IVADO

Initiative IA + Société
AI + Society

Quand l'IA s'immisce dans les élections

Quatre actions à mettre en œuvre pour protéger l'intégrité des élections et défendre la démocratie[1]

Catherine Régis, Florian Martin-Bariteau, Jake Okechukwu Effoduh, Juan David Gutiérrez, Gina Neff, Carlos Affonso Souza et Célia Zolynski

Pourquoi la question de l'IA et des élections revêt une importance capitale

Les technologies influencent depuis longtemps les élections, tant positivement que négativement, en façonnant leurs résultats et la qualité du débat public les entourant. Par exemple, Internet permet à la population de se mobiliser plus efficacement que jamais, lui donnant un outil pour défendre des idées et des causes précises. Néanmoins, Internet est également un redoutable canal de désinformation.

L'essor de l'intelligence artificielle (IA) s'accompagne de nouvelles menaces importantes, notamment la multiplication des vidéos hypertruquées, la hausse des risques liés à la cybersécurité, l'émergence d'agents manipulateurs persuasifs ou, encore, la prolifération des données synthétiques et des faux comptes. Dans un même temps, l'IA s'avère un outil puissant qu'utilisent les partis politiques pour communiquer avec l'électorat, influencer l'opinion publique et façonner les flux d'information. En exploitant les tendances électorales existantes, l'IA pourrait profondément remodeler les processus démocratiques et avoir un impact sur les résultats électoraux. Cependant, sans mesures proactives, l'IA pourrait exacerber des tendances inquiétantes comme la polarisation politique et la perte de confiance envers la démocratie.

Les gouvernements doivent agir de manière décisive à l'égard de l'IA, en particulier en cette période où, dans les démocraties du monde, les élections font face à des attaques et à des défis croissants. En agissant sur plusieurs fronts, ils soutiendront les systèmes démocratiques, renforceront la confiance de la population et assureront que l'IA soit utilisée d'une manière qui permet de protéger l'intégrité des élections.

Principaux points à retenir

- Des exemples récents, au Brésil, en Roumanie, au Gabon, aux États-Unis et dans d'autres pays, montrent de quelle manière le recours à l'IA en contexte politique peut porter atteinte à l'intégrité électorale et à la démocratie.
- Souvent, les pays ne sont pas prêts à relever les défis liés à l'IA du fait de l'insuffisance des règles gouvernant l'IA lors d'élections, de mésententes entre les partis politiques sur l'application des pratiques électorales à l'ère de l'IA et de l'incapacité de plusieurs gouvernements à réprimer efficacement les attaques menées contre les institutions démocratiques avec l'IA.
- Nous recommandons quatre mesures : les gouvernements devraient actualiser leurs règles électorales (p. ex. interdire le contenu trompeur généré par l'IA) ; les partis politiques devraient adopter un code de conduite établissant des directives claires quant à une utilisation politique responsable de l'IA ; les autorités électorales devraient mettre en place des équipes indépendantes capables d'intervenir en cas de perturbations découlant de l'usage de l'IA ; et les gouvernements devraient mettre en place un Groupe international de sauvegarde des élections à l'ère de l'IA, ainsi que des protocoles, pour traiter des ingérences transfrontalières.

En quoi l'IA est une menace pour les élections et la démocratie

Les parties prenantes politiques, tant locales qu'étrangères, peuvent utiliser l'IA de diverses façons afin de nuire à l'intégrité des élections et de la démocratie.

Les élections tenues au Brésil en octobre 2024 en sont un exemple. Une étude menée par le Digital Forensic Research Lab a révélé que, six mois avant le jour des élections, les figures politiques locales ou leurs soutiens ont eu recours à l'IA au moins 75 fois pour produire des images, du contenu audio ou des vidéos synthétiques dans le but de mousser leurs candidatures ou d'affaiblir leurs adversaires. Notamment, cinq candidates ont été victimes de pornographie hypertruquée[2], un phénomène dont l'ampleur finit souvent par décourager les femmes d'occuper un rôle public[3].

En décembre 2024, le Service de renseignement extérieur de la Roumanie a signalé que la Russie avait tenté d'influencer son élection présidentielle. La Russie a tout d'abord utilisé du contenu généré par l'IA et de la propagande d'extrême droite prorusse diffusés par un important réseau de canaux de médias sociaux et de comptes générés par l'IA. Elle aurait ensuite utilisé l'IA (qui peut aider à développer des logiciels malveillants qui échappent aux défenses de cybersécurité) pour orchestrer quelque 85 000 attaques contre l'Autorité électorale permanente de la Roumanie afin d'accéder à ses bases de données. Au final, l'interférence russe a mené la Cour constitutionnelle de la Roumanie à annuler le premier tour de l'élection présidentielle[4].

Lors de la campagne électorale tenue au Gabon en 2023, une controverse a éclaté au moment où le pays se préparait à voter dans une triple élection historique — présidentielle, législative et locale. Vers la fin de la campagne, des enregistrements audio ont fait surface sur Internet, suggérant que deux personnalités de l'opposition discutaient de stratégies, d'alliances et de soutien extérieur. Le président sortant a accusé l'opposition de « fomenter un soulèvement populaire », tandis que la coalition d'opposition a condamné les enregistrements comme une « utilisation infâme de l'IA ». Le cas du Gabon montre comment le recours accru aux outils d'IA complique le débat public et fait en sorte qu'il est de plus en plus difficile pour l'électorat de distinguer la réalité de la fiction[5].

Enfin, les principaux modèles d'IA utilisés durant la campagne électorale présidentielle états-unienne de 2024 ont été testés afin de déterminer dans quelle mesure ils produisaient des informations exactes à propos de cette élection. Ces tests ont révélé des incohérences entre les informations rapportées dans différentes langues et entre, d'une part, les engagements énoncés par les entreprises d'IA en matière d'exactitude des informations électorales et, d'autre part, les performances réelles de leurs modèles[6].

Ces exemples illustrent que les pays et les gouvernements sont souvent mal préparés à relever les défis qu'entraîne l'utilisation croissante de l'IA. Nous proposons certaines actions pour éviter ou atténuer les effets néfastes de cette technologie sur les élections.

Les élections locales sont particulièrement vulnérables à l'influence de l'IA. À cette échelle, les ressources et les protections nécessaires pour contrer efficacement ses impacts sont souvent manquantes.

Premier défi
Plusieurs gouvernements n'ont toujours pas adopté de règles gouvernant l'usage de l'IA durant les élections

L'absence de règles claires et précises gouvernant l'utilisation de l'IA durant les élections crée une incertitude juridique. Il est ainsi difficile pour les autorités de déterminer les responsabilités des différentes parties prenantes en cas de problème ou de prendre des mesures efficaces contre les abus.

Partout dans le monde, les règles électorales ont été adoptées bien avant que l'IA générative ne devienne publiquement accessible et largement utilisée. Par conséquent, ces règles sont généralement trop larges pour gérer les risques uniques qu'entraîne l'IA. Par exemple, bon nombre de lois ne définissent pas des termes tels que « médias synthétiques » ou « contenus générés par l'IA » et n'établissent aucune limite quant à leur utilisation dans un contexte électoral.

Peu de législateurs ont adopté ou même débattu des propositions de règles électorales ciblant directement les défis liés à l'IA durant les élections. Au Royaume-Uni, par exemple, les lois actuelles en matière de diffamation visent à protéger les personnes contre des déclarations fausses, mais elles sont ambiguës en ce qui a trait aux fausses images ou vidéos[7].

Des règles claires et harmonisées sont essentielles pour assurer la reddition de comptes, accroître la transparence et permettre des interventions opportunes. En comblant les lacunes législatives, les responsables politiques peuvent mettre en place des protections robustes pour défendre l'intégrité des processus démocratiques et réduire l'insécurité grandissante entourant les défis électoraux liés à l'IA.

Action 1
Les gouvernements devraient actualiser les règles électorales

Les gouvernements devraient actualiser les règles électorales pour veiller à ce que les personnalités politiques, les partis politiques, les entreprises de technologies, ainsi que l'électorat connaissent exactement :

- → **de quelle manière un média synthétique peut être utilisé pour des activités électorales ;**
- → **les utilisations de l'IA qui sont interdites ou limitées dans un contexte électoral ;**
- → **de quelle façon la responsabilité est attribuée lorsqu'il y a violation des obligations établies dans les règles électorales.**

Afin de ne pas indûment limiter la liberté des communications politiques, les nouvelles règles électorales devraient être proportionnelles au risque qu'elles cherchent à prévenir. Les autorités indépendantes qui surveillent l'usage de l'IA lors d'élections devront posséder l'expertise technique et le financement nécessaires pour mettre efficacement ces règles en application.

Les gouvernements devraient clarifier la définition de termes clés comme « donnée synthétique », « IA générative », « contenu d'IA générative » et « information trompeuse », ainsi qu'évaluer la nécessité d'amender certains aspects particuliers de leurs règles actuelles. En outre, ils devraient sérieusement considérer l'adoption des règles obligatoires suivantes :

- → **l'interdiction d'utiliser, de publier, de montrer à l'écran ou de faire circuler du contenu trompeur généré par l'IA afin d'influencer une élection. Par exemple, les gouvernements devraient considérer l'interdiction de l'utilisation d'images, de vidéos ou de contenus audio générés par l'IA qui amplifient la désinformation au sujet de candidatures, de campagnes référendaires ou de processus électoraux, ou les représentent de manière fausse ou trompeuse ;**
- → **les personnalités politiques ainsi que leur parti devraient être tenus de respecter des obligations en matière de transparence, notamment en indiquant sur les images et extraits audio et vidéo utilisés, publiés, montrés à l'écran ou diffusés lors d'élections qu'ils sont générés par l'IA. Pour créer et améliorer ces étiquettes, les gouvernements pourraient consulter les recherches scientifiques et recueillir l'avis du public. Les gens devraient être en mesure de facilement reconnaître ces étiquettes de sorte qu'il serait important de considérer des aspects comme leur conception visuelle, les mots utilisés, leur taille, leur durée, leur emplacement et le moment choisi pour les afficher ;**
- → **les gouvernements devraient obliger les plateformes en ligne à mettre en œuvre des politiques en matière d'étiquetage des publicités politiques générées par l'IA et à établir et strictement mettre en application des règles de modération pour freiner la diffusion de contenus générés par l'IA pouvant causer des préjudices.**

Les règles électorales devraient viser les agents conversationnels, qui peuvent produire des informations trompeuses au sujet d'éléments importants d'une élection, comme l'emplacement des bureaux de vote, les documents requis pour pouvoir voter ou le casier judiciaire d'une personne qui se présente aux élections[8].

Deuxième défi
Les partis politiques ne se sont pas entendus sur ce que constituent des élections libres et justes à l'ère de l'IA

Les partis politiques et leurs équipes peuvent dorénavant potentiellement tirer parti d'outils d'IA pour créer des vidéos hypertruquées sophistiquées, générer du contenu trompeur à grande échelle, microcibler l'électorat avec de la désinformation adaptée ou manipuler le discours public par l'usage de comptes automatisés.

En l'absence de réglementations, de directives claires ou de cadres éthiques, les partis politiques pourraient utiliser l'IA d'une manière qui contribue à miner la confiance de l'électorat. En diffusant de fausses informations avec l'IA, ils pourraient indûment influencer le résultat d'une élection.

Sans règles convenues, les partis politiques pourraient se sentir contraints d'accroître leur propre usage des outils d'IA afin d'éviter de voir leurs adversaires les devancer. La pression politique pourrait entraîner une spirale dans laquelle les partis priorisent l'utilisation de l'IA pour gagner à tout prix, au détriment du maintien de l'intégrité électorale.

Action 2
Les partis devraient adopter un code de conduite comme point de départ pour assumer leurs responsabilités en matière de comportement électoral à l'ère de l'IA

Avec un code de conduite, les partis politiques conviennent de s'engager en faveur d'élections libres et justes en adoptant ou évitant certains comportements. Les codes de conduite en matière d'IA soutiennent généralement la transparence et l'honnêteté dans l'utilisation de cette technologie à des fins électorales.

De tels codes existent déjà dans certaines régions. En 2023, par exemple, cinq partis suisses ont convenu de faire preuve de transparence dans leur utilisation de l'IA et de ne pas y recourir à des fins dénigrantes. En vue des élections au Parlement européen de 2024, les partis européens ont conjointement souscrit à un code de conduite contenant des dispositions précises gouvernant le recours à l'IA. Des efforts visant la mise en place de tels codes ont été déployés dans des pays comme le Royaume-Uni ainsi que dans des entités infranationales.

Les codes de conduite encadrant l'utilisation de l'IA à des fins électorales devraient inciter les partis à :

- → **ne pas utiliser les outils d'IA pour produire du matériel notablement mensonger ou pour tromper l'électorat ;**
- → **clairement étiqueter tout contenu pour lequel les partis ont eu recours à l'IA de manière non négligeable (étant donné les lacunes législatives susmentionnées et l'urgence d'agir sur cette question) ;**
- → **ne pas amplifier du contenu synthétique trompeur ; les partis devraient aussi dénoncer les mauvais comportements, qu'il s'agisse de la publication ou de l'amplification de contenu trompeur ;**
- → **donner des directives claires et offrir une formation appropriée à l'ensemble des membres des partis politiques ainsi qu'à toute personne militante ou partisane sur l'utilisation des outils d'IA dans le cadre d'une campagne électorale ;**
- → **s'abstenir de produire, d'utiliser ou de diffuser du contenu trompeur, y compris des faux comptes, des robots logiciels automatiques ou des agents conversationnels, dans le but de manipuler l'opinion de l'électorat ;**
- → **introduire des « niveaux de modération » dans leurs propres agents conversationnels afin qu'ils orientent les internautes vers l'information électorale officielle ;**
- → **s'engager à surveiller, à vérifier et à revoir, au terme d'une élection, leurs usages de l'IA et les outils alimentés par l'IA.**

Troisième défi
la plupart des gouvernements ne sont pas préparés à parer les attaques alimentées par l'IA contre les élections et les institutions démocratiques

Les gouvernements ont établi des stratégies et des mécanismes pour faire face à des crises majeures comme les catastrophes naturelles, les troubles civils ou les pandémies. Or, la plupart d'entre eux ne sont pas prêts à contrer des attaques alimentées par l'IA visant l'intégrité des élections et des institutions démocratiques.

Résister efficacement aux menaces alimentées par l'IA contre l'intégrité électorale s'avère un défi multidimensionnel. Premièrement, plusieurs gouvernements ne disposent pas du système de surveillance complet requis pour détecter la désinformation, le contenu hypertruqué ainsi que d'autres campagnes d'influence automatisées par l'IA ciblant leurs processus démocratiques. De plus, les mécanismes de collaboration entre les parties prenantes telles que les agences gouvernementales, les plateformes de médias sociaux, les organes médiatiques et les groupes de la société civile sont insuffisants. En cas de détection d'activités suspectes, il n'y a pas de protocoles clairs pour partager l'information et coordonner les réponses.

Deuxièmement, une partie des fonctionnaires des autorités électorales ne possèdent pas les connaissances en IA requises pour reconnaître les menaces que celle-ci pose. Les outils nécessaires pour agir leur manquent. Ce déficit de capacités s'étend souvent à l'ensemble de l'écosystème démocratique. Par exemple, le personnel des bureaux de vote ainsi que les responsables de l'observation électorale, qui agissent comme première ligne de défense de l'intégrité électorale, peuvent recevoir une formation limitée, voire aucune formation, sur les menaces numériques. Ils peuvent aussi éprouver des difficultés à gérer les questions du public au sujet du contenu et des tentatives de manipulation générés par l'IA.

Troisièmement, les agences gouvernementales ne disposent souvent pas de l'infrastructure technique, de l'expertise humaine et des capacités nécessaires pour surveiller et contrer efficacement les attaques alimentées par l'IA. À défaut, les gouvernements sont forcés de réagir aux incidents au cas par cas plutôt que de mettre en œuvre des stratégies de défense proactives.

Action 3
Les autorités électorales devraient mettre sur pied une équipe interfonctionnelle indépendante chargée de prévenir les perturbations électorales causées par l'IA et d'intervenir lorsque ces dernières surviennent

Les autorités électorales devraient compter sur une équipe interfonctionnelle indépendante exerçant ses activités sous surveillance judiciaire. Cette équipe devrait pouvoir compter sur l'appui de l'ensemble des parties prenantes aux processus électoraux et démocratiques d'un gouvernement et établir des liens appropriés avec les médias, les plateformes en ligne et les autres entités régionales et internationales pertinentes. Les partis politiques devraient en faire partie afin que les protocoles d'urgence et d'atténuation soient considérés comme justes et équilibrés.

L'équipe interfonctionnelle indépendante devrait exercer ses activités pendant la période électorale, comme avant et après celle-ci, afin d'assurer une surveillance constante des attaques contre la démocratie. Elle serait responsable d'établir un plan d'intervention publique complet contre les menaces électorales alimentées par l'IA. Ce plan d'intervention électoral en matière d'IA définirait clairement les cadres d'évaluation, les responsabilités, les stratégies de communication, etc. Cette approche s'inspire des stratégies de préparation aux urgences bien établies pour la gestion de crises en santé publique, en cas de catastrophe naturelle et dans le cas d'incidents de cybersécurité. Ces stratégies ont permis la mise en œuvre réussie de systèmes d'alerte précoce, de protocoles de signalement, de mécanismes de divulgation obligatoire des incidents, d'accords de

partage des ressources et d'équipes d'intervention rapide.

Tous les membres de l'écosystème médiatique et numérique devraient participer à la mise en œuvre du plan d'intervention afin de limiter la propagation d'une attaque et d'alerter adéquatement la population.

Les autorités électorales devraient mener des exercices pratiques ou des simulations afin de permettre aux différentes parties prenantes de comprendre de quelle manière l'IA peut être mise en œuvre et utilisée, de faire connaître le plan d'intervention et de le tester, d'analyser les réactions concrètes aux incidents et de détecter les possibles vulnérabilités qui pourraient être exploitées.

Le plan d'intervention devrait tenir compte des droits fondamentaux de la population afin de la protéger des menaces de surveillance ou de contrôle de l'expression politique.

Pour s'assurer que les perturbations électorales causées par l'IA sont contrées efficacement, une formation adéquate sur l'IA et la cybersécurité devrait être fournie à toutes les parties prenantes de l'écosystème électoral et démocratique, y compris les bénévoles et les responsables de l'observation dans les bureaux de vote.

Quatrième défi
L'ingérence électorale facilitée par l'IA implique souvent des parties clandestines œuvrant dans plusieurs pays

La nature transnationale de plusieurs attaques électorales menées avec l'IA explique pourquoi il est difficile pour les gouvernements de les gérer efficacement sur une base individuelle. Ce problème est exacerbé par l'asymétrie des ressources et des connaissances entre les gouvernements, certains ne disposant pas de l'expertise, des outils ou des capacités nécessaires pour adéquatement détecter et contrer les menaces électorales menées avec des systèmes d'IA.

Sans protocoles internationaux harmonisés, il est difficile de rendre responsables les personnes impliquées en raison des différences entre les systèmes juridiques, les capacités d'enquête et les frontières juridictionnelles.

Les États démocratiques devraient reconnaître qu'une attaque sur une démocratie est une attaque contre les principes qui unissent toutes les démocraties. Une action collective est ainsi cruciale pour protéger les valeurs démocratiques communes, renforcer la confiance de la population et veiller à ce que l'intégrité des élections à l'échelle mondiale soit préservée.

Action 4
Les gouvernements devraient établir un Groupe international de sauvegarde des élections à l'ère de l'IA, ainsi que des protocoles internationaux assurant un appui juridique mutuel en cas d'ingérence électorale causée par l'IA

Les États devraient établir une plateforme internationale centralisée et s'unir pour en apprendre davantage sur les cas d'ingérence liés à l'IA et y réagir. Ils devraient créer le Groupe international de sauvegarde des élections à l'ère de l'IA.

Le Groupe serait composé de spécialistes multidisciplinaires et d'institutions engagés pour détecter, contrer et atténuer les ingérences électorales causées par l'IA. Il servirait de ressource sociotechnique pour les pays vulnérables à de telles ingérences. Le Groupe offrirait également du soutien en cas de crise en déployant des équipes d'intervention rapide lors d'événements électoraux actifs ainsi qu'un suivi et des stratégies d'atténuation en temps réel dans le cas de scénarios à haut risque.

La création du Groupe pourrait découler de programmes existants (ou s'aligner sur eux) pour aider ou protéger les pays contre les menaces électorales.

Des mesures pourraient, par exemple, être prises pour améliorer (de manière temporaire ou permanente) les ressources en IA ou les compétences techniques et juridiques de la Division de l'assistance électorale des Nations Unies[9], qui aide les États membres à tenir des élections qui expriment de manière légitime la volonté de la population et qui sont jugées crédibles par les parties prenantes nationales. Le nouveau Réseau international d'instituts de sécurité de l'IA pourrait être mis à profit dans la formation de gardiens et gardiennes des élections et dans leur déploiement dans le monde pour mener des missions particulières.

Lorsqu'une expertise technologique est requise, le Groupe devrait pouvoir compter sur le soutien des entreprises et des plateformes d'IA, notamment celles qui sont à l'origine du récent accord sur l'utilisation de l'IA dans les élections[10].

De plus, la possibilité de compter sur des mécanismes d'entraide juridique internationale pour enquêter et engager des poursuites dans les cas d'ingérence électorale menée par l'IA facilitera la coopération étroite des différents gouvernements, aidera à recueillir et à partager des preuves admissibles provenant de divers pays et permettra de faire en sorte que les personnes coupables d'utiliser l'IA dans le but de manipuler des élections à l'échelle transnationale ne puissent pas exploiter les frontières juridictionnelles pour éviter d'en être tenues responsables.

Ces mécanismes judiciaires ont déjà permis de relever efficacement des défis transnationaux nécessitant une étroite collaboration transfrontalière et le partage de preuves, notamment dans les domaines de la lutte contre la cybercriminalité, la fraude numérique, le terrorisme, le crime organisé, les violations contre les droits de la personne et les crimes de guerre.

Ces mécanismes internationaux devront être transparents pour assurer la protection des droits fondamentaux.

Conclusion

L'effet de l'IA sur la démocratie n'est pas gravé dans le marbre.

Bien que cet énoncé porte plus particulièrement sur les risques de l'IA, celle-ci pourrait servir à renforcer les démocraties. Les fonctionnaires électoraux pourraient utiliser des outils d'IA pour effectuer efficacement des tâches complexes. Ces outils pourraient rendre le vote plus accessible et accroître la participation citoyenne. Par exemple, une élection contestée s'est tenue en 2024 au Pakistan ; l'IA y a permis à un leader de l'opposition emprisonné de diffuser des messages audio à son électorat, et de le mobiliser malgré les restrictions en place[11]. À l'avenir, quiconque milite pour la démocratie devrait explorer de quelles manières l'IA peut améliorer les systèmes démocratiques.

Pour l'instant, cependant, la priorité consiste à protéger les démocraties d'une menace pressante : l'utilisation malveillante de l'IA par des acteurs nationaux et étrangers.

Pour ce faire, nous devons agir sur deux fronts.

Au sein de chaque pays, les gouvernements doivent mettre à jour leurs lois ; les partis politiques doivent travailler ensemble ; et les autorités électorales doivent se préparer à défendre l'intégrité démocratique contre une utilisation malveillante de l'IA.

Entre les pays, la coopération est essentielle. Aucun pays ne peut faire face seul aux défis de l'IA. Les pays doivent harmoniser leurs lois en matière d'ingérence électorale menée par l'IA. Ce faisant, ils renforceront leurs défenses individuelles et bâtiront une résistance collective contre les tentatives visant à affaiblir la démocratie à l'échelle mondiale.

En mettant ces mesures en œuvre dès aujourd'hui, nous créerons des systèmes démocratiques plus solides, plus inclusifs et plus fiables pour l'avenir.

Notes

1. La version originale de cet énoncé a été produite en anglais sous le titre *AI in the Ballot Box*.
2. Farrugia, B. (2024, 26 novembre). Brazil's electoral deepfake law tested as AI-generated content targeted local elections. DFRLab. https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes
3. Pour plus d'informations sur la manière dont l'IA pose de graves problèmes pour la sécurité des femmes, consultez : Organisation des Nations Unies pour l'éducation, la science et la culture. (2023). Violence de genre facilitée par la technologie à l'ère de l'IA générative (Tendances mondiales en matière de liberté d'expression et de développement des médias). https://unesdoc.unesco.org/ark:/48223/pf0000387483
4. Harward, C. (2024, 6 décembre). Likely Kremlin-backed election interference against Romania threatens Bucharest's continued support for Ukraine and NATO. Institute for the Study of War. https://understandingwar.org/backgrounder/likely-kremlin-backed-election-interference-against-romania-threatens-bucharests
5. RFI. (2023, 23 août). Élections au Gabon : polémique après des enregistrements supposés de candidats de l'opposition. RFI. https://www.rfi.fr/fr/afrique/20230823-%C3%A9lections-au-gabon-pol%C3%A9mique-apr%C3%A8s-des-enregistrements-suppos%C3%A9s-de-candidats-de-l-opposition
6. Palta, R., Angwin, J., et Nelson, A. (2024, 27 février). How we tested leading AI models performance on election queries. Proof. https://www.proofnews.org/how-we-tested-leading-ai-models-performance-on-election-queries; Impelli, M. (2024, 31 octobre). Voting rights groups warn about AI generating unfounded claims in Spanish. Newsweek. https://www.newsweek.com/2024-election-spanish-latino-voters-artifical-intelligence-concerns-1978170; Ott, H., et Lyons, E. (2024, 25 juin). ChatGPT gave incorrect answers to questions about how to vote in battleground states. CBS News. https://www.cbsnews.com/news/chatgpt-chatbot-ai-incorrect-answers-questions-how-to-vote-battleground-states
7. Stockwell, S., Hughes, M., Swatton, P., et Bishop, K. (2024). AI-enabled influence operations: the threat to the UK general election. CETaS Briefing Papers. https://cetas.turing.ac.uk/sites/default/files/2024-05/cetas_briefing_paper_-_ai-enabled_influence_operations_-_the_threat_to_the_uk_general_election.pdf
8. Kaye, R. (2023, 5 avril). Australian mayor readies world's first defamation lawsuit over ChatGPT content. Reuters. https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05
9. Département des affaires politiques et consolidation de la paix des Nations Unies. (2023). 2023 factsheet: electoral assistance. https://dppa.un.org/sites/default/files/electoral_assistance.pdf
10. Accord sur l'utilisation de l'IA dans les élections (2024, 16 février). A tech accord to combat deceptive use of AI in 2024 elections. https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL_.pdf
11. Zhuang, Y. (2024, 11 février). Imran Khan's 'Victory Speech' from jail shows A.I.'s peril and promise. The New York Times. https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html

Les Énoncés de politiques mondiales sur l'IA

Les Énoncés de politiques mondiales sur l'IA sont un projet conjoint d'IVADO, le principal consortium de recherche et de mobilisation des connaissances en IA au Canada, et de l'Initiative IA + Société de l'Université d'Ottawa. Ce projet vise à fournir aux responsables politiques des recommandations de politiques publiques pour relever les grands défis mondiaux actuels en matière d'IA.

Pour ce premier énoncé, les professeurs Catherine Régis et Florian Martin-Bariteau ont convié un groupe de chercheuses et de chercheurs de renommée mondiale en IA pour établir des orientations de politiques publiques applicables à l'échelle mondiale concernant l'effet de l'IA sur la démocratie et l'intégrité électorale. Ce document est le fruit d'une retraite d'une semaine tenue dans les bureaux de la Società Italiana per l'Organizzazione Internazionale (SIOI) en décembre 2024, à Rome, en Italie. Il a été rédigé avec le soutien de Réjean Roy, directeur, mobilisation des connaissances, chez IVADO.

Ce projet a été rendu possible par le soutien du Fonds de recherche du Québec ; du CEIMIA ; de la Chaire Canada-CIFAR en IA et droits de la personne, Mila ; de la Chaire de recherche de l'Université d'Ottawa en technologie et société, ainsi qu'avec l'aide de la Délégation du Québec à Rome et de la SIOI pour l'organisation logistique de la retraite.

Les opinions exprimées dans cet énoncé sont exclusivement celles des personnes qui l'ont rédigé.

Catherine Régis est professeure de droit à l'Université de Montréal et directrice, innovation sociale et politiques internationales, chez IVADO. Experte de la gouvernance de l'IA, elle copréside le programme de recherche de l'Institut canadien de la sécurité de l'IA et est titulaire de la Chaire Canada-CIFAR en IA et droits de la personne, Mila.

Florian Martin-Bariteau est titulaire de la Chaire de recherche de l'Université en technologie et société et professeur agrégé de droit à l'Université d'Ottawa, où il dirige l'Initiative IA + Société et le Centre de recherche en droit, technologie et société. Il est chercheur associé du Berkman-Klein Center à la Harvard University.

Professeur agrégé à la Lincoln Alexander School of Law de la Toronto Metropolitan University, **Jake Okechukwu Effoduh** se spécialise dans le droit de l'IA et les droits de la personne à l'échelle internationale. Il contribue à l'élaboration de cadres réglementaires en matière d'IA dans plusieurs pays et dirige d'importants projets de recherche entre le Canada et l'Afrique.

Juan David Gutiérrez, professeur agrégé à l'Universidad de los Andes, à Bogotá, étudie les intersections entre les politiques publiques et les technologies. À titre de membre expert du Partenariat mondial sur l'intelligence artificielle (PMIA), il codirige le projet sur la transparence algorithmique.

Gina Neff est professeure en IA responsable à la Queen Mary University of London et dirige le Minderoo Centre for Technology and Democracy de l'University of Cambridge. Ses recherches analysent l'impact des environnements numériques sur le travail et la vie quotidienne.

Expert juridique spécialisé en droit numérique, **Carlos Affonso Pereira de Souza** dirige l'Instituto de Technologia e Sociedade do Rio de Janeiro. En tant que professeur de droit et technologie, il a contribué à l'élaboration des lois brésiliennes sur Internet et la protection des données.

Professeure de droit privé à l'Université Paris 1 Panthéon-Sorbonne, **Célia Zolynski** est une spécialiste du droit numérique et de la propriété intellectuelle. En tant que coordinatrice de l'Observatoire de l'IA de Paris 1, elle se concentre sur la régulation de l'IA et les droits fondamentaux.

Une initiative conjointe de

IVADO

uOttawa | Initiative IA + Société AI + Society

Avec le soutien de

Fonds de recherche Québec

CIFAR

ceimia

Cette initiative a été menée grâce, en partie, au soutien financier du Fonds d'excellence en recherche Apogée Canada.