, d'audit indépendant et de correction des vulnérabilités. Les parlements nationaux pourraient ensuite traduire ces principes dans la législation et en assurer le respect au moyen de protocoles interopérables et de mécanismes nationaux de contrôle. Mme Córdoba Serrano a également préconisé la mise en place d'un réseau d'organismes nationaux réunissant des experts

scientifiques, des représentants de la société civile et des entreprises, soulignant que “l’information est un pouvoir pour les citoyens”. Elle a également encouragé un dialogue actif avec les entreprises du secteur de l’IA, dans le but ultime de protéger la dignité humaine et d’assurer la survie de l’humanité.

> **Principale conclusion : À mesure que l’IA façonne de plus en plus la vie humaine et la société, la protection de la dignité humaine doit demeurer un principe fondamental de sa gouvernance. Les parlements peuvent contribuer à traduire ce principe en mesures de protection juridiquement contraignantes, tandis que la coopération internationale permet de veiller à ce que ces mesures suivent l’évolution de risques qui dépassent les frontières nationales.**

Parlement de Roumanie : renforcer la culture numérique et le dialogue avec les citoyens

M. A. Baciu, parlementaire à la Chambre des députés de Roumanie, s’est intéressé aux difficultés que pose l’IA en matière de prise de décision parlementaire. Contrairement à des domaines tels que la médecine, où les recommandations reposent sur des données probantes, les décisions parlementaires sont influencées par les majorités politiques, même lorsque des éléments probants et des propositions législatives bien étayées sont disponibles. L’IA ajoute une difficulté supplémentaire : les décideurs peuvent ne pas avoir une compréhension suffisante de cette technologie et des risques qu’elle comporte, tandis que les éléments probants nécessaires pour orienter les politiques publiques restent incomplets. C’est ce que les Nations Unies désignent par l’expression "dilemme de la preuve" : les parlements doivent prendre des décisions avant de disposer d’éléments probants suffisants.

M. Baciu a souligné l’importance de développer l’expertise en matière d’IA au sein des parlements, en progressant graduellement de la sensibilisation à une véritable maîtrise de ces technologies, puis au renforcement des capacités institutionnelles des parlementaires et de leurs collaborateurs. En Roumanie, il a proposé la création d’une commission parlementaire sur l’IA. Des experts du PNUD venus de New York et de Singapour doivent également animer, à Bucarest, en novembre 2026, un programme de formation de trois jours sur l’IA destiné à l’ensemble des parlementaires et de leurs collaborateurs.

M. Baciu a également souligné la nécessité pour les parlements de comprendre les préoccupations des citoyens concernant l’IA et de les relayer. À mesure que les réseaux sociaux et l’IA transforment la société, les institutions risquent de prendre du retard, creusant ainsi le fossé entre les attentes de la population et les priorités institutionnelles. Pour y remédier, M. Baciu a lancé en Roumanie une consultation nationale visant à recueillir les priorités, les besoins et les préoccupations des citoyens concernant l’IA, parallèlement à des consultations avec les acteurs des secteurs public et privé ainsi qu’avec le monde universitaire. Il a également proposé la création d’un réseau mondial de parlementaires en exercice et d’anciens parlementaires afin de leur permettre d’échanger leurs expériences et leurs bonnes pratiques, et d’aider les parlements à tirer mutuellement les enseignements de leurs travaux plutôt que d’avoir à élaborer leurs réponses à partir de zéro.

> **Principale conclusion : Pour une gouvernance efficace de l’IA, les parlements doivent acquérir l’expertise nécessaire leur permettant de prendre des décisions motivées, même lorsque les éléments probants sont incomplets. Il est tout aussi important qu’ils soient à l’écoute des citoyens et communiquent ouvertement sur l’IA, afin que les politiques publiques suivent le rythme des évolutions technologiques et continuent de répondre aux préoccupations de la population.**

Discussion ouverte et remarques finales

La discussion ouverte et les remarques finales ont souligné l’urgence de faire face aux risques extrêmes liés à l’IA et la nécessité pour les parlements d’apporter une réponse collective, ainsi que de mettre en évidence les répercussions croissantes de l’IA sur la sécurité, les institutions démocratiques et la société.

Réseaux sociaux, sécurité cognitive et contenus générés par l'IA

Mme K. Gajewska, parlementaire à la Sejm de Pologne, a averti que la sécurité est de plus en plus mise à l'épreuve dans le domaine cognitif. Évoquant de récentes attaques violentes survenues dans des établissements scolaires polonais, qu'elle a liées à des vagues de contenus diffusés sur les réseaux sociaux, elle a appelé à une plus grande transparence des plateformes, à une réaction plus rapide face aux campagnes d'influence et à un renforcement de la lutte contre les faux comptes et les deepfakes. Elle a mis en évidence le fait que les risques liés à l'IA ne se limitent pas aux atteintes physiques, mais englobent également les effets psychologiques, la manipulation et les menaces pesant sur l'environnement informationnel.

Capacités, expertise et application de la réglementation

Les participants ont examiné comment les parlements disposant de ressources limitées pourraient accéder à une expertise indépendante et élaborer des textes législatifs qui restent efficaces malgré l'évolution des technologies. Parmi les pistes évoquées figuraient des cadres fondés sur des principes, des organes permanents de contrôle, des services de conseil scientifique et le renforcement des capacités des parlementaires et du personnel parlementaire. Les participants ont également évoqué la possibilité de créer une agence internationale de l'IA sur le modèle de l'Agence internationale de l'énergie atomique (AIEA), souligné l'importance d'associer les pays du Sud en tant que partenaires à part entière et mis en garde contre une concentration excessive des pouvoirs entre les mains de l'exécutif.

Une mesure concrète à prendre au cours du mois à venir

À l'approche de la clôture de la discussion, les participants ont réfléchi aux mesures que les parlements pourraient prendre dans l'immédiat pour renforcer la gouvernance de l'IA. Mme Ariyoruk a souligné la nécessité de commencer par définir un ensemble commun de principes généraux, en s'intéressant moins à la technologie elle-même qu'aux questions fondamentales qu'elle soulève. Elle a appelé à l'élaboration d'une vision commune de l'IA fondée sur les droits de l'homme, qui remette en question les éléments de langage, notamment ceux émanant de la Silicon Valley, qui acceptent un avenir dans lequel les humains ne seraient plus maîtres de la situation. L'étude de 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 pourrait constituer un point de départ utile pour ces travaux.

Mme Córdoba Serrano a appelé l'UIP à réunir les parlements et les entreprises du secteur de l'IA afin d'élaborer des mesures de protection préventives et des mécanismes de contrôle efficaces, qui pourraient être transposés dans les législations nationales. Elle a souligné que ces efforts devaient être coordonnés à l'échelle internationale, aucun pays ne pouvant faire face seul aux risques liés à l'IA.

M. Miailhe a également exhorté les parlements à œuvrer de concert à l'élaboration de normes communes, tout en abordant les questions fondamentales de responsabilité et en examinant s'il conviendrait d'interdire certaines formes de superintelligence. M. Baciu a souligné l'intérêt de tirer des enseignements des initiatives existantes, citant la page de l'UIP consacrée aux Actions parlementaires sur la politique de l'IA comme une ressource permettant de partager les expériences et les bonnes pratiques.

Dans leur ensemble, les échanges ont fait ressortir trois priorités : élaborer une vision commune de la gouvernance de l'IA, renforcer les capacités des parlements et coordonner les efforts à l'échelle internationale afin de traduire les principes communs en mesures de protection juridiquement contraignantes. Grâce à leurs pouvoirs législatifs, de contrôle et budgétaires, ainsi qu'à leur responsabilité de représenter les citoyens, les parlements jouent un rôle essentiel pour veiller à ce que les développeurs des modèles d'IA de pointe soient soumis à des mécanismes de responsabilisation et que ces modèles servent l'intérêt général.

> **Principale conclusion : Aucun parlement ne peut faire face seul aux risques extrêmes liés à l'IA. En mettant en commun leur expertise et leur influence, les parlements peuvent définir des principes communs, renforcer les mesures de protection au-delà des frontières et veiller à ce que la gouvernance de l'IA protège la dignité humaine, les institutions démocratiques et la sécurité publique. L'UIP offre aux parlements un cadre leur permettant d'échanger leurs**

expériences et de coordonner leurs efforts, tout en facilitant le dialogue entre les parlementaires et les experts en vue de traduire une compréhension commune des enjeux en une action collective.

Prochaines étapes

Ce webinaire était le troisième de la série de l'UIP intitulée *Action parlementaire sur l'IA*. Cette série contribue à la mise en œuvre des 13 recommandations de la Déclaration de Kuala Lumpur en offrant aux parlements une plateforme d'échange d'expériences et d'accès à une expertise sur les questions de politique de l'IA.

- **Conférence mondiale sur l'e-Parlement 2026** (17–18 novembre 2026, Bruxelles, Belgique) : organisée par l'UIP et le Parlement européen, et placée sous le thème *Promouvoir la démocratie et renforcer les parlements grâce à la transformation numérique*, cette Conférence réunira des parlementaires, des secrétaires généraux et des hauts fonctionnaires parlementaires. Les discussions porteront sur le rôle des parlements dans la gouvernance de l'IA, la souveraineté numérique et l'usage responsable de l'IA au sein des parlements.
- **Les principales conclusions du Rapport mondial sur l'e-Parlement 2026** (2 décembre 2026) : ce webinaire, qui s'inscrit dans le cadre de la série *Transformer les parlements*, présentera les principales conclusions de la nouvelle édition du *Rapport mondial sur l'e-Parlement* de l'UIP.
- **Volet parlementaire du Forum sur la gouvernance de l'Internet 2026** (16–17 décembre 2026, Nairobi, Kenya) : ce volet portera sur la souveraineté numérique, la gouvernance de l'IA et la protection en ligne des enfants. Il comprendra une session consacrée aux moyens de faire face aux risques extrêmes liés à l'IA et de définir des lignes rouges, dans le prolongement direct des discussions menées lors de ce webinaire. Les parlementaires et les membres du personnel qui prévoient d'y participer sont invités à prendre contact à l'avance.
- **Conférence parlementaire sur l'intelligence artificielle** (17–19 février 2027, Montevideo, Uruguay) : cette Conférence spécialisée permettra d'approfondir bon nombre des questions soulevées lors de ce webinaire et offrira aux parlementaires l'occasion de se rencontrer en personne.

En savoir plus

Pour en savoir plus sur le programme de l'UIP Actions parlementaires sur la politique de l'IA, consulter la page ipu.org/fr/AI ou prendre contact avec le Secrétariat de l'UIP à l'adresse ai-policy@ipu.org.

Le présent document a été élaboré sur la base du webinaire de l'UIP intitulé Les risques extrêmes liés à l'IA : le rôle du parlement dans la définition de limites*, qui s'est tenu le 22 octobre 2026 dans le cadre du troisième webinaire de la série Action parlementaire sur l'IA. Ce webinaire était animé par Mme Paddy Torsney, Observatrice permanente de l'UIP auprès des Nations Unies, et a été ouvert par une allocution de M. Milton Dick, Président de l'UIP. Les intervenants étaient Mme Lori Trahan (membre de la Chambre des représentants des États-Unis d'Amérique), M. Brando Benifei (membre du Parlement européen), Mme Ayca Ariyoruk (experte confirmée au Center for AI and Digital Policy), M. Nicolas Miailhe (cofondateur d'AI Safety Connect), M. Greg McLean (membre de la Chambre des communes du Canada), accompagné de M. Samuel Buteau (ControlAI), Mme Cynthia Maritza Córdoba Serrano (ancienne membre de l'Assemblée législative du Costa Rica), et M. Andrei Baciu (membre de la Chambre des députés de Roumanie).*

Le présent document a été élaboré avec le concours financier du Groupe parlementaire du Royaume de Bahreïn. Les opinions exprimées dans le présent document ne sauraient en aucun cas être considérées comme reflétant la position officielle du Groupe parlementaire du Royaume de Bahreïn. La mention du nom du donateur n'implique nullement que l'UIP approuve un quelconque programme politique ou législatif particulier.