

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA GESTION ÉLECTORALE



L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA GESTION ÉLECTORALE

Prathm Juneja



IDEA International
Strömsborg
SE-103 34 Stockholm
SUÈDE
+46 8 698 37 00
info@idea.int
www.idea.int

© 2024 Institut international pour la démocratie et l'assistance électorale

©2024 Édition en anglais

Les publications d'IDEA International sont indépendantes de tout intérêt national ou politique particulier. Les points de vue exprimés dans la présente publication ne reflètent pas nécessairement les opinions d'IDEA International, de son conseil d'administration ou des membres du conseil.



À l'exception des images et photos de tiers, la version électronique de la présente publication est disponible sous Creative Commons Licence (CCL)–Creative Commons Attribution–NonCommercial–ShareAlike 4.0 Licence. Vous pouvez librement partager cette publication ou en faire des travaux dérivés uniquement à des fins non commerciales, et à condition d'en avoir correctement nommé les sources et de les diffuser sous une licence identique à celle-ci. Pour de plus amples informations sur cette licence, veuillez consulter : <<http://creativecommons.org/licenses/by-nc-sa/4.0>>.

IDEA International
Strömsborg
SE-103 34 Stockholm
SUÈDE
Téléphone : +46 8 698 37 00
Courriel : info@idea.int
Site Internet : <<https://www.idea.int>>

Illustration de la couverture: générée avec DALL E
Graphisme: IDEA International
Révision: Christèle Jany

DOI: <<https://doi.org/10.31752/idea.2024.60>>

ISBN: 978-91-7671-801-8 (édition PDF)

Table des matières

Abréviations	v
Résumé	1
Introduction	4
Chapitre 1	
Présentation générale : L'IA et les élections	6
1.1. Définition de l'IA	6
1.2. Progrès de l'IA et utilisation dans le cadre d'élections	7
Chapitre 2	
Opportunités et défis de l'utilisation de l'IA pour la gestion des élections	10
2.1. Introduction	10
2.2. Période préélectorale	11
2.3. Période électorale	20
2.4. Période post-électorale	29
2.5. Autres défis, préoccupations et stratégies d'atténuation	31
2.6. Voies à suivre	38
Chapitre 3	
Utilisation de l'IA par d'autres acteurs politiques et implications pour les OGE	40
3.1. IAg et mésinformation	40
3.2. Organisations politiques	43
3.3. Menaces pour la sécurité des systèmes électoraux	45
3.4. Voies à suivre	46
Chapitre 4	
Cadres réglementaires de l'IA et implications pour les élections	49
4.1. Législation européenne sur l'IA	49
4.2. Décret présidentiel des États-Unis sur l'intelligence artificielle	51
4.3. Règlement du Tribunal électoral brésilien	52
4.4. Réglementation de l'IA dans d'autres pays	53
Chapitre 5	
Conclusion	54
Références bibliographiques	57
Annexe A. Termes clés	66
À propos de l'auteur	68
À propos d'IDEA International	69

Abréviations

IA	Intelligence artificielle
OGE	Organe de gestion électorale
RGPD	Règlement général sur la protection des données
IAg	Intelligence artificielle générative
LLM	Modèle de langage de grande taille
OCR	Reconnaissance optique de caractères
OMR	Reconnaissance optique de marques

RÉSUMÉ

L'intelligence artificielle (IA), notamment le rôle qu'elle peut jouer pour influencer sur une élection, prenant une importance croissante, les organes de gestion électorale (OGE) doivent élaborer des plans pour faire face à l'IA et, dans certains cas, l'utiliser pour la tenue d'élections libres, équitables et sûres. L'IA est une catégorie de technologies qui évolue rapidement et qui, pour une large part, n'est pas réglementée. De plus, très peu de recherches ont été menées jusqu'à présent concernant son impact potentiel sur les élections.

Ce rapport a pour but d'aider les OGE et d'autres parties concernées à mieux comprendre les possibilités, les défis et les implications juridiques de l'utilisation de l'IA dans le cadre des élections. Il s'articule autour de deux axes principaux. Premièrement, il offre un point de départ pour examiner certaines des façons dont les OGE pourraient utiliser l'IA pour améliorer l'administration des élections ; il présente les risques et les stratégies d'atténuation potentielles associés à ces utilisations. Deuxièmement, il couvre certaines des façons dont des acteurs autres que les OGE peuvent utiliser l'IA pour influencer sur les processus électoraux, ainsi que les stratégies potentielles de réponse des OGE. Il décrit certains des cadres réglementaires relatifs à l'IA qui commencent à prendre forme dans le monde et explique comment ils peuvent influencer sur le travail des OGE qui envisagent d'utiliser l'IA dans le cadre du processus électoral et de réagir au recours à l'IA par d'autres acteurs.

L'utilisation de l'IA par les OGE étant encore à ses balbutiements, le présent rapport se penche sur le corpus limité d'exemples et travaux universitaires sur le sujet et les croise avec des éclairages issus de divers secteurs et d'autres domaines universitaires pour mettre en évidence les domaines potentiels d'utilisation de l'IA pour

Les OGE doivent élaborer des plans pour faire face à l'IA et, dans certains cas, l'utiliser pour la tenue d'élections libres, équitables et sûres.

le personnel des OGE dans les phases préélectorale, électorale et post-électorale du cycle électoral, ainsi que l'utilisation d'outils généralistes d'IA générative, tels que ChatGPT. On peut recourir à l'IA, entre autres, pour la gestion des listes électorales, l'inscription des électeurs, la planification de l'allocation des ressources, la prévision des coûts électoraux, la publicité ciblée, le suivi de la campagne, la biométrie et la vérification de l'identité des électeurs, le dépouillement des bulletins de vote et les audits post-électoraux. Chacune de ces utilisations soulève une série de questions éthiques, pratiques et relatives aux droits humains, telles que la surveillance, les préjugés, la discrimination, la précision, la performance, les capacités techniques, la cybersécurité et la confiance du public. Dans de nombreux cas, les OGE qui envisagent d'utiliser l'IA peuvent être en mesure d'atténuer ces préoccupations grâce à une supervision humaine attentive, à des tests et à des audits des systèmes d'IA.

Ce rapport ne prend pas position sur la question de savoir si les OGE devraient envisager de recourir à l'IA pour les élections ; il propose en revanche une introduction à ce sujet pour les OGE qui en envisageraient l'utilisation, ainsi que des recommandations pour élaborer des règles de mise en œuvre claires, transparentes et respectueuses des droits.

Ce rapport aborde la question souvent débattue de l'utilisation de l'IA par d'autres acteurs politiques, notamment ceux qui produisent de fausses informations, les chargés de campagnes politiques et les pirates informatiques. Bien que la désinformation électorale ne soit pas un phénomène nouveau, les progrès de l'IA générative aggravent les problèmes existants en augmentant le volume des informations erronées et, dans certains cas, en rendant les fausses informations de plus en plus convaincantes. Garantir la transparence, s'engager dans une coopération inter-agences et forger des partenariats avec les fournisseurs et les diffuseurs de contenus générés par l'IA sont des stratégies potentielles d'atténuation de ce problème.

Les campagnes politiques sont susceptibles d'utiliser l'IA pour tout, de la publicité ciblée aux prévisions électorales.

Les campagnes politiques sont susceptibles d'utiliser l'IA pour tout, de la publicité ciblée aux prévisions électorales, et les OGE devraient examiner dans quelle mesure ces utilisations peuvent nécessiter d'actualiser leur mandat et leurs réglementations. L'IA peut également accroître la menace de cyberattaques, notamment par le biais de tentatives d'hameçonnage (ou *phishing*) de meilleure qualité, et les OGE devraient envisager de renforcer les protocoles de cybersécurité existants pour se défendre contre ces avancées.

L'évolution rapide de l'environnement réglementaire peut également influencer le rôle de l'IA dans les élections. Dans ce rapport, nous présentons brièvement quelques approches réglementaires de l'IA, notamment le Règlement européen sur l'intelligence artificielle – et son accent sur les applications à haut risque – ainsi que le décret présidentiel américain sur l'intelligence artificielle et la réglementation du Tribunal supérieur électoral du Brésil. Dans ces trois cas, les réglementations ont une incidence sur la manière dont les OGE peuvent utiliser l'IA dans le cadre de leur propre travail et elles peuvent avoir un impact sur les mandats des OGE, en particulier en ce qui concerne la supervision des campagnes politiques.

Bien qu'il y ait encore beaucoup d'incertitudes sur la manière dont les OGE peuvent utiliser l'IA, ainsi que sur l'impact de l'utilisation de l'IA par d'autres acteurs sur les élections, il est de plus en plus important pour les OGE de commencer à élaborer des plans pour s'adapter à ce nouvel environnement technologique. Ce rapport offre un point de départ pour ce travail en proposant une vue d'ensemble de l'IA pour les élections, y compris les opportunités, les défis et les stratégies d'atténuation associés à son utilisation par les OGE et d'autres acteurs concernés.

Il est de plus en plus important pour les OGE de commencer à élaborer des plans pour s'adapter à ce nouvel environnement technologique.

INTRODUCTION

Le débat sur l'IA et les élections met l'accent sur le rôle que l'IA peut jouer dans la production et la diffusion de fausses informations.

L'intelligence artificielle (IA) est un sujet de plus en plus important pour les organes de gestion électorale (OGE) et les autres organisations impliquées dans les processus électoraux. En général, le débat sur l'IA et les élections met l'accent sur le rôle l'IA que peut jouer dans la production et la diffusion de fausses informations¹. Bien qu'il s'agisse là d'un aspect important, abordé en de nombreux endroits de ce rapport, un sujet bien plus vaste mérite l'attention, à savoir le rôle et l'impact potentiels de l'IA sur les élections, ce qui englobe tout le processus, de la façon dont les OGE peuvent envisager de mettre en œuvre l'IA dans le cadre des processus électoraux à la manière dont d'autres acteurs politiques pourraient utiliser l'IA pour influencer sur les élections.

Pour commencer à combler cette lacune, ce rapport propose un cadre aux OGE qui s'intéressent à l'utilisation de l'IA et à son impact dans les domaines des élections et de la gestion électorale. L'IA et les élections étant un sujet vaste et en pleine évolution, ce rapport met en évidence les domaines que les OGE peuvent éventuellement explorer lorsqu'ils entreprennent de développer des stratégies d'IA dans leurs contextes spécifiques.

Bien que les recherches sur l'utilisation de l'IA dans la gestion des élections soient encore peu nombreuses, l'objectif principal de ce rapport est d'offrir aux OGE un point de départ – en s'inspirant d'exemples provenant d'autres domaines et en examinant les processus existant au sein des OGE – pour comprendre comment

¹ Selon la définition du Haut Commissariat des Nations Unies (2022), la mésinformation est le fait de diffuser une information fautive ou inexacte ; la désinformation consiste quant à elle à diffuser délibérément des informations erronées, y compris des contenus malveillants tels que des canulars, le harponnage ou *spear phishing*, ou de la propagande.

l'IA peut être utilisée pour améliorer l'administration des élections. La grande majorité des exemples d'utilisation de l'IA par les OGE présentés dans ce rapport proviennent des États-Unis, qui ont eu de nombreuses occasions de recourir à l'IA en raison de leur système électoral fédéralisé, souvent géré au niveau des États et des comtés, ainsi que du nombre important d'entreprises d'IA présentes dans le pays.

Les progrès de l'IA ont permis aux OGE de déployer des systèmes dotés de meilleures capacités de raisonnement et analytiques et génératives susceptibles d'accroître l'accessibilité aux élections, d'optimiser leur planification logistique et d'améliorer l'environnement informationnel dans lequel ils évoluent. Ces avantages potentiels s'accompagnent d'éventuelles externalités négatives en matière de cybersécurité, de droits humains, de discrimination et d'autres enjeux.

Les progrès de l'IA ont permis aux OGE de déployer des systèmes dotés de meilleures capacités.

Il convient de noter que ce rapport n'a pas pour but de recommander explicitement l'utilisation de l'IA par les OGE, ni de donner des instructions pour sa mise en œuvre ; il s'agit plutôt d'une introduction générale à l'intention des OGE intéressés par le sujet. Un autre objectif du rapport est de fournir aux OGE un point de départ pour examiner comment d'autres acteurs, tels que les chargés de campagnes politiques et les pirates informatiques, peuvent utiliser l'IA pour influencer la gestion et le résultat des élections. Compte tenu de la prolifération et de la facilité d'accès des outils d'IA avancés, les OGE doivent commencer à planifier en fonction de ces utilisations de l'IA, y compris la mise en œuvre de stratégies d'atténuation et l'élaboration d'approches réglementaires.

Le rapport est organisé comme suit. Dans le chapitre 1, nous proposons une définition de l'IA et un contexte historique de son utilisation dans les élections, et nous expliquons en quoi les progrès récents de l'IA motivent le présent rapport. Au chapitre 2, nous dressons une liste non exhaustive des cas d'utilisation possibles de l'IA par les OGE au cours du cycle électoral, y compris les étapes de la mise en œuvre, les problèmes associés aux utilisations concrètes et les solutions potentielles pour atténuer certains de ces problèmes. Le chapitre 3 aborde un domaine distinct mais pertinent pour les OGE, à savoir la manière dont d'autres acteurs politiques peuvent utiliser l'IA pour influencer la gestion des élections, et ce à quoi les OGE doivent commencer à se préparer à court terme. Enfin, au chapitre 4, nous examinons certaines approches mondiales et nationales de la réglementation de l'utilisation de l'IA, en particulier pour les organismes publics, et la manière dont ces réglementations peuvent façonner l'utilisation de l'IA par les OGE et leur réponse à celle-ci.

Chapitre 1

PRÉSENTATION GÉNÉRALE : L'IA ET LES ÉLECTIONS

1.1. DÉFINITION DE L'IA

Pour ce rapport, nous nous appuyons sur la définition largement acceptée des systèmes d'IA fournie par l'Organisation de coopération et de développement économiques (2019) :

Un système d'IA est un système informatique qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer des environnements physiques ou virtuels. Les différents systèmes d'IA varient en termes de niveaux d'autonomie et d'adaptabilité après leur déploiement.

Les méthodes statistiques traditionnelles, telles que les régressions linéaires et le filtrage par modèle de probabilité, ainsi que les techniques modernes d'apprentissage automatique, telles que les réseaux neuronaux, sont toutes couvertes par cette définition si elles sont utilisées pour développer des résultats susceptibles d'influencer des environnements physiques ou virtuels. Sur la base de cette définition, nous utilisons le terme « IA » dans le présent rapport pour nous référer à une large gamme de systèmes, et nous utilisons des termes plus spécifiques pour décrire les technologies sous-jacentes. Pour plus d'informations sur les termes, voir l'annexe A : Termes clés.

1.2. PROGRÈS DE L'IA ET UTILISATION DANS LE CADRE D'ÉLECTIONS

L'IA est utilisée depuis longtemps dans le cadre de la gestion électorale. Aux États-Unis, par exemple, l'Electronic Registration Information Center (ERIC) travaille avec un consortium d'États pour analyser l'inscription des électeurs, les registres d'immatriculation des véhicules automobiles et d'autres registres officiels afin de tenir à jour les listes électorales. Le logiciel de l'ERIC est basé sur l'apprentissage automatique et signale aux responsables électoraux des États les électeurs susceptibles d'avoir été inscrits deux fois et les électeurs dotés de la capacité à voter mais non-inscrits (Electronic Registration Information Center 2024). Les systèmes de vérification biométrique, déjà en place ou encore à l'essai dans de nombreux pays, sont souvent des exemples d'IA qui utilisent des modèles d'apprentissage profond afin de faire correspondre des données biométriques à des ensembles de données existants (Wolf *et al.*, 2017). Les outils de comparaison des signatures, dont l'usage est également très répandu aux États-Unis, sont un autre exemple d'IA (Bender, 2022). Les pays qui utilisent des techniques de modélisation statistique pour l'affectation des ressources, l'implantation des bureaux de vote, les campagnes publicitaires ou l'analyse des scrutins peuvent également avoir recours à diverses formes d'IA.

Bien que rarement reconnue comme telle, l'IA n'est pas une nouveauté pour les élections ou les administrateurs électoraux. Les progrès réalisés dans le développement, le déploiement et la commercialisation de l'IA ont toutefois accru les possibilités offertes par son utilisation dans les élections ainsi que les concessions qui en découlent.

Les recherches sur ce que nous considérons aujourd'hui comme l'IA ont probablement commencé entre le début et le milieu du XX^e siècle, avec le test de Turing et la conception des premiers réseaux neuronaux artificiels. Les premiers progrès de l'IA se sont surtout concentrés sur la tâche étroite de concevoir des systèmes dits experts, ou des modèles entraînés de manière à pouvoir imiter les experts humains dans des domaines spécifiques, et de nombreux développements de l'IA étaient axés sur la prise de décision dans les jeux. Jusqu'à récemment, la plupart des progrès de l'IA ont davantage concerné ces systèmes plus restreints, avec des modèles fonctionnant comme des statistiques traditionnelles, prenant des entrées spécifiques et développant des formules interprétables sur la

façon dont elles aboutissent à des sorties, plutôt que les abstractions que nous associons aux approches d'apprentissage en profondeur.

L'ère actuelle de l'IA a été grandement stimulée par les progrès de l'apprentissage profond, y compris l'architecture de type « transformeur » (Vaswani *et al.*, 2017). Ces innovations, parallèlement à la disponibilité croissante de grands ensembles de données et de la puissance de traitement informatique, ont permis aux modèles d'apprentissage profond de prendre en charge de vastes pans de données non structurées, notamment des textes, des images et des vidéos, et de les utiliser pour former des modèles généralisés. Les progrès de l'apprentissage par transfert ont permis aux développeurs de spécialiser ces modèles plus vastes pour les besoins de divers domaines, notamment la médecine, la science, les médias et, de plus en plus, la politique. Bien que les approches d'apprentissage profond aient considérablement amélioré les performances dans de nombreuses tâches, en particulier dans la modélisation des langues, elles souffrent souvent d'un manque d'interprétabilité, en raison des niveaux d'abstraction inhérents aux réseaux neuronaux profonds. Alors que les régressions traditionnelles offrent des formules claires sur la manière dont les entrées sont transformées en sorties, les réseaux neuronaux profonds occultent comment et pourquoi des entrées spécifiques aboutissent à des sorties spécifiques.

Ce sont ces avancées plus récentes, sources de nouvelles opportunités et de préoccupations pour les autorités électorales, qui ont motivé la rédaction de ce rapport. Les modèles de langage de grande taille (LLM) offrent aux OGE et aux acteurs politiques la possibilité d'analyser, de générer et de résumer des textes complexes. D'autres modèles d'IA générative (IAg) offrent des capacités similaires pour obtenir d'autres types de résultats, notamment des données vidéo, audio et numériques. Les progrès réalisés dans des techniques telles que les réseaux neuronaux graphiques et les méthodes de *boosting* et de *bagging* ouvrent de nouvelles voies pour l'analyse des réseaux et des ensembles de données complexes. Dans la partie suivante, nous examinons comment les OGE peuvent utiliser les systèmes d'IA pour améliorer la gestion des élections. Nous examinerons ensuite comment l'utilisation de l'IA par d'autres acteurs est susceptible d'avoir un impact sur les OGE.

Il convient de noter que des organismes gouvernementaux et des entreprises du monde entier procèdent déjà à des essais impliquant

bon nombre de ces avancées en matière d'IA sous diverses formes, et que de nombreux pays sont en train d'établir des directives pour l'utilisation de l'IA (Carrasco *et al.*, 2024). Ces stratégies d'IA du secteur public au sens large sont susceptibles d'avoir un impact sur les ressources et sur les capacités auxquelles les OGE auront accès lors de la mise en œuvre de l'IA pour la gestion des élections.

**De nombreux pays
sont en train d'établir
des directives pour
l'utilisation de l'IA.**

Chapitre 2

OPPORTUNITÉS ET DÉFIS DE L'UTILISATION DE L'IA POUR LA GESTION DES ÉLECTIONS

2.1. INTRODUCTION

Dans ce chapitre, nous présentons une liste non exhaustive de cas d'utilisation potentiels de l'IA pour les OGE pendant les phases préélectorale, électorale et post-électorale du cycle électoral, certaines utilisations concrètes demeurant applicables tout au long du cycle électoral. Bon nombre de ces utilisations n'ont pas été testées et sont basées sur des travaux du secteur et d'autres domaines d'études. Nous couvrons également le cas des OGE qui intègrent des outils d'IAg pour des usages généraux, tels que l'application Copilot de Microsoft, dans leur travail quotidien.

Pour chaque utilisation, nous couvrons les défis en matière d'éthique, de droits humains et les aspects pratiques associés à sa mise en œuvre. À la fin, nous incluons également une liste générale de défis supplémentaires liés à l'utilisation par l'OGE de tout système basé sur l'IA. Nous présentons des stratégies d'atténuation potentielles afin de répondre à certaines de ces préoccupations. Enfin, nous formulons des recommandations sommaires à l'intention des OGE qui envisagent d'utiliser l'IA pour la gestion des élections.

2.2. PÉRIODE PRÉÉLECTORALE

La période préélectorale est la partie du cycle électoral regroupant la planification, la formation, le partage d'informations et l'inscription sur les listes électorales.

2.2.1. Inscription des électeurs et capacité à voter

Gestion des listes électorales

Cas d'utilisation de l'IA. La gestion des listes électorales, à savoir le toilettage et l'audit des listes électorales, est une tâche à laquelle les modèles d'IA sont particulièrement bien adaptés. Dans de nombreux cas, les pays, par exemple l'Indonésie (Akbar *et al.*, 2021), utilisent déjà des approches simples de rapprochements de modèles pour détecter et signaler les doublons, ainsi que des outils de filtrage pour rechercher les données manquantes, incomplètes ou incorrectes. Des modèles de rapprochement des données plus avancés peuvent se révéler utiles pour rechercher les inscriptions multiples en suggérant la probabilité que plusieurs inscriptions concernent la même personne. Les modèles peuvent comparer les informations d'inscription avec d'autres sources de documentation officielle ou de données historiques et recommander que certaines inscriptions fassent l'objet d'un examen plus approfondi.

Mise en œuvre. Les approches algorithmiques sont une procédure courante en matière de gestion des listes électorales, mais il existe peu d'exemples d'utilisation de méthodes d'apprentissage automatique plus avancées. L'ERIC aux États-Unis utilise l'apprentissage centré sur l'entité pour croiser différents fichiers, notamment ceux de la sécurité sociale, des changements d'adresse, des listes électorales et du département responsable de l'immatriculation des véhicules (Electronic Registration Information Center, 2024).

Préoccupations. L'utilisation de toute approche algorithmique pour la gestion des listes électorales suscite de vives inquiétudes, en particulier les approches d'IA ininterprétables utilisées sans supervision humaine (Padmanabhan, Simoes et MacCarthaigh, 2023). Les modèles imprécis – qu'il s'agisse d'approches traditionnelles de rapprochement de modèles ou de modèles d'apprentissage profond plus avancés – risquent d'exclure indûment du droit de vote des électeurs et pourraient donner lieu à des résultats discriminatoires si les différences dans la répartition des noms et des adresses ne sont pas prises en compte. Un manque de

La gestion des listes électorales, à savoir le toilettage et l'audit des listes électorales, est une tâche à laquelle les modèles d'IA sont particulièrement bien adaptés.

transparence pourrait amener à craindre pour l'intégrité électorale. Il est prouvé que Crosscheck, un outil de gestion des listes électorales anciennement utilisé aux États-Unis, a failli radier à tort au moins 300 électeurs pour empêcher un seul cas de double vote (Goel *et al.*, 2020). Pour atténuer certains de ces problèmes, les OGE devraient envisager d'utiliser des approches algorithmiques pour la gestion des listes uniquement dans le cadre d'un processus sous supervision humaine plus approfondi, probablement comme point de départ d'enquêtes.

Inscription et identification des électeurs

Cas d'utilisation de l'IA. L'un des objectifs du processus d'inscription des électeurs est de vérifier au préalable la capacité d'une personne à voter afin que, lorsqu'un électeur soumet son bulletin de vote, seule son identité doit être vérifiée. Dans les circonscriptions où est exigée l'inscription active des électeurs, ce processus impose souvent aux électeurs de présenter une forme quelconque de pièce d'identité officielle, une preuve de leur capacité à voter, et éventuellement de fournir des données biométriques, telles que des empreintes digitales, des photos d'identité ou une signature. Les modèles d'IA entraînés à comparer des documents d'identité ou des données biométriques peuvent accélérer ce processus, et potentiellement en améliorer la précision, et empêcher les inscriptions en doublon. L'IA offre de nouvelles formes d'identification biométrique des électeurs dans les bureaux de vote, telles que l'identification faciale et l'empreinte du pouce, où un modèle peut comparer les données biométriques d'un électeur avec les données biométriques figurant sur le registre électoral.

Mise en œuvre. Dans de nombreux cas, les outils biométriques reposent sur l'IA et utilisent des modèles d'apprentissage profond pour comparer les hachages biométriques (c'est-à-dire les représentations numériques des données biométriques telles que les empreintes digitales). L'utilisation d'un système biométrique pour l'inscription des électeurs offre aux OGE la possibilité de revérifier les données biométriques dans les bureaux de vote ou de les inclure dans les pièces d'identité des électeurs. En 2016, 35 % des OGE interrogés capturaient des données biométriques dans le cadre de leur processus d'inscription (Wolf *et al.*, 2017). L'Inde, qui dispose d'un système général d'identification biométrique comprenant l'iris, les empreintes digitales et les données faciales, étudie la possibilité d'utiliser ces données à des fins d'identification des électeurs (Livemint, 2022).

Préoccupations. Il convient de noter que dans les circonscriptions où la fraude électorale est extrêmement rare, des méthodes de vérification strictes pourraient se révéler peu efficaces pour améliorer la sécurité des élections tout en privant à tort des électeurs légitimes de leur droit de vote (Padmanabhan, Simoes et MacCarthaigh, 2023). La précision des outils de comparaison de signatures peut être de seulement 74,3 %, ce qui pourrait conduire à exclure des électeurs indûment du droit de vote (Hussain *et al.*, 2015). Bien que les taux d'erreur des systèmes biométriques soient souvent faibles, lorsqu'il y a erreur, elle peut frapper de manière disproportionnée les personnes de couleur et entraîner une privation du droit de vote relevant de la discrimination (Padmanabhan, Simoes et MacCarthaigh, 2023 ; Wolf *et al.*, 2017). La biométrie pose de sérieux problèmes de sécurité des données et de respect de la vie privée qui, outre les problèmes qu'elle pose, peuvent dissuader les électeurs soucieux du respect de la vie privée ou historiquement cibles de discriminations de participer aux élections (Wolf *et al.*, 2017). Les OGE peuvent atténuer certaines de ces préoccupations en proposant des alternatives à la vérification biométrique préalable et en créant des procédures claires et facilement accessibles de recours contre les décisions liées à des systèmes biométriques.

2.2.2. Planification

Implantation des bureaux de vote et allocation des ressources

Cas d'utilisation de l'IA. L'un des aspects essentiels du processus de planification préélectorale consiste à décider de l'affectation des ressources électorales, telles que l'implantation des bureaux de vote, le nombre d'isoloirs et le nombre d'agents électoraux dans les différents bureaux de vote. Une estimation précise des ressources nécessaires rend les processus électoraux plus accessibles, plus rapides et plus faciles pour les électeurs. Les modèles et simulations d'IA peuvent être utiles pour optimiser ce processus et, dans certains cas, le rendre plus objectif en prédisant la popularité des lieux de vote et en minimisant la distance entre les électeurs et leurs lieux de vote. De même, les modèles peuvent être utiles pour estimer les endroits où le personnel électoral est le plus nécessaire. L'utilisation de ces modèles pourrait améliorer l'accès aux bureaux de vote, ce qui pourrait avoir un impact sur les taux de participation.

Mise en œuvre. Comme le notent Padmanabhan, Simoes et MacCarthaigh (2023), bien qu'il y ait peu de preuves que l'IA soit utilisée pour sélectionner l'emplacement des sites de vote, d'autres secteurs utilisent l'IA pour optimiser l'implantation d'installations

Les modèles et simulations d'IA peuvent être utiles pour optimiser le processus de planification préélectorale.

(Al-Haidary *et al.*, 2021). Les outils de planification et d'affectation des employés basés sur l'IA peuvent être utiles pour répartir le personnel sur différents sites de vote (Talarico et Maya Duque, 2015). Les modèles construits en interne à ces fins peuvent utiliser des algorithmes supervisés, entraînés sur des scénarios « idéaux » pour les sites de vote et l'allocation des ressources sur la base de données historiques, ou des algorithmes non supervisés, visant à optimiser la distance ou l'efficacité.

Préoccupations. Le fait que les données disponibles pour les modèles ne soient pas nuancées pose un sérieux problème en ce qui concerne l'utilisation de l'IA pour sélectionner l'emplacement des bureaux de vote (par exemple, alors qu'un agent électoral peut comprendre les enjeux d'accessibilité ou de sécurité d'un lieu spécifique, les modèles peuvent ne pas tenir compte de cette nuance). Les ensembles de données peuvent également manquer d'informations sur l'accessibilité, l'importance de la communauté, la visibilité et la qualité de la salle, caractéristiques dont certaines se sont avérées avoir un impact sur les taux de participation (Mann et Stein, 2019). Les algorithmes visant à optimiser en permanence l'implantation des bureaux de vote peuvent augmenter le coût de la communication sur les nouveaux emplacements, et la volatilité pourrait troubler les électeurs, ce qui pourrait faire baisser les taux de participation (Padmanabhan, Simoes et MacCarthaigh, 2023). Bien qu'importante, la supervision humaine peut être difficile ici aussi, car les changements manuels, tels que le déplacement d'un bureau de vote, peuvent avoir un impact sur les calculs du modèle, ce qui complique encore son objectivité. L'optimisation de variables spécifiques, telles que la distance standard par rapport à un bureau de vote, pourrait entraîner une discrimination à l'encontre de certaines catégories d'électeurs, comme les électeurs en zones rurales. L'allocation générale des ressources, en termes d'isoloirs et de personnel électoral, suscite des préoccupations similaires (Kwon, Moreno et Raman, 2023).

Établissement de l'estimation de référence

Cas d'utilisation de l'IA. Dans certains cas, et en fonction de son mandat, un OGE peut souhaiter développer un ensemble de prévisions concernant divers résultats électoraux, y compris la collecte de fonds pour la campagne, les dépenses de campagne, les taux de participation des électeurs et même les résultats de l'élection. Dans tous les cas, ces estimations peuvent constituer un référentiel utile pour détecter des anomalies pendant ou après une élection. Par exemple, les prévisions concernant la collecte de

fonds pour la campagne électorale peuvent permettre aux OGE de mieux contrôler les dépenses de campagne, les demandes d'audit et les achats de médias. Les prévisions des taux de participation électorale peuvent permettre aux OGE de mieux se préparer aux besoins logistiques, tels que la fourniture des bulletins de vote avant l'élection et le dépouillement des bulletins de vote après l'élection. Les techniques statistiques traditionnelles, telles que les régressions, et les modèles d'IA plus avancés peuvent être utiles pour ces processus.

Mise en œuvre. L'estimation de référence la plus importante, qui pourrait être utile à d'autres domaines de travail des OGE, consiste à utiliser des techniques d'IA ou de science des données pour prédire les taux de participation électorale potentiels. Les OGE pourraient envisager des méthodes traditionnelles utilisées par les universitaires et les instituts de sondage à cette fin ou des méthodes plus avancées, telles que les techniques d'apprentissage à base d'arbres de décision ou de *boosting* (Moses et Box-Steffensmeier, 2021 ; Kennedy, Wojcik et Lazer, 2017). Des méthodes similaires peuvent être utiles pour prédire les dépenses de campagne et les tendances en matière de collecte de fonds, certaines recherches examinant des méthodes pour des tâches similaires dans les domaines de l'investissement, du financement participatif et des espaces à but non lucratif (Liu et Hu, 2024). Le nombre de start-ups politiques cherchant à vendre des outils d'apprentissage automatique permettant de prédire le taux de participation et la collecte de fonds pour les campagnes politiques a augmenté (Markay, 2022). Les différences substantielles entre les résultats réels et les résultats estimés peuvent servir de signal pour approfondir la question.

Préoccupations. La principale préoccupation liée à l'utilisation de l'IA pour l'estimation de référence est la forte probabilité que les techniques de modélisation produisent des résultats inexacts. Les statistiques relatives à la participation électorale et à la collecte de fonds pour les campagnes électorales sont influencées par divers facteurs, dont beaucoup ne sont pas mesurés. Il est peu probable que l'IA et les méthodes statistiques traditionnelles offrent des estimations suffisamment fiables pour permettre aux OGE de prendre de bonnes décisions ou pour servir de base de comparaison, sauf dans les situations où les prévisions diffèrent radicalement de la réalité. L'imprécision pourrait avoir une incidence sur la prise de décision des OGE et sur l'équité du processus d'audit. L'utilisation par les OGE de prédictions, sous quelque forme que ce soit, pourrait se révéler problématique pour l'intégrité électorale. En cas de fuite,

ces modèles représentent un risque important pour l'intégrité électorale, les activités de campagne et la confiance du public. Les OGE qui envisagent d'utiliser l'IA à ces fins peuvent atténuer ces préoccupations en adoptant des pratiques strictes en matière de cybersécurité et en pilotant et comparant minutieusement les nouveaux modèles afin d'en tester la fiabilité.

Il peut être utile aux OGE de prévoir le coût administratif d'une élection dans le cadre de leur processus de budgétisation.

Prévision des coûts des élections

Cas d'utilisation de l'IA. Il peut être utile aux OGE de prévoir les coûts administratifs d'une élection dans le cadre de leur processus de budgétisation. Comme les élections ont de nombreux coûts variables, allant de l'achat de machines à voter et de bulletins de vote à l'embauche d'agents électoraux, l'IA peut être utile pour améliorer les estimations de l'équipement, du personnel et des autres ressources nécessaires. De nombreux OGE effectuent déjà des prévisions approximatives à des fins budgétaires, en se basant souvent sur le scénario le plus défavorable des élections précédentes, mais l'IA peut permettre d'obtenir des estimations plus précises. Comme pour l'allocation des ressources et l'établissement d'estimations de référence, les modèles d'IA peuvent offrir des prévisions approximatives de divers coûts, tels que ceux liés à la sécurité des élections, aux machines de vote, aux employés, aux bulletins de vote en papier et autres.

Mise en œuvre. Peu de recherches ont été menées sur les coûts de la gestion électorale, et nous n'avons pas pu trouver de travaux utilisant l'IA (Clark, 2019). Cependant, certaines recherches ont examiné le rôle que les algorithmes d'apprentissage profond peuvent jouer dans les stratégies de budgétisation des gouvernements, généralement en utilisant les dépenses potentielles comme intrants pour optimiser des résultats spécifiques (Valle-Cruz, Fernandez-Cortez et Gil-Garcia, 2022). Les progrès réalisés dans l'utilisation de l'apprentissage automatique dans les domaines de la prédiction des risques et de la tarification des assurances peuvent servir de point de départ utile (Kan *et al.*, 2019).

Préoccupations. En l'absence de recherches sur les méthodes de prévision des coûts électoraux, la principale préoccupation liée à l'utilisation de l'IA à cette fin est la précision. Les modèles peu précis, en particulier ceux qui servent à prendre des décisions, risquent de sous-préparer les OGE, ce qui pourrait avoir de graves conséquences sur l'intégrité électorale. Les OGE peuvent être en mesure d'atténuer ces préoccupations en pilotant des prévisions basées sur l'IA et en testant leur précision par rapport aux méthodes existantes.

Prévision de la sécurité/violence électorale

Cas d'utilisation de l'IA. Afin de maintenir la sécurité et l'intégrité des élections, les OGE et les agences de sécurité peuvent bénéficier de prévisions sur les sites où la violence électorale pourrait potentiellement survenir. Un peu comme dans les sections précédentes, les modèles entraînés sur les zones où des actes de violence se sont déjà produits ou les zones présentant d'autres corrélats de violence peuvent aider les OGE à décider où prioriser les services de sécurité. En outre, les LLM peuvent être utiles pour détecter les messages sur les réseaux sociaux concernant des violences prévues ou potentielles dans différents lieux de vote. Combinés, ces modèles peuvent permettre aux OGE de prévoir les lieux de vote à haut risque et d'empêcher la violence de se produire.

Mise en œuvre. Les modèles supervisés entraînés sur des sites de vote ou des zones géographiques ayant déjà connu des problèmes de violence électorale peuvent être utiles pour prédire où des incidents futurs se produiront (Padmanabhan, Simoes et MacCarthaigh, 2023). Des LLM affinis, exécutés sur des messages des réseaux sociaux, peuvent être utiles pour signaler des menaces potentielles de violence ou pour mettre en évidence des zones spécifiques recevant une attention démesurée de la part de groupes violents. Bien qu'il y ait peu de travaux sur les sites de vote en particulier, l'IA est utilisée depuis longtemps à des fins de police prédictive, de nombreux gouvernements et entreprises privées développant des outils dans ce but (Hardyns et Rummens, 2018).

Préoccupations. Les efforts de police prédictive sont très controversés, avec de sérieuses préoccupations en matière d'éthique et de droits humains concernant sa précision et la discrimination. En raison du manque de données de haute qualité, des biais existants et de l'impossibilité d'interpréter la plupart des algorithmes d'apprentissage profond, il est prouvé que ces systèmes perpétuent les inégalités systémiques dans le maintien de l'ordre sans preuve solide d'efficacité (Gstrein, Bunnik et Zwitter, 2019 ; Richardson, Schultz et Crawford, 2019). Il existe peu de preuves que le maintien de l'ordre prédictif donne des résultats efficaces, mais de nombreux travaux décrivent son potentiel d'exacerbation des violations des droits humains, notamment des droits civils (Van Brakel, 2016). Le renforcement de la présence policière dans les bureaux de vote peut réduire les taux de participation, avoir un impact sur les résultats électoraux et amenuiser la confiance dans le processus (Padmanabhan, Simoes et MacCarthaigh, 2023).

Les LLM peuvent être utiles pour détecter les messages sur les réseaux sociaux concernant des violences prévues ou potentielles dans différents lieux de vote.

2.2.3. Éducation civique et mobilisation des électeurs

Échange d'informations électorales

Cas d'utilisation de l'IA. L'IA, en particulier les LLM, peut être utile pour adapter les informations électorales à des sous-ensembles spécifiques de la population. Comme de nombreux OGE ont pour mandat d'accroître l'équité et l'accès au vote, l'utilisation de diverses stratégies de communication pour différents sous-ensembles de la population peut être un moyen de garantir un accès égal à l'information. Cette communication différenciée est particulièrement pertinente pour les électeurs ayant des connaissances techniques limitées, car l'IA peut être utilisée de manière à développer des façons de présenter les informations électorales de façon à ce qu'elles soient comprises de manière plus intuitive. Par exemple, les chatbots (ou agents conversationnels) basés sur le LLM entraînés sur les informations des OGE et les questions fréquemment posées peuvent constituer un moyen utile pour les OGE de proposer des informations existantes dans un format adapté aux questions spécifiques des électeurs, plus facile à utiliser que la navigation manuelle sur les sites web électoraux (Eisen *et al.*, 2023).

Mise en œuvre. Certaines recherches ont développé une architecture de chatbot visant à améliorer l'accès aux informations électorales pour les personnes âgées et les électeurs qui votent pour la première fois ; le chatbot est entraîné spécifiquement pour répondre aux questions fréquemment posées aux OGE (Muppasani *et al.*, 2023). Les OGE doivent être prudents lorsqu'ils utilisent des chatbots, en veillant à utiliser des technologies en boucle fermée telles que la génération augmentée de récupération pour s'assurer que le LLM n'utilise que des informations prédéfinies pour répondre aux requêtes.

Préoccupations. L'utilisation de chatbots de LLM pour la gestion des élections pose de sérieux problèmes de validité des informations ; les OGE devront procéder à des tests et à des audits approfondis pour éviter les hallucinations des LLM et la diffusion de fausses informations (Rawte, Sheth et Das, 2023). Les audits de sécurité sont nécessaires compte tenu de la capacité des acteurs malveillants à « s'évader de prison » ou à exploiter les LLM pour faire fuiter des données ou fournir des informations incorrectes (Wei, Haghtalab et Steinhart, 2023). Même avec une faible probabilité d'erreurs, toute fausse information partagée par un chatbot approuvé par l'OGE est susceptible de provoquer une controverse et de compromettre l'intégrité électorale. Les OGE peuvent être en mesure d'atténuer ces

problèmes en procédant à des tests et à des audits approfondis, ainsi qu'en utilisant des modèles dont les probabilités d'hallucination sont limitées.

Publicité ciblée

Cas d'utilisation de l'IA. Les OGE qui ont pour mission d'augmenter le taux de participation électorale ou de diffuser des informations sur les élections auprès de diverses populations peuvent tirer parti de l'IA pour créer des campagnes publicitaires ciblées. La publicité ciblée peut être utile pour améliorer l'accès à l'information pour les personnes qui ne sont pas normalement impliquées dans les processus électoraux. Les modèles d'IA générative peuvent être en mesure d'automatiser le processus de création ou d'élaboration de la première version d'une publicité destinée à de petits groupes de population. L'IA, en particulier les modèles non supervisés, tels que les modèles de regroupement, peut être utile pour identifier les groupes qui ont été historiquement négligés dans les communications de l'OGE.

Mise en œuvre. La plupart des travaux sur le rôle de l'IAg dans la mobilisation des électeurs se concentrent sur le rôle qu'elle peut jouer dans la publicité à caractère politique ciblée de la part des chargés de campagne et des organisations affiliées. Certains travaux montrent que l'utilisation d'outils d'IAg pour modifier les publicités en fonction des traits de personnalité des utilisateurs a entraîné une augmentation de l'engagement (Simchon, Edwards et Lewandowsky, 2024). Des travaux antérieurs étudiant les publicités microciblées sur Facebook ont révélé un impact sur les taux de participation uniquement lors d'élections américaines très concurrentielles (Haenschen, 2022). La mise en œuvre nécessiterait l'intégration de données sur les utilisateurs (généralement fournies par les entreprises de réseaux sociaux) dans les outils d'IAg afin de générer des publicités ciblées pour des sous-ensembles de la base d'utilisateurs.

Préoccupations. Le microciblage, en particulier sous l'impulsion de l'IAg, soulève de sérieuses préoccupations concernant la confidentialité, la manipulation et l'exactitude des données. Les électeurs peuvent désapprouver l'utilisation de leurs données personnelles dans le but de les inciter à voter, et les interventions réussies risquent de créer des inégalités dans le processus électoral et de remettre en question l'intégrité des élections. Les systèmes entièrement automatisés peuvent donner lieu à des hallucinations, à des informations incorrectes sur les élections ou à des préjugés

Les OGE qui ont pour mission d'augmenter le taux de participation électorale ou de diffuser des informations sur les élections auprès de diverses populations peuvent tirer parti de l'IA pour créer des campagnes publicitaires ciblées.

politiques de la part des outils d'IAg. En outre, le processus de sélection des groupes à microcibler et les plateformes utilisées pour diffuser ces publicités soulèvent des inquiétudes quant à la création d'inégalités, car les OGE peuvent faire de la publicité de manière disproportionnée auprès de certains sous-groupes de la population (Ali *et al.*, 2019). L'utilité potentielle de ces outils n'a pas encore fait l'objet de recherches suffisantes, et il se peut qu'ils n'aient pas d'impact significatif sur les taux de participation par rapport à des stratégies plus générales de mobilisation des électeurs, ce qui peut soulever la question de la proportionnalité.

2.3. PÉRIODE ÉLECTORALE

La période électorale est la partie du cycle électoral où l'accent est mis sur la campagne, le vote, le suivi et la compilation des résultats.

2.3.1. Surveillance de la campagne et des médias

Veille de la désinformation sur les réseaux sociaux

Cas d'utilisation de l'IA. L'un des cas d'utilisation potentiels de l'IA pour les OGE est le recours aux LLM et réseaux neuronaux graphiques sur les plateformes de réseaux sociaux pour détecter et résumer les fausses informations courantes concernant les élections. Les LLM peuvent être en mesure de détecter les tendances en matière de désinformation et de signaler les cas les plus préoccupants, tels que les catégories de messages contenant des informations trompeuses sur la date ou le lieu d'une élection ou sur la capacité à voter de certains électeurs. Les modèles peuvent également être utiles pour détecter des messages spécifiques qui violent les lois électorales. Cela pourrait permettre aux OGE d'élaborer des plans pour réagir plus rapidement et plus facilement qu'en surveillant manuellement les plateformes de réseaux sociaux, éléments clés pour réduire l'impact de la désinformation sur les élections. La menace de la désinformation électorale sur les réseaux sociaux est examinée plus en détail au chapitre 3.

Mise en œuvre. Un nombre non négligeable de recherches portent sur l'utilisation des LLM pour détecter ou résumer les tendances en matière de désinformation, et diverses entreprises privées et organisations à but non lucratif travaillent à l'élaboration d'outils pour cette tâche (Kondamudi *et al.*, 2023 ; Dhiman *et al.*, 2023). La mise en œuvre de ces outils nécessitera une planification minutieuse

pour inclure des informations sur le contexte spécifique d'une élection, une formation aux langues parlées dans la circonscription concernée, l'identification des plateformes clés sur lesquelles les fausses informations sont diffusées et le recours à des observateurs humains. Des partenariats avec des plateformes, des *fact-checkeurs* (ou initiatives de vérification des informations) et d'autres tiers peuvent s'avérer utiles pour accéder aux informations erronées en relation avec les élections, les supprimer et y remédier.

Préoccupations. Une dépendance excessive à l'égard de l'IA pour la détection des fausses informations pourrait conduire les OGE à passer à côté de sujets et de préoccupations essentiels, en particulier sur les plateformes de messagerie privée (par exemple WhatsApp), où la disponibilité des données est limitée. La plupart des LLM sont optimisés principalement pour la langue anglaise, et souvent pour le contexte américain, ce qui pourrait faire passer les modèles à côté de détails importants. La détection des fausses informations nécessite une compréhension claire de ce qui constitue une fausse information et de la légalité du contrôle ou de la réponse à cette mésinformation. Les OGE peuvent être en mesure d'atténuer ces préoccupations en n'utilisant l'IA que dans le cadre d'une stratégie plus large de lutte contre la mésinformation. Des questions relatives à la liberté d'expression, à la surveillance et au contrôle des plateformes publiques par le gouvernement peuvent se poser, notamment en ce qui concerne les droits humains, plus particulièrement la liberté d'expression (Commission interaméricaine des droits de l'homme, 2017).

Surveillance de la campagne et des médias

Cas d'utilisation de l'IA. Dans de nombreux pays, les OGE sont chargés de contrôler le contenu et le calendrier des communications émanant des chargés de campagne, d'autres groupes politiques et des organisations médiatiques. Par exemple, certains pays imposent une période de silence électoral avant le scrutin, or l'IA peut aider à détecter les violations éventuelles. Des LLM affinés avec les réseaux sociaux et les flux de données Internet peuvent être utiles pour signaler un contenu spécifique qui va à l'encontre des directives de l'OGE, de manière similaire au processus décrit pour la détection de la mésinformation.

Mise en œuvre. La mise en œuvre de cette tâche sera plus personnalisée que celle de la détection de fausses informations, car peu de travaux ont été réalisés sur le sujet. Les LLM peuvent être affinés à partir d'ensembles de données sur les contenus

« autorisés » et « interdits », puis alimentés par les comptes de réseaux sociaux des campagnes politiques et des organisations médiatiques afin de les signaler en cas de violations potentielles.

Préoccupations. Comme dans le cas de la détection de la mésinformation, une dépendance excessive à l'égard des outils basés sur l'IA à cette fin suscite de vives inquiétudes, car ceux-ci sont susceptibles de passer à côté d'infractions potentielles. En outre, les modèles peuvent fonctionner de manière discriminatoire, en détectant davantage de violations de la part d'un parti politique, par exemple, en raison de données de formation mal conçues. Cela pourrait avoir des effets discriminatoires si ce n'est pas compensé par d'autres formes d'observation. Pour atténuer certains de ces problèmes, les OGE qui envisagent ce cas d'utilisation devraient le faire dans le cadre d'une stratégie plus large de supervision des médias.

2.3.2. Opérations de vote

Pièces d'identité de l'électeur

Cas d'utilisation de l'IA. Les modèles d'IA peuvent être utiles pour vérifier les pièces d'identité des électeurs. De nombreux OGE et gouvernements utilisent déjà des outils technologiques pour scanner et comparer les pièces d'identité aux bases de données existantes, et l'IA peut améliorer la précision de ces technologies. Les modèles peuvent permettre aux agents électoraux de vérifier que l'adresse d'un électeur se situe dans la circonscription électorale.

Mise en œuvre. Étant donné que de nombreux OGE utilisent déjà des outils matériels et logiciels pour la vérification des pièces d'identité, la mise en œuvre de l'IA peut impliquer la mise à jour des modèles utilisés pour la numérisation et la vérification des documents. Des modèles supervisés, entraînés sur des pièces d'identité valides et non valides, sont susceptibles d'être les plus utiles pour cette tâche. Les outils de reconnaissance optique des caractères et des marques (OCR/OMR) basés sur l'IA peuvent être utiles pour scanner et interroger des formes d'identification non standard.

Préoccupations. Dans de nombreux cas, les outils de vérification de l'identité reposent sur la lecture de codes-barres, de bandes magnétiques ou de puces sécurisées sur ou à l'intérieur des documents d'identité et des cartes. Ces approches sont susceptibles d'être plus performantes que les modèles d'IA, car elles ne reposent pas sur l'inférence ou les prédictions. Les modèles d'IA peuvent

être moins précis que les formes traditionnelles de vérification de l'identité. Il convient de noter que dans les pays où les taux de fraude électorale ou de possession d'une pièce d'identité sont faibles, l'obligation d'identification des électeurs est susceptible de priver les électeurs de leur droit de vote sans avoir d'incidence sur la sécurité des élections (Hajnal, Kuk et Lajevardi, 2018).

Biométrie et identification des électeurs

Cas d'utilisation de l'IA. Comme indiqué au point 2.2.1, les modèles d'IA peuvent être utiles aux pays qui utilisent la reconnaissance biométrique (par exemple, l'iris, le visage, la paume de la main, l'empreinte du pouce) pour vérifier l'identité des électeurs. Un modèle peut comparer les données biométriques d'une personne présentées lors de l'inscription ou d'autres processus officiels avec les données biométriques d'une personne présentant un bulletin de vote. Cela peut permettre d'authentifier les électeurs sans pièce d'identité et d'améliorer la sécurité des élections.

Mise en œuvre. La mise en œuvre de cette tâche est un processus en deux étapes : d'abord la conception d'un système pour capturer les informations biométriques au cours du processus d'inscription (voir 2.2.1) et ensuite la vérification de ces données biométriques sur le lieu de vote. C'est dans cette partie du processus que l'IA est la plus susceptible d'être utilisée, avec des modèles d'apprentissage profond pour faire correspondre les hachages biométriques. Ces modèles seront probablement développés par des prestataires externes, car ils nécessitent de grands ensembles de données de formation que les OGE n'auront probablement pas la capacité de constituer eux-mêmes. Comme nous l'avons déjà mentionné, en 2016, 35 % des OGE interrogés enregistraient des données biométriques au cours du processus d'inscription (Wolf *et al.*, 2017). Certains pays, dont l'Inde, pilotent l'utilisation de ces données pour l'identification des électeurs (Livemint, 2022). Les outils de comparaison de signatures basés sur l'IA sont régulièrement utilisés lors d'élections, au moins 29 des plus grands comtés des États-Unis les utilisant pour vérifier les bulletins de vote par correspondance (Bender, 2022).

Préoccupations. Comme indiqué au point 2.2.1, la fraude électorale est extrêmement rare dans de nombreuses circonscriptions, et les méthodes de vérification peuvent causer beaucoup plus de tort que de bien en fonction des circonstances spécifiques d'un pays (Padmanabhan, Simoes et MacCarthaigh, 2023). En outre, la précision des outils de comparaison de signatures peut être aussi faible que 74,3 %, ce qui pourrait exclure indûment des électeurs

Les modèles d'IA peuvent être utiles aux pays qui utilisent la reconnaissance biométrique pour vérifier l'identité des électeurs.

du droit de vote (Hussain *et al.*, 2015). Bien que les taux d'échec des systèmes biométriques soient souvent faibles, lorsqu'ils échouent, ils peuvent échouer de manière démesurée pour les personnes de couleur et entraîner une privation discriminatoire du droit de vote (Padmanabhan, Simoes et MacCarthaigh 2023 ; Wolf *et al.*, 2017). Les systèmes biométriques posent de sérieux problèmes en matière de sécurité des données, de respect de la vie privée et de droits humains, et risquent de dissuader les gens de participer aux processus électoraux. Cela soulève des questions de proportionnalité : les risques de sécurité associés, les préoccupations potentielles en matière de droits humains et les probabilités de privation de droits l'emportent-ils sur les avantages de l'identification biométrique ?

2.3.3. Surveillance des bureaux de vote

Détection des incidents dans les bureaux de vote

Cas d'utilisation de l'IA. Au cours des dernières années, les électeurs ont fréquemment publié sur les plateformes de réseaux sociaux des plaintes concernant des problèmes concernant les élections et survenus dans des bureaux de vote. Il peut s'agir de machines qui ne fonctionnent pas, de longues files d'attente, de suppression d'électeurs ou de comportements illégaux. Les LLM peuvent être utilisés pour mener une veille sur les plateformes de réseaux sociaux à la recherche de ces plaintes, les classer automatiquement par catégories et les transmettre aux autorités compétentes.

Mise en œuvre. Il est prouvé que des LLM affinés peuvent détecter des rapports d'incidents dans les bureaux de vote lors des élections américaines avec un degré élevé de précision (Juneja et Floridi, 2023). La mise en œuvre nécessite l'accès aux données des réseaux sociaux, très probablement par le biais de partenariats avec des plateformes, pour des mots clés spécifiques liés aux élections et la création d'ensembles de données étiquetés « incidents » et « non-incidents ». Comme dans le cas de la détection de fausses informations, les observateurs humains doivent vérifier les incidents potentiels pour en assurer le suivi.

Préoccupations. Des préoccupations similaires à celles concernant l'observation de la mésinformation sur les plateformes de réseaux sociaux se posent ici, notamment le risque de passer à côté d'informations en raison d'une confiance excessive dans les solutions d'IA et d'une inégalité potentielle des performances. En tant que tels, les outils devraient être utilisés en complément des

méthodes existantes de détection des incidents dans les bureaux de vote. En outre, la collecte massive de données publiques par les gouvernements, en particulier concernant les sujets politiques, soulève de graves préoccupations en matière de surveillance, de protection de la vie privée et de droits humains, et pourrait potentiellement se révéler problématique pour la liberté d'expression (Commission interaméricaine des droits de l'homme, 2017).

Vidéosurveillance

Cas d'utilisation de l'IA. La vidéosurveillance basée sur l'IA peut servir plusieurs objectifs pendant les élections. Les modèles d'IA utilisant la vidéosurveillance pour surveiller les bureaux de vote peuvent être en mesure de détecter des incidents ou des anomalies (par exemple, si un ensemble d'images de vidéosurveillance semble différent de l'ensemble moyen d'images). En outre, les modèles d'IA peuvent servir à détecter les fraudes électorales si une personne apparaît deux fois sur le même site de vote ou sur plusieurs sites de vote (Padmanabhan, Simoes et MacCarthaigh, 2023). Dans tous les cas, ces incidents peuvent être signalés pour être suivis par les agents de l'OGE ou par les observateurs électoraux.

Mise en œuvre. La mise en œuvre nécessitera des capacités étendues de vidéosurveillance et l'infrastructure nécessaire pour alimenter les modèles de reconnaissance d'images et de vidéos par l'IA à partir des données fournies par les caméras. Il peut également être important d'affiner les modèles pour des tâches telles que la reconnaissance faciale et la détection d'anomalies (par exemple, la caractérisation des comportements appropriés et inappropriés dans les bureaux de vote).

Préoccupations. Les outils de vidéosurveillance basés sur l'IA sont connus pour fonctionner de manière discriminatoire, et il est prouvé que le taux d'erreurs de la technologie de reconnaissance faciale est disproportionnellement plus élevé en relation avec les visages non blancs (Perkowitz, 2021). L'inexactitude des modèles, en particulier en ce qui concerne la détection des fraudes, peut susciter des inquiétudes quant à l'intégrité des élections et pourrait accroître la charge de travail des OGE et des enquêteurs chargés de la lutte contre la fraude électorale. En outre, toute forme de surveillance de masse, en particulier par les gouvernements, peut susciter de graves préoccupations en matière de droits humains, décourageant probablement les électeurs soucieux de leur vie privée ou historiquement cibles de discrimination d'exercer leur liberté d'expression et leur droit de vote.

2.3.4. Dépouillement et analyse des votes

Comptage et compilation

Cas d'utilisation de l'IA. Les systèmes OCR/OMR, qui utilisent des outils technologiques pour lire les formulaires remplis et écrits, sont déjà régulièrement utilisés pour le dépouillement et la compilation des votes à l'urne et par correspondance. Ces systèmes peuvent être utilisés avec différents types de bulletins, y compris des bulletins spécialement conçus pour les systèmes OCR/OMR ou des bulletins remplis manuellement. Ils peuvent également être utilisés à différentes étapes du processus, notamment lorsque les électeurs déposent leurs bulletins, dans les bureaux de vote, pour les bulletins par correspondance, lorsque les bulletins sont centralisés et pour les feuilles de dépouillement. Les systèmes OCR/OMR peuvent également être utilisés pour scanner les signatures. L'IA peut améliorer les systèmes OCR/OMR traditionnels, car les cas limites posent souvent des problèmes aux systèmes automatisés existants (Zhao *et al.*, 2023). Ces systèmes pourraient être utilisés pour détecter des différences ou des anomalies parallèlement aux méthodes existantes de comptage des voix. Ces systèmes peuvent inclure, par exemple, des modèles d'IA de vision par ordinateur entraînés pour compter les bulletins de vote papier, reconnaître les adjonctions manuscrites de noms de candidats, et reconnaître et vérifier les signatures.

Mise en œuvre. Les outils de comparaison de signatures basés sur l'IA développés par des entreprises privées sont largement utilisés lors des élections pour vérifier les bulletins de vote par correspondance, et des outils similaires peuvent être appliqués à d'autres formes de comptage des bulletins de vote qui nécessitent des signatures (Bender, 2022). Dans de nombreux pays, les outils existants s'appuient sur des formes rudimentaires d'IA pour compter les bulletins de vote papier standardisés pouvant être scannés (MIT Election Data Science Lab, 2023). Les approches basées sur l'apprentissage profond ont montré des améliorations par rapport à la technologie traditionnelle dans certaines recherches, avec une précision testée atteignant 99,984 % (Barretto *et al.*, 2021 ; Zhao *et al.*, 2023).

Préoccupations. Bien qu'il soit prouvé que les systèmes basés sur l'IA sont plus performants que les technologies traditionnelles de dépouillement automatisé des bulletins de vote, même très faibles, les taux d'erreur peuvent affecter à la fois l'intégrité électorale et la confiance du public dans les élections. C'est particulièrement

vrai pour les modèles d'apprentissage profond ininterprétables, pour lesquels les erreurs et les cas limites peuvent être difficiles à expliquer au public. En outre, les outils de comparaison de signatures peuvent présenter des taux de précision aussi bas que 74,3 % (Hussain *et al.*, 2015). En Indonésie, par exemple, le système Sirekap, basé sur la reconnaissance optique des caractères (OCR) pour scanner les feuilles de dépouillement, a fait l'objet d'une controverse à la suite d'informations faisant état d'irrégularités dans les données de comptage des voix (Suhenda, 2024). Pour atténuer ces préoccupations, les OGE devraient effectuer des tests de comparaison approfondis avec les méthodes existantes, mettre en place une surveillance humaine et envisager d'utiliser l'IA comme méthode supplémentaire, et non comme méthode de remplacement, pour le dépouillement des bulletins de vote.

Analyse de la participation et détection des anomalies en temps réel

Cas d'utilisation de l'IA. De nombreux OGE examinent régulièrement, et dans certains cas publient, les taux de participation tout au long de la journée électorale afin de gérer la logistique et de détecter les anomalies potentielles. L'IA, sous la forme de modèles statistiques traditionnels et de modèles d'apprentissage profond, peut être utile pour accroître l'importance de ces données en surveillant les mesures de participation dans les bureaux de vote ou dans des zones géographiques spécifiques qui sont significativement différentes des attentes. Cette surveillance peut alerter sur des problèmes potentiels, notamment des incidents dans les bureaux de vote, des suppressions d'électeurs ou des fraudes électorales, sur lesquels les responsables peuvent choisir d'enquêter.

Mise en œuvre. Bien que nous n'ayons pu trouver aucune recherche sur l'analyse en temps réel d'une élection, la mise en œuvre sera similaire aux audits post-électorales. Les modèles élaborés avant les élections, qui prévoient la participation des électeurs et les résultats tout au long de la journée électorale, peuvent être comparés aux résultats en temps réel fournis par les bureaux de vote. Si des différences significatives apparaissent entre les résultats prévus et les résultats réels, les OGE peuvent choisir d'enquêter sur des sites de vote spécifiques pour détecter d'éventuels problèmes.

Préoccupations. Étant donné qu'il est peu probable que les simulations préélectorales soient parfaitement exactes, les modèles développés pour détecter les anomalies de participation tout au long de la journée électorale peuvent avoir une forte probabilité de

faux positifs, ce qui pourrait entraîner une mauvaise affectation des ressources de l'OGE pour enquêter sur les sites de vote, en interférant potentiellement avec des sites de vote parfaitement fonctionnels et en passant à côté de problèmes réels sur d'autres sites. Le développement de systèmes sûrs et précis pour ce cas d'utilisation est une tâche techniquement difficile, car les modèles doivent tenir compte non seulement de la tâche déjà difficile de prédire les taux de participation totaux, mais aussi de la façon dont la participation peut varier tout au long de la période électorale.

Encadré 2.1. Les élections numériques

Il convient de noter que l'IA peut être utile aux pays qui explorent de nouvelles formes de scrutin et d'élections. Par exemple, dans les pays dotés de systèmes de vote en ligne où les électeurs utilisent leurs propres appareils, l'IA peut s'avérer utile pour diverses tâches. Par exemple, les systèmes de vote en ligne peuvent utiliser des logiciels de reconnaissance faciale basés sur l'IA pour l'identification, des modèles entraînés à la détection de l'activité des robots ou des données anormales sur les pages web pour examiner la fraude électorale, et des modèles censés analyser les menaces de cybersécurité pour protéger l'intégrité des serveurs. L'IA peut également être utile pour créer des agents utilisateurs simulés afin de tester les vulnérabilités et les problèmes potentiels des systèmes de vote en ligne.

Dans les pays qui explorent de nouvelles formes de gouvernance démocratique, telles que la démocratie participative en ligne, les

LLM peuvent être utiles pour résumer les positions et les croyances des électeurs, et les modèles de regroupement peuvent être utiles pour regrouper des idées et des déclarations similaires (Eisen *et al.*, 2023). Par exemple, les pays qui cherchent à recevoir des commentaires sur des politiques spécifiques peuvent créer des plateformes sur lesquelles les utilisateurs peuvent commenter et partager leurs opinions, puis utiliser une combinaison d'IA et de supervision humaine pour mieux comprendre les croyances des participants et, dans certains cas, même parvenir à des solutions de compromis. À Taïwan, le programme vTaiwan utilise la plateforme Polis pour solliciter des commentaires participatifs sur les positions politiques, les modèles d'IA étant utilisés pour la synthèse et le regroupement, et les chatbots étant utilisés pour parler au nom de positions spécifiques (Landemore, 2023).

2.4. PÉRIODE POST-ÉLECTORALE

La période post-électorale est la phase du cycle électoral au cours de laquelle l'accent est mis sur l'examen, l'analyse, la réforme et la stratégie de l'élection.

2.4.1. Analyse et communication des résultats électoraux

Audits post-électoraux

Cas d'utilisation de l'IA. L'IA peut être utile pour les pratiques d'audit post-électorale. Par exemple, l'IA peut être utilisée pour détecter des incidents frauduleux, et les modèles développés avant une élection peuvent fournir des termes de comparaison avec les résultats réels. En outre, l'apprentissage automatique et les statistiques traditionnelles, telles que les estimateurs de doubles différences, peuvent être utilisés pour évaluer l'efficacité et l'affectation des ressources de divers bureaux de vote. Les algorithmes de partitionnement peuvent être utiles pour repérer les sites de vote qui présentent des différences significatives par rapport aux autres.

Mise en œuvre. La recherche a examiné le rôle que peuvent jouer les algorithmes non supervisés et supervisés entraînés sur les données des sondages dans la détection de la fraude électorale. Dans certains cas, ces modèles utilisent des techniques de simulation entraînées sur des données de sondage et des données électorales connexes afin de déterminer dans quelle mesure les résultats réels sont similaires aux résultats simulés. En général, ces modèles nécessitent des niveaux élevés de fraude afin de fournir un haut degré d'exactitude, de précision (c.-à-d. un faible nombre de faux positifs) et de rappel (c.-à-d. un faible nombre de faux négatifs) (Yamin *et al.*, 2023). En lieu et place des sondages, d'autres tentatives ont utilisé des données synthétiques, générant une version manipulée et non manipulée des résultats électoraux, pour former un modèle qui est ensuite appliqué à d'autres élections. Ces travaux ont montré que cette technique pouvait constituer un point de départ utile pour d'autres recherches en criminalistique électorale (Zhang, Alvarez et Levin, 2019). Les algorithmes non supervisés peuvent également se révéler utiles, en permettant aux OGE de regrouper les bureaux de vote et de rechercher et signaler les anomalies potentielles (Green, 2021). Les OGE devraient envisager d'utiliser des seuils de probabilité prédéfinis pour éliminer les faux positifs (par exemple, en n'examinant que les zones géographiques pour lesquelles les modèles prévoient une probabilité de fraude supérieure à 90 %).

Problèmes. Comme il est peu probable que les OGE aient accès à des ensembles de données contenant des cas de fraude électorale parfaitement étiquetés, il est difficile de développer des modèles supervisés adaptés à cette tâche. Le manque de données de référence rend difficile l'évaluation de l'adéquation d'un modèle. Un faible rappel et une confiance excessive peuvent amener les OGE à passer à côté de cas de fraude électorale et d'autres problèmes, tandis qu'une faible précision peut amener les OGE à enquêter sur un grand nombre de faux positifs. Ces deux problèmes pourraient ébranler la confiance du public dans l'intégrité électorale. Les OGE qui envisagent de mettre en œuvre ce cas d'utilisation de l'IA peuvent atténuer certaines de ces préoccupations en l'utilisant comme un élément d'une approche d'audit plus large.

Consolidation du financement politique

Cas d'utilisation de l'IA. L'IA peut être utile pour la consolidation et l'audit des documents et rapports de financement politique pendant et après une élection. Les modèles d'OCR peuvent permettre de numériser des reçus physiques et les modèles de correspondance peuvent permettre de développer des pistes d'audit à partir des rapports de financement politique. Les LLM et les modèles de résumé peuvent également être utiles pour consolider les diverses dépenses de campagne et les dons dans des formats standardisés que les responsables électoraux peuvent examiner. L'IA peut être utile pour détecter les fraudes en matière de financement politique, par exemple lorsque des personnes font des dons sous des noms/adresses différents ou font des dons inéligibles.

Mise en œuvre. Bien que nous n'ayons pas pu trouver de recherches portant sur ce cas d'utilisation spécifique, l'IA est de plus en plus utilisée dans l'audit financier des entreprises, certaines pratiques étant transposables au financement politique. Par exemple, les quatre plus grands cabinets comptables mondiaux (Deloitte, EY, KPMG et PwC) proposent tous une version ou une autre des outils d'IA pour l'audit des entreprises, notamment la détection des anomalies, la détection des fraudes, les audits de trésorerie automatisés et la détection des schémas (Üçoğlu, 2020). Des modifications d'outils similaires peuvent être utiles pour retracer les dons et les dépenses politiques. Les outils de vision par ordinateur et de reconnaissance optique des caractères peuvent être utilisés pour la saisie des données, et les outils d'IAg peuvent être utiles pour mettre les documents de déclaration dans des formats de données normalisés afin d'alimenter les systèmes d'audit.

Préoccupations. Les outils d'IA utilisés pour consolider les données peuvent souffrir d'hallucinations ou d'autres problèmes de précision, ce qui pourrait entraîner des faux positifs ou permettre aux OGE de passer à côté d'informations importantes. Étant donné qu'il ne semble pas y avoir d'outils créés spécifiquement pour la consolidation du financement politique, il faudra également travailler à affiner les outils existants afin de répondre aux demandes particulières des OGE, par exemple en incorporant des réglementations sur les plafonds de dons et de dépenses, ce qui pourrait accroître la complexité et diminuer l'efficacité des approches de l'IA.

2.5. AUTRES DÉFIS, PRÉOCCUPATIONS ET STRATÉGIES D'ATTÉNUATION

L'utilisation de l'IA pour la gestion des élections est prometteuse dans de nombreux domaines, car elle permet d'améliorer les résultats, d'accroître l'efficacité et de mettre en place des systèmes plus équitables. Dans le même temps, elle suscite ou exacerbe souvent de sérieuses préoccupations.

Dans les sections précédentes, nous avons fait part d'une série de préoccupations liées à chaque utilisation potentielle spécifique de l'IA pour les OGE. Il convient de noter que, dans tous les cas, il existe d'importants problèmes éthiques, pratiques et relatifs aux droits humains, allant d'une mise en œuvre techniquement difficile à de graves problèmes d'intégrité électorale. Outre ces préoccupations spécifiques, cette section aborde d'autres questions susceptibles d'être soulevées par l'utilisation de l'IA dans le cadre de la gestion des élections, telles que les vulnérabilités en matière de cybersécurité, la consolidation privée de l'infrastructure publique, les droits humains, les préjugés et la discrimination, et la confiance du public dans les élections.

Dans certains cas, ces problèmes peuvent être résolus ; dans d'autres, ils sont susceptibles de se produire lors de la mise en œuvre du cas d'utilisation de l'IA. Bien qu'elles n'entrent pas totalement dans le cadre du présent rapport, certaines stratégies d'atténuation potentielles sont incluses pour répondre à certaines de ces préoccupations et encourager les OGE à aborder la mise en œuvre de l'IA dans le cadre d'un processus éclairé d'analyse des possibilités et des contraintes de chaque cas d'utilisation.

Encadré 2.2. Utilisation de chatbots d'IA généralistes au sein des OGE

Après avoir abordé les cas d'utilisation spécifiques de l'IA pour les OGE, il convient de discuter de la manière la plus immédiate dont les OGE peuvent commencer à utiliser les outils d'IA dans leur travail : pour une aide généraliste. Les chatbots IA généralistes, tels que ChatGPT d'OpenAI, Copilot de Microsoft et Gemini de Google, sont déjà largement utilisés dans les cadres privé et professionnel, et il est probable que de nombreux responsables d'OGE ont déjà commencé à examiner officiellement, ou officieusement, la capacité de ces outils à améliorer la productivité interne.

Dans la plupart des cas, ces outils sont principalement accessibles via une interface de chatbot, où les utilisateurs envoient des questions ou des commandes (ou *prompts*) au modèle, qui génère des réponses et d'autres résultats. Ces outils peuvent être utilisés pour résumer des informations dans des documents existants, rédiger des contenus pour des courriels, des documents ou des présentations, et consolider des informations provenant d'Internet. Dans certains cas, comme l'intégration de Copilot par Microsoft, les modèles peuvent produire du contenu autre que du texte, notamment générer des images, modifier des feuilles de calcul ou éditer des présentations.

Pour les OGE, ces outils peuvent s'avérer prometteurs en tant qu'assistants pour les employés, en les aidant à rédiger et à résumer des courriels, des documents et d'autres contenus. Pour le personnel technique, ces outils peuvent être utiles pour rédiger, compléter ou vérifier le code. Bien que les recherches sur le sujet soient encore peu

nombreuses, les premiers éléments indiquent que ces outils permettent d'accroître modestement la productivité des salariés en entreprise (Brynjolfsson, Li et Raymond, 2023 ; Noy et Zhang, 2023).

Il convient de noter que de nombreux gouvernements et entreprises en sont encore aux premières étapes du pilotage de ces outils, et que davantage d'informations sont nécessaires avant de formuler des recommandations spécifiques sur la question de savoir si, comment et quand les employés devraient les utiliser. Les OGE qui envisagent d'utiliser ces outils devraient travailler avec d'autres agences gouvernementales et en partenariat étroit avec les fournisseurs pour mener des programmes pilotes contrôlés et surveillés afin de repérer où et quand ils pourraient être utiles (Carrasco *et al.*, 2024).

Comme dans d'autres cas d'utilisation de l'IA, l'utilisation de ces outils d'IA généralistes soulève des inquiétudes, principalement en matière de fiabilité et de sécurité. La principale préoccupation liée à l'utilisation de ces outils au sein des OGE est leur propension à produire des informations relevant d'hallucinations, ce qui peut poser un sérieux problème, en particulier lorsqu'ils sont utilisés pour rédiger des documents destinés au public (Rawte, Sheth et Das, 2023). Ce problème se pose également lorsque ces outils sont utilisés pour résumer des informations, telles que des documents juridiques, où les outils peuvent ne pas inclure des informations importantes, produire des informations relevant d'hallucinations ou déformer des informations contenues dans le document d'origine. En général, on ne peut

Encadré 2.2. Utilisation de chatbots d'IA généralistes au sein des OGE (suite)

pas faire entièrement confiance aux résultats de ces outils, ce qui complique leur utilisation à de nombreuses fins.

En outre, bien que nombre de ces outils disposent de versions d'entreprise dotées de protocoles de sécurité renforcés, les besoins et les responsabilités des gouvernements en matière de sécurité sont souvent beaucoup plus stricts, en particulier lorsqu'il s'agit d'informations sensibles. Selon l'outil utilisé, il existe un risque que les données de l'utilisateur soient incorporées dans les données de formation de l'outil, ce qui pourrait entraîner la fuite d'informations internes. Certains organismes publics ont interdit l'utilisation de ces outils en interne, invoquant des problèmes de sécurité (Solender et Fried, 2024).

Bien qu'il s'agisse de préoccupations sérieuses, les OGE peuvent être en mesure d'en atténuer certaines. Pour des raisons de sécurité, de nombreuses entreprises d'IAg sont en train de créer des versions gouvernementales de leurs outils conformes aux normes plus strictes requises pour une

utilisation dans le secteur public (Solender et Fried, 2024). Compte tenu de la nouveauté et de l'impact potentiel de cette technologie, les OGE devraient envisager de mener des tests plus approfondis que ceux habituellement effectués pour les outils logiciels dont ils font l'acquisition.

Les problèmes de fiabilité peuvent être plus difficiles à atténuer, en particulier dans les premières phases de développement de ces technologies. Ces outils doivent être envisagés pour des cas d'utilisation spécifiques ; par exemple, l'utilisation de l'IA pour résumer des documents d'orientation que les OGE utiliseront pour prendre des décisions est un cas d'utilisation beaucoup plus risqué que l'utilisation de ces outils pour rédiger de brefs courriels internes. Les OGE qui testent ces outils devraient insister sur leur manque de fiabilité auprès de leur personnel et former celui-ci de manière approfondie à l'importance de la vérification des faits, de la supervision humaine et de l'évaluation des risques liés à l'utilisation de ces outils.

Plus précisément, nous attirons l'attention sur les concepts de nécessité (c'est-à-dire l'importance d'un cas d'utilisation), de minimisation des données (c'est-à-dire la collecte de la quantité minimale de données nécessaires pour un cas d'utilisation) et de proportionnalité (c'est-à-dire s'assurer que les avantages liés à la restriction de la protection de la vie privée ne sont pas surpassés par les inconvénients liés au non-respect de la vie privée) du Règlement général de l'UE sur la protection des données (RGPD).

Il convient de noter que, dans de nombreux cas, le fait de se concentrer sur une supervision humaine approfondie des systèmes d'IA peut contribuer à atténuer bon nombre des préoccupations

mentionnées dans les sections précédentes et suivantes. Par exemple, le risque potentiel lié à l'utilisation de l'IA pour décider de l'affectation du personnel électoral est beaucoup plus élevé si ces recommandations sont mises en œuvre sans avoir été testées et vérifiées de manière approfondie par le personnel de l'OGE ayant une expertise en la matière. Étant donné que la plupart de ces cas d'utilisation potentiels n'ont pas été testés et n'ont pas fait l'objet de recherches suffisantes, une supervision humaine significative est particulièrement importante dans les phases pilotes, et une stratégie d'atténuation potentielle consiste à exécuter en parallèle des versions automatisées et des versions pilotées par l'homme de chaque cas d'utilisation, puis à en comparer les résultats.

2.5.1. Préoccupations générales et stratégies d'atténuation

Le cadre juridique

L'utilisation de l'IA pour les élections nécessitera une compréhension approfondie des cadres juridiques et réglementaires concernant la question de savoir si et quand les technologies numériques et la prise de décision automatisée peuvent être utilisées pour les processus électoraux. Les applications de l'IA dans le processus électoral peuvent nécessiter une mise à jour de la législation existante sur les élections, l'utilisation de la technologie par le gouvernement et les marchés publics. En outre, plusieurs pays sont en train d'adopter des réglementations sur l'IA qui peuvent imposer des exigences et des restrictions supplémentaires à l'utilisation de ces technologies dans l'administration des processus démocratiques et des élections, comme dans le cas de la législation européenne sur l'intelligence artificielle. Cette question est examinée plus en détail au chapitre 4.

Risques en matière de cybersécurité

Toute utilisation de l'IA pour les élections est susceptible d'introduire de nouveaux problèmes de cybersécurité, en plus des cybermenaces supplémentaires liées à l'IA et provenant d'autres acteurs (voir chapitre 3). Pour la mise en œuvre, les risques de cybersécurité sont doubles : premièrement, l'utilisation d'un plus grand nombre de technologies numériques augmente la surface d'attaque (points d'entrée) pour les cyberattaquants, leur donnant plus d'occasions de trouver des vulnérabilités au sein d'un système électoral. Le recours croissant aux technologies numériques dans le cadre du processus électoral offre aux attaquants de nouveaux moyens de porter atteinte à l'intégrité des élections. Deuxièmement, l'utilisation de l'IA dans le cadre du processus électoral oblige les OGE à collecter davantage de données, soit sur les électeurs, soit

sur l'élection, telles que les données biométriques des électeurs ou les images des caméras des bureaux de vote. Cela augmente à la fois le nombre de données précieuses pour les attaquants et les inconvénients d'une cyberattaque réussie. L'utilisation de l'IA par des acteurs malveillants peut accroître la sophistication des cyberattaques. Dans la pratique, les problèmes de cybersécurité peuvent nuire directement et indirectement à l'intégrité des élections. Directement, des cyberattaques réussies peuvent empêcher les gens de voter, modifier les résultats, perturber les bases de données d'inscription des électeurs et corrompre les données. Indirectement, des cyberattaques infructueuses, ou même la simple menace de cyberattaques, pourraient éroder la confiance dans le système électoral, dissuadant certains sous-groupes de la population de participer aux élections.

Dans de nombreux cas, ces problèmes peuvent être résolus. Pour atténuer les risques en matière de cybersécurité associés à l'utilisation de l'IA, les OGE devraient envisager de réaliser, en partenariat avec des agences et des experts en cybersécurité, des audits de cybersécurité des systèmes électoraux afin de protéger ces nouveaux points d'entrée. Le respect du principe de minimisation des données peut également réduire le risque global de cybersécurité, les OGE devant donner la priorité à la collecte du minimum de données privées nécessaire à l'exécution de fonctions spécifiques de l'IA.

Dépendance excessive à l'égard des entreprises privées

En raison de la difficulté de la mise en œuvre technique de bon nombre de ces cas d'utilisation, la dépendance croissante des OGE à l'égard des entreprises privées est une autre source d'inquiétude. L'utilisation de l'IA nécessite au minimum une infrastructure technique, telle que des GPU (unités de traitement graphique), qui sont produites par un nombre limité d'entreprises, qui en assurent aussi la maintenance. Dans de nombreux cas, les OGE auront probablement besoin d'autres infrastructures informatiques (par exemple, l'informatique en nuage), de talents techniques provenant d'entreprises privées et d'une assistance en matière de pratiques de cybersécurité. Le respect de ces exigences pourrait conférer à un groupe restreint d'entreprises un pouvoir accru dans l'administration des élections, ce qui soulève des inquiétudes quant à l'influence du secteur privé sur le gouvernement et la politique (Jungherr, 2023).

En outre, les outils d'IA sont susceptibles d'être développés par les fournisseurs traditionnels de technologies électorales. L'acquisition de ces technologies peut s'intégrer facilement dans les pratiques

existantes des OGE, mais il convient de noter qu'elles peuvent nécessiter beaucoup plus de tests et d'analyses de la part des OGE que d'habitude.

Pour commencer à atténuer certaines de ces préoccupations, les OGE devraient collaborer avec d'autres organismes publics pour déterminer si les cas d'utilisation de l'IA peuvent être développés en interne et lesquels pourraient nécessiter des partenariats privés. Les OGE devraient envisager d'entreprendre des audits plus approfondis des technologies développées par le secteur privé et fixer des normes spécifiques et élevées en matière d'efficacité et d'équité pour les fournisseurs. Il peut également être important de fixer des normes de transparence et de responsabilité pour les technologies développées par le secteur privé, en particulier au regard des politiques des États en matière d'accès à l'information sur les processus décisionnels du gouvernement.

Préjugés, discrimination, surveillance et droits humains

L'utilisation de l'IA et des techniques statistiques traditionnelles à des fins de discrimination à l'encontre de groupes spécifiques de personnes, notamment par le biais de l'incarcération de masse, du refus de prestations et de la discrimination électorale, ne date pas d'hier (Crawford, 2022). L'éthique de l'IA étant un sujet bien étudié, le présent rapport aborde brièvement les domaines que les OGE devraient examiner de manière plus approfondie. Toute utilisation de systèmes d'IA impliquant la collecte de grandes quantités de données, en particulier par les gouvernements, risque de perpétuer la surveillance et les violations des droits humains qui y sont associées. Par exemple, l'IA qui repose sur la collecte massive de messages publics sur les réseaux sociaux peut constituer une surveillance qui a pour effet de dissuader la liberté d'expression, même si ces données ne sont pas utilisées à mauvais escient (Commission interaméricaine des droits de l'homme, 2017). L'IA qui s'appuie sur des données biométriques pose des problèmes similaires, car elle peut dissuader des personnes de participer à des processus électoraux pour des raisons de protection de la vie privée ou de sécurité.

Ces risques se multiplient lorsqu'ils sont considérés sous l'angle de la discrimination, l'IA étant souvent utilisée pour perpétuer les préjugés existants dans la société. Par exemple, les modèles de reconnaissance faciale basés sur l'IA sont moins susceptibles d'identifier correctement les personnes de couleur, la plupart des LLM sont entraînés principalement sur des données en langue anglaise, et les algorithmes de police prédictive ont tendance à perpétuer

les préjudices existants dans les systèmes judiciaires (Perkowitz, 2021 ; Gstrein, Bunnik et Zwitter, 2019 ; Stokel-Walker, 2024). Étant donné que les modèles d'IA sont souvent entraînés sur des données produites par des humains ou basées sur le comportement humain, les biais existants sont souvent amplifiés dans leurs résultats.

Même sans intention malveillante, l'IA et la collecte massive de données par les OGE présentent de sérieux risques pour les droits humains, car l'acte de collecte de données peut entraîner l'utilisation de ces données pour empêcher ou décourager le vote ou pour divulguer l'identité des personnes, ainsi que le risque de fuites de données ou l'utilisation accidentelle de données à mauvais escient. L'utilisation de l'IA et la collecte de données peuvent généralement accroître le sentiment de surveillance, ce qui peut avoir un effet dissuasif ou inhibiteur. Il s'agit de l'effet négatif qu'une action de l'État (par exemple, la surveillance) a sur la population, ce qui dissuade des individus de manière préventive d'exercer leurs droits (par exemple, le vote) par crainte de conséquences formelles ou informelles (Pech, 2021). Si des acteurs malveillants ont accès aux données en question, les risques augmentent, car les données relatives au vote, à la parole, à la vidéo et à la biométrie (toutes les sources de données potentielles pour les organes de gestion des élections) peuvent toutes être utilisées pour causer un préjudice explicite aux électeurs.

Pour répondre à certaines de ces préoccupations, les OGE devraient accorder une attention particulière aux principes de nécessité, de proportionnalité et de minimisation des données mentionnés plus haut, en se concentrant sur une analyse approfondie des externalités négatives potentielles et des compromis des cas d'utilisation de l'IA. Comme nous l'indiquons au chapitre 4, de nombreuses approches de la réglementation de l'IA reposent sur un cadre fondé sur le risque, qui met l'accent sur l'établissement de lignes directrices strictes pour les situations à haut risque. Les OGE devraient collaborer avec d'autres agences et experts afin d'examiner dans quelle mesure l'utilisation de l'IA à haut risque pourrait avoir un impact sur les droits humains, comme la surveillance de masse et la dissuasion de la liberté d'expression, et ils devraient également se concentrer spécifiquement sur l'impact que les cas d'utilisation pourraient avoir sur les communautés marginalisées. Les OGE devraient envisager de procéder à des audits continus fondés sur l'éthique pour les cas d'utilisation de l'IA (Mökander et Floridi, 2021). Accorder une attention particulière aux biais existants dans les données de formation peut être un moyen utile d'éviter de perpétuer les préjudices antérieurs.

Confiance du public dans les élections

Enfin, il existe un risque de baisse de la confiance du public dans les élections. Les utilisations visibles de l'IA dans le système électoral peuvent rendre les électeurs sceptiques quant à l'impartialité et à la sécurité des élections (Padmanabhan, Simoes et MacCarthaigh, 2023). En ce qui concerne les utilisations moins visibles de l'IA, telles que la gestion des listes électorales, les électeurs peuvent être informés de ces pratiques par des sources non officielles, ce qui risque d'entamer encore plus la confiance. Le rôle des entreprises privées dans le processus électoral peut encore compliquer le gain de la confiance. Ces préoccupations peuvent être réparties inégalement au sein de la population, en particulier dans les pays ayant des antécédents de discrimination à l'encontre de certains groupes de personnes. L'utilisation de modèles d'apprentissage profond souvent ininterprétables peut exacerber ce problème, en particulier compte tenu de leurs implications pour la transparence du gouvernement. Si les modèles sont utilisés pour prendre des décisions sur des questions telles que l'emplacement des bureaux de vote ou la capacité à voter des électeurs, le public ou les réglementations (par exemple, le RGPD) peuvent exiger un niveau de transparence (par exemple, comment et pourquoi la décision a été prise) que les modèles peuvent ne pas être en mesure de fournir.

Pour atténuer certaines de ces préoccupations, les OGE devraient envisager des normes élevées de transparence pour l'utilisation de l'IA, y compris des explications détaillées sur les cas d'utilisation et le rôle joué par l'IA dans les processus décisionnels (Padmanabhan, Simoes et MacCarthaigh, 2023). Comme indiqué précédemment, une supervision humaine approfondie et des procédures d'appel peuvent contribuer à atténuer les préoccupations relatives à la confiance du public. Le fait de se concentrer sur des modèles d'IA facilement interprétables, plutôt que sur des approches basées sur l'apprentissage profond, peut également permettre aux OGE d'offrir des explications plus complètes au public sur la manière dont les décisions impliquant l'IA ont été prises et sur les raisons qui les ont motivées.

2.6. VOIES À SUIVRE

Bien que l'objectif de ce rapport ne soit pas de suggérer des pistes ou des cas d'utilisation spécifiques à mettre en œuvre par les OGE, nous présentons ci-dessous une série de recommandations à l'intention

des OGE désireux d'explorer l'utilisation de l'IA pour la gestion des élections.

1. Les OGE devraient appliquer les principes de nécessité, de minimisation des données et de proportionnalité lorsqu'ils envisagent de mettre en œuvre l'IA pour la gestion des élections, en concentrant leurs efforts sur les cas d'utilisation qui offrent le plus d'avantages tout en minimisant les externalités négatives.
2. Les OGE devraient examiner les cas d'utilisation de l'IA dans le contexte des pratiques existantes, en se concentrant sur les domaines où l'IA peut améliorer les résultats existants, et procéder à des comparaisons approfondies des coûts et des possibilités de mise en œuvre de l'IA.
3. Dans la mesure du possible, les OGE devraient mettre en place un contrôle humain des systèmes d'IA et se concentrer sur les moyens d'intégrer l'IA à d'autres stratégies, plutôt que de l'y substituer.
4. Les OGE devraient procéder à des audits approfondis et continus de la sécurité, des performances et de l'éthique des systèmes d'IA.
5. Les OGE devraient établir des normes strictes en matière de transparence, d'interprétabilité et de responsabilité pour les systèmes d'IA développés en interne et pour ceux fournis par des prestataires.
6. Les OGE devraient travailler en étroite collaboration avec d'autres agences, des groupes de défense des droits humains et des groupes d'intérêt communautaires lorsqu'ils envisagent la mise en œuvre et la conception de systèmes d'IA.
7. Les OGE doivent clairement indiquer tout contenu généré par les systèmes d'IA et y insérer un filigrane.
8. Les OGE qui envisagent d'utiliser l'IA devraient d'abord se concentrer sur le développement de leur infrastructure interne, de leur expertise technique et de leurs pratiques d'éthique et d'audit, même lorsqu'ils envisagent d'acheter des outils auprès de prestataires, afin de mesurer et de gérer de manière appropriée la mise en œuvre de l'IA et les préoccupations potentielles qu'elle suscite.

Chapitre 3

UTILISATION DE L'IA PAR D'AUTRES ACTEURS POLITIQUES ET IMPLICATIONS POUR LES OGE

À court terme, les principales implications des progrès de l'IA proviendront probablement de son utilisation par d'autres acteurs lors des élections.

L'objectif premier de ce rapport est de couvrir les cas d'utilisation potentiels de l'IA pour la gestion des élections. Toutefois, à court terme, les principales implications des progrès de l'IA pour les OGE proviendront probablement de son utilisation par d'autres acteurs pendant les élections. Dans ce chapitre, nous examinons quelques-unes des façons dont les acteurs externes, tels que les chargés de campagnes politiques, les producteurs de fausses informations et les pirates informatiques, peuvent utiliser l'IA pour influencer les élections et les activités des OGE. Nous présentons des stratégies d'atténuation potentielles pour les OGE et les autres acteurs concernés.

3.1. IAG ET MÉSINFORMATION

Le sujet le plus discuté à l'intersection de l'IA et des élections est sans doute le rôle que l'IA générative peut jouer dans la création et la diffusion de fausses informations politiques. Comme il s'agit d'un vaste sujet, nous nous concentrons dans ce rapport exclusivement sur les fausses informations pertinentes pour la gestion des élections, plutôt que sur celles concernant les candidats ou les points de vue politiques. Il convient de noter que la mésinformation induite par l'IAG sur les candidats et les positions politiques existe déjà et est susceptible d'avoir un impact sur le travail des OGE, en particulier en ce qui concerne le maintien de l'intégrité électorale, la confiance du public et la prévention de la violence électorale (Hsu, Thompson et Myers, 2024). Dans ce rapport, nous nous concentrons principalement sur la mésinformation concernant les processus électoraux, tels que le calendrier et le lieu des élections, ainsi que la sécurité et l'impartialité des élections.

La mésinformation en tant que forme de « suppression » électorale existait bien avant les progrès de l'IA. Des recherches antérieures menées par l'Institut international pour la démocratie et l'assistance électorale (IDEA International) ont examiné l'environnement informationnel dans 53 pays et ont révélé que les types de mésinformation les plus courants étaient les attaques contre l'impartialité des OGE, les informations fausses ou trompeuses sur les méthodes et les conditions de vote, et d'autres tentatives de tromper les gens afin qu'ils n'aillent pas voter (Bicu, 2023). Les techniques de mésinformation hors ligne et en ligne sont utilisées depuis longtemps pour induire les gens en erreur – en particulier les communautés marginalisées – sur la logistique des élections et la capacité à voter (Vandewalker, 2020).

Pour cette section, la question principale est la suivante : En quoi l'IA exacerbe-t-elle ce problème ?

L'IA augmente la quantité et améliore la qualité de l'offre de formes traditionnelles de mésinformation, telles que les articles de fausses nouvelles et les messages trompeurs sur les plateformes de réseaux sociaux. Grâce aux plateformes d'IA et aux modèles open source (libres), les acteurs malveillants peuvent rapidement générer du contenu textuel, audio et vidéo avec des objectifs spécifiques ciblant des groupes de personnes spécifiques, souvent d'une qualité similaire ou supérieure à la mésinformation traditionnelle rédigée par des humains et avec une probabilité plus faible de détection automatisée (Zhou *et al.*, 2023). S'il est peu probable que l'utilisation de ces plateformes et modèles exacerbe les problèmes de mésinformation dans les domaines où l'offre n'était pas déjà préoccupante (par exemple, les messages destinés à de larges audiences sur les plateformes de réseaux sociaux), cette amélioration des capacités peut poser un problème pour des domaines précédemment négligés, tels que les groupes de réseaux sociaux de petites communautés, que les auteurs d'attaques ont pu ignorer par le passé en raison de contraintes de temps et de ressources. Il est probable que la principale menace de la mésinformation basée sur l'IA se situe au niveau de la communauté, où les OGE sont moins susceptibles de prendre conscience de sa diffusion et où la désinformation par des acteurs malveillants peut être hyperciblée sur des groupes ou des individus spécifiques. Les fausses informations peuvent être diffusées sur diverses plateformes, notamment les principaux réseaux sociaux, les listes de diffusion, les moteurs de recherche et les services de messagerie privée. Pour ces derniers, il sera difficile de détecter la

Grâce aux plateformes d'IA et aux modèles open source, les acteurs malveillants peuvent rapidement générer du contenu textuel, audio et vidéo avec des objectifs spécifiques visant des groupes de personnes spécifiques.

mésinformation, car les plateformes de messagerie cryptées ne sont pas en mesure de modérer le contenu des messages.

L'IA offre de nouvelles possibilités de désinformation, notamment la production de faux contenus audio et vidéo de grande qualité. Les risques liés à ces formes de désinformation peuvent être spécifiques à chaque pays. Au Canada et aux États-Unis, par exemple, nous pensons qu'une menace majeure de la désinformation par l'IA est le développement de deepfakes audio qui imitent les candidats politiques, les responsables électoraux et les dirigeants des communautés locales, et utiliser ces imitations pour appeler les électeurs et les tromper sur les processus électoraux (Bond, 2024). Il existe déjà des preuves que cela s'est produit lors des élections américaines (Hsu, 2024). Cette menace est plus prononcée lorsqu'elle est exécutée dans de petites communautés ciblées, où les responsables sont moins susceptibles d'apprendre l'existence d'une désinformation avant qu'elle ne se soit propagée.

Les vidéos *deepfake* ou hypertruquées sont susceptibles d'être utilisées à des fins similaires et peuvent constituer une menace importante dans d'autres pays. Bien qu'elles ne soient pas encore en mesure d'imiter parfaitement le réalisme d'une vidéo réelle, elles restent une préoccupation sérieuse au sein des communautés ayant un faible niveau de culture numérique. Juste avant les dernières élections générales au Pakistan, de nombreuses vidéos *deepfake* ont été diffusées sur des plateformes à travers le pays, y compris de fausses vidéos de politiciens déclarant qu'ils boycotteraient le vote, ce qui pourrait avoir un impact sur l'intégrité électorale (Mughal, 2024). Bien que nous ne disposions pas actuellement de preuves de l'efficacité des fichiers vidéo ou audio *deepfake* sur l'intégrité électorale dans un contexte mondial, les OGE doivent se préparer à une augmentation de la quantité et à une amélioration de la qualité de ce type de désinformation.

En outre, une mésinformation de meilleure qualité risque de ternir encore davantage la confiance dans les informations en ligne. Cela pourrait inciter les candidats et les autres parties concernées à recourir au « dividende du menteur » et à prétendre que des enregistrements ou des images légitimes sont générés par l'IA. Il en résultera probablement une baisse générale de la confiance dans l'information, ce qui rendra plus difficile la diffusion d'informations exactes pour les OGE. En outre, il est prouvé que le fait d'inquiéter excessivement les gens au sujet de la propagation de la désinformation a peu de chances de les rendre moins sensibles

à cette dernière, tout en augmentant potentiellement leur volonté de soutenir les restrictions à la liberté d'expression (Jungherr et Rauchfleisch, 2024).

Il convient de noter qu'en raison de l'adoption par le grand public des chatbots d'IA, il est concevable que les électeurs puissent poser à des chatbots tels que ChatGPT et Gemini des questions sur les élections, telles que la date à laquelle elles auront lieu, l'endroit où l'on peut voter, et si elles sont sûres et sécurisées. Comme dans le cas des électeurs utilisant des moteurs de recherche à cette fin, cette utilisation des chatbots soulève des inquiétudes quant à l'exactitude des informations. Étant donné que les chatbots LLM n'ont pas tous accès à Internet et qu'ils sont souvent entraînés sur la base d'informations obsolètes, ajouté à leur tendance à l'hallucination, il n'est pas exclu que ces chatbots puissent fournir des informations incorrectes sur la capacité à voter des électeurs et la logistique des élections. Dans certains cas, les plateformes d'IAg ont annoncé des projets de partenariat avec des sources d'informations électorales faisant autorité vers lesquelles elles peuvent diriger les utilisateurs ayant des questions, mais l'efficacité et l'envergure de ces projets, en particulier en dehors des États-Unis, sont encore inconnues (OpenAI, 2024).

3.2. ORGANISATIONS POLITIQUES

Depuis un certain temps, les chargés de campagnes politiques dans divers pays utilisent la science des données et les techniques d'apprentissage automatique dans le cadre de leurs stratégies, plusieurs exemples récents marquants étant l'utilisation de la science des données pour l'organisation de la campagne présidentielle américaine de Barack Obama en 2012 et la collecte de fonds à cette fin, le scandale Cambridge Analytica de 2016 au Royaume-Uni et aux États-Unis, et leur utilisation croissante dans les élections en Inde (Dommett, 2019 ; Varna, 2019).

Les organisations politiques sont susceptibles d'utiliser l'IA pour diverses tâches, dont certaines peuvent être importantes pour les OGE. Il est prouvé que le microciblage hautement personnalisé pour la publicité politique peut être plus efficace que la publicité générique sur les plateformes de réseaux sociaux (Simchon, Edwards et Lewandowsky, 2024). Les chargés de campagnes et autres organisations politiques peuvent utiliser l'IA pour élaborer des

Depuis un certain temps, les chargés de campagnes politiques de différents pays utilisent la science des données et les techniques d'apprentissage automatique dans le cadre de leurs stratégies.

publicités spécifiques ciblant des individus ou de petits groupes de la population afin d'influencer leur comportement électoral. Dans les pays où les OGE sont chargés de contrôler les communications des chargés de campagnes, la charge de travail des OGE pourrait s'en trouver considérablement alourdie, lorsque des campagnes utilisent l'IA pour générer plusieurs versions d'une même publicité. Les OGE pourraient être amenés à repenser leurs procédures en matière de rapports et de contrôle des campagnes publicitaires. Étant donné que les modèles d'IA peuvent halluciner ou produire de fausses informations, les risques liés à ces publicités peuvent augmenter, en particulier lorsque les organisations utilisent des systèmes entièrement automatisés. Les organisations politiques peuvent sciemment utiliser l'IA pour développer et diffuser de fausses informations. La résolution de ces problèmes peut nécessiter davantage de réglementation et de supervision de la part de l'OGE et, dans certains cas, des partenariats avec d'autres agences gouvernementales ou l'adaptation des mandats de l'OGE.

D'autres formes de stratégies d'IA orientées vers le public utilisées par les chargés de campagnes peuvent également être pertinentes pour les OGE. Des candidats politiques du monde entier ont déjà utilisé l'IA pour créer des *deepfakes* d'eux-mêmes prononçant des discours ou s'exprimant dans des langues étrangères (Calma, 2023 ; Zhuang, 2024). Pour les OGE chargés de suivre les communications de campagne, ce type d'utilisation de l'IA peut soulever des questions complexes sur les définitions de la désinformation ou de la communication trompeuse. Dans plusieurs pays, dont l'Indonésie et le Pakistan, les chargés de campagnes ont commencé à créer des chatbots perfectionnés qui imitent les candidats ou fournissent des informations avec lesquelles les électeurs peuvent interagir (Parkin et Bokhari, 2024 ; Rayda, 2024). Ces chatbots présentent des problèmes similaires à ceux posés par les chatbots généralistes, dans la mesure où les réponses aux questions des utilisateurs liées aux élections peuvent être inexactes.

Les organisations politiques sont susceptibles d'utiliser l'IA pour toute une série d'autres tâches liées à la campagne, telles que la rédaction de discours/contenus, l'allocation de ressources, l'organisation de stratégies, l'analyse interne et le financement participatif de positions politiques. Dans certains cas, ces utilisations de l'IA peuvent avoir un impact sur le travail des OGE. Par exemple, les chargés de campagnes peuvent utiliser l'IA pour développer de meilleures capacités d'analyse de données, les aidant à décider où concentrer leurs efforts lorsqu'ils font de la publicité, du porte-à-porte

ou organisent des événements. Pour les OGE chargés de protéger les droits des électeurs en matière de confidentialité des données, l'utilisation de l'IA, qui nécessite généralement des ensembles de données plus importants que les méthodes statistiques traditionnelles, peut susciter des inquiétudes. En outre, si ces méthodes s'avèrent efficaces, elles peuvent avoir un impact sur les taux de participation, obligeant les OGE à reconsidérer l'affectation des ressources dans les bureaux de vote ou dans différentes zones géographiques.

3.3. MENACES POUR LA SÉCURITÉ DES SYSTÈMES ÉLECTORAUX

Les systèmes électoraux et les OGE sont depuis longtemps la cible de cyberattaques (Van der Staak et Wolf, 2019). Bien que de nombreuses menaces de cybersécurité pèsent sur les OGE et d'autres organismes responsables des élections, nous nous concentrons exclusivement, dans le présent rapport, sur le domaine où les progrès de l'IA peuvent exacerber le problème à court terme, à savoir les tentatives d'hameçonnage (ou *phishing*) de meilleure qualité. Bien que les progrès de l'IA soient susceptibles d'améliorer la qualité des logiciels malveillants et des techniques de développement de codes d'exploitation, le principal risque à court terme de l'IA pour la cybersécurité liée aux OGE est une amélioration de la qualité de l'hameçonnage (National Cyber Security Centre, 2024).

Les pirates qui ciblent les élections ont souvent recours à l'ingénierie sociale (c'est-à-dire à des tactiques visant à manipuler, influencer ou tromper les victimes) pour accéder à des systèmes privés, généralement par le biais d'attaques d'hameçonnage. L'hameçonnage consiste à faire croire aux destinataires que les communications proviennent de sources fiables et à tirer parti de cette tromperie pour amener les victimes à communiquer des informations sensibles ou à télécharger des fichiers nuisibles. Dans le passé, les tentatives d'hameçonnage à grande échelle étaient généralement de mauvaise qualité, étant donné le temps nécessaire pour créer des communications frauduleuses de grande qualité ciblant des individus spécifiques (cet hameçonnage ciblé étant appelé harponnage ou *spear phishing*). Comme dans le cas de la désinformation, l'IA générative rend le processus de recherche de victimes potentielles et de génération d'un contenu de haute qualité nettement plus efficace,

Les systèmes électoraux et les OGE sont depuis longtemps la cible de cyberattaques.

ce qui augmente potentiellement les chances de réussite (Norden et Ramachandran, 2023). En affinant les modèles de langage à l'aide de communications officielles antérieures ou en leur fournissant des informations sur la structure des bureaux électoraux, il est possible de générer des résultats très convaincants et d'apparence légitime (Gupta *et al.*, 2023).

L'IA est susceptible d'exacerber l'hameçonnage textuel, qui est le plus courant, et de renforcer les nouvelles formes d'hameçonnage, telles que les imitations vocales et les appels téléphoniques de hauts fonctionnaires (Cybersecurity and Infrastructure Security Agency, 2024). Les tentatives d'hameçonnage réussies peuvent amener les responsables électoraux à divulguer des données confidentielles ou à donner aux auteurs de l'attaque l'accès à des systèmes clés, tels que les sites web des OGE, les ensembles de données sur les électeurs, les bases de données d'inscription ou même les résultats des élections.

En outre, les OGE qui fournissent des plateformes sur lesquelles les électeurs peuvent déposer des plaintes ou des demandes d'information auprès des fonctionnaires peuvent être vulnérables à l'inondation d'informations par l'IA. Par exemple, les organes de gestion des élections qui gèrent un système permettant aux électeurs de soumettre des problèmes dans les bureaux de vote peuvent recevoir des déclarations réalistes, mais fausses, générées par l'IA. Un tel afflux de questions pourrait submerger les systèmes techniques conçus pour traiter un petit nombre de plaintes, évincer les problèmes réels dans les lieux de vote ou amener les OGE à prendre des décisions sur la base d'informations erronées.

3.4. VOIES À SUIVRE

Nous présentons ci-dessous une série de recommandations à l'intention des OGE et des autres parties concernées afin de répondre à certaines des préoccupations évoquées dans la présente section. Il convient de noter que, dans presque tous les cas, les progrès de l'IA ne font qu'exacerber les sujets de préoccupation existants pour les OGE, et que les meilleures méthodes d'atténuation consistent à renforcer les pratiques de sécurité existantes.

1. Les OGE doivent travailler en étroite collaboration avec les responsables locaux et les groupes d'intérêt communautaires afin d'identifier la diffusion de fausses informations autour des élections. Les OGE doivent mettre en place des méthodes pour signaler la mésinformation électorale à l'OGE et à d'autres agences gouvernementales.
2. Les OGE devraient avoir une présence vérifiée sur les principales plateformes afin de lutter contre la diffusion de fausses informations et devraient réagir rapidement aux cas de fausses informations. Les OGE devraient amplifier les contenus exacts et informatifs autour des élections.
3. Si cela fait partie de leur mandat, les OGE devraient s'engager de manière proactive sur les principales plateformes de réseaux sociaux et d'IAg afin de mettre à disposition les ressources nécessaires pour prévenir et démythifier les informations électorales erronées. Ils devraient également s'efforcer de rendre les informations électorales disponibles dans des formats lisibles par machine afin que les plateformes puissent facilement intégrer des informations correctes et précises dans les contenus destinés aux utilisateurs.
4. Les OGE devraient coopérer avec d'autres agences gouvernementales, telles que les instances de régulation des communications et les agences de cybersécurité, afin d'empêcher la prolifération de fausses informations et de demander des comptes aux parties responsables, notamment en empêchant l'usurpation d'appel ou de numéro, ainsi qu'en réglementant les appels automatisés et l'utilisation de *deepfakes* d'IA sur les réseaux de communication.
5. Les OGE devraient renforcer les pratiques existantes en matière de cybersécurité en utilisant des outils anti-hameçonnage, en formant le personnel, en recourant à l'authentification multifactorielle et à d'autres formes de collaboration avec des agences et des experts en cybersécurité. Les OGE devraient imposer des mesures similaires aux fournisseurs de technologies électorales.
6. Les OGE devraient collaborer avec les plateformes d'IAg et leur demander des comptes afin d'empêcher l'utilisation de leurs outils pour la diffusion de fausses informations liées aux élections. Ces mesures peuvent aller de la réglementation de

l'utilisation et du développement des outils d'IAg à la fourniture aux plateformes d'informations précises sur la logistique des élections. Les OGE devraient exiger des plateformes d'IAg des lignes directrices transparentes sur la manière dont leurs outils peuvent être utilisés pour des événements politiques et sur la manière dont ces règles seront appliquées.

7. Les OGE devraient demander des comptes aux plateformes de réseaux sociaux et s'assurer que les décisions de modération appropriées sont prises conformément aux normes et lois tant nationales qu'internationales.
8. Les OGE doivent informer les organisations politiques des menaces potentielles en matière d'information et tenir les partis responsables de leur utilisation de l'IA. Parmi les actions possibles, on peut citer l'obligation de rendre transparente l'utilisation de l'IA à des fins politiques et l'interdiction faite aux organisations politiques de diffuser de la désinformation sur la logistique liée aux élections.
9. Les OGE devraient prendre en compte l'impact de l'IA dans toutes ces stratégies d'atténuation, en mettant l'accent sur les communautés marginalisées, qui sont particulièrement visées par les campagnes de désinformation et les plus vulnérables à la perpétuation des préjugés par les modèles d'IA.

Chapitre 4

CADRES RÉGLEMENTAIRES DE L'IA ET IMPLICATIONS POUR LES ÉLECTIONS

Le paysage juridique de l'utilisation de l'IA est encore en développement, avec diverses approches envisagées et mises en œuvre dans différents pays. Dans ce chapitre, nous présentons brièvement certains cadres réglementaires applicables à l'IA et la mesure dans laquelle ils pourraient avoir un impact sur le travail des autorités électorales.

Le paysage juridique de l'utilisation de l'IA est encore en développement, avec diverses approches envisagées et mises en œuvre dans différents pays.

4.1. LÉGISLATION EUROPÉENNE SUR L'IA

Le règlement européen sur l'IA² vise à réglementer le développement et l'utilisation des systèmes d'IA dans les États Membres de l'UE. Ce texte a été approuvé par le Parlement européen en mars 2024, ses dispositions entrant en vigueur de manière échelonnée à partir de 2024 (Chee, 2024).

La plupart des recherches sur le règlement sur l'IA se concentrent sur les implications de la réglementation pour les entreprises privées, mais l'utilisation de l'IA par les gouvernements de l'UE est également couverte par ses règles. Dans cette section, nous nous concentrons sur les implications réglementaires potentielles du règlement européen sur la mise en œuvre de systèmes d'IA par les OGE et d'autres autorités électorales.

² Au moment de la rédaction de ce rapport, le règlement 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle n'est pas encore entré en vigueur. Le présent rapport doit être considéré comme un premier aperçu des implications potentielles de ce texte sur l'utilisation de l'IA au sein des OGE dans les États Membres de l'UE.

Le règlement européen adopte une approche fondée sur les risques pour réglementer les systèmes d'IA, en classant les cas d'utilisation selon quatre niveaux de risque : inacceptable, élevé, limité et minimal.

De nombreux cas d'utilisation de l'IA pour la gestion des élections sont susceptibles d'entrer dans la catégorie à haut risque.

De nombreux cas d'utilisation de l'IA pour la gestion des élections sont susceptibles de relever de la catégorie à haut risque, qui couvre les systèmes utilisés pour « l'administration de la justice et les processus démocratiques », y compris « les systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur droit de vote lors d'une élection ou d'un référendum. Cela n'inclut pas les systèmes d'IA dont les résultats ne sont pas directement exposés aux personnes physiques, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques d'un point de vue administratif et logistique » (Parlement européen et Conseil de l'Union européenne 2024, 40, 40a).

Il convient de noter que le règlement sur l'IA interdit (à quelques exceptions près, notamment à des fins de sécurité nationale) l'utilisation de systèmes d'IA présentant un risque inacceptable. Pour les OGE qui utilisent et réglementent l'IA, cette interdiction couvre les pratiques suivantes :

- le recours à des techniques subliminales, manipulatrices ou trompeuses avec pour objectif ou effet d'altérer le comportement en portant atteinte à la capacité à prendre une décision éclairée, causant ainsi un préjudice important ;
- la constitution de bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'Internet ou de la vidéosurveillance ;
- l'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives (à quelques exceptions près).

Le règlement européen sur l'IA réglemente principalement les fournisseurs de systèmes à risque élevé, qui peuvent être des vendeurs de technologies électorales ou les OGE eux-mêmes. Il réglemente également ce que l'on appelle les « déployeurs », c'est-à-dire les OGE qui utilisent des systèmes d'IA développés en interne comme en externe. Pour les systèmes à risque élevé, certaines exigences pour les fournisseurs comprennent l'établissement de systèmes de gestion des risques, la conduite de la gouvernance des

données, la possibilité de contrôle humain et l'atteinte de niveaux appropriés de précision, de robustesse et de cybersécurité ; pour les déployeurs de systèmes à risque élevé, certaines exigences comprennent l'attribution d'une supervision humaine à des personnes qualifiées, la surveillance et l'exploitation du système conformément aux instructions d'utilisation et l'information des fournisseurs sur les problèmes (Parlement européen et Conseil de l'Union européenne, 2024).

Le cadre fondé sur les risques du règlement sur l'IA offre aux OGE un moyen utile d'envisager la mise en œuvre de l'IA dans les processus électoraux. Un bon point de départ consiste à examiner la gravité des risques liés à un cas d'utilisation de l'IA (par exemple, impact sur les résultats électoraux ou simple amélioration de l'efficacité d'un processus existant) et à prendre les mesures proposées en fonction du niveau de risque, y compris l'analyse de la nécessité et de la proportionnalité du cas d'utilisation. Pour les systèmes à haut risque, les exigences de la loi sur l'IA en matière de supervision humaine, d'audits de performance des modèles et de gouvernance des données sont des moyens essentiels d'atténuer certaines des préoccupations liées à la mise en œuvre de l'IA.

4.2. DÉCRET PRÉSIDENTIEL DES ÉTATS-UNIS SUR L'INTELLIGENCE ARTIFICIELLE

Un autre texte réglementaire potentiellement pertinent est le décret américain sur l'intelligence artificielle (décret sur l'IA) (États-Unis d'Amérique, 2023). Le décret sur l'IA couvre l'utilisation de l'IA par les autorités gouvernementales américaines et pourrait donc avoir un impact sur l'utilisation de l'IA pour la gestion des élections aux États-Unis. En particulier, le décret sur l'IA comprend des dispositions visant à :

- demander aux agences fédérales de développer et d'utiliser des outils permettant de vérifier l'authenticité des communications gouvernementales ;
- évaluer et renforcer la manière dont les agences fédérales achètent et utilisent les ensembles de données commerciales, et renforcer les orientations en matière de protection de la vie privée ;

- publier des orientations sur l'utilisation de l'IA par les agences fédérales, y compris sur la manière de protéger les droits et la sécurité ;
- s'attaquer aux violations des droits civils et des libertés civiles liées à l'utilisation de l'IA dans les secteurs privé et public.

Il convient de noter que le décret sur l'IA n'est pas une législation américaine ; il s'agit plutôt d'une directive de l'exécutif axée principalement sur l'allocation de ressources fédérales et la clarification de l'application des lois existantes dans le contexte de l'IA. Les États-Unis, comme beaucoup d'autres pays, discutent actuellement d'une législation complète sur l'IA, semblable au règlement européen sur l'IA, qui pourrait avoir un impact supplémentaire sur le travail des autorités électorales.

4.3. RÈGLEMENT DU TRIBUNAL ÉLECTORAL BRÉSILIEN

Les récents règlements électoraux adoptés par le Tribunal supérieur électoral du Brésil (Conceição, 2024) sont potentiellement pertinents. Il s'agit d'un rare exemple de réglementation de l'IA spécifiquement adaptée aux élections. Une grande partie de la réglementation couvre l'utilisation de l'IA pour les campagnes politiques, exigeant que :

- les gestionnaires de campagnes apposent un filigrane visible sur tout contenu de campagne électorale généré par l'IA ;
- les contenus fabriqués ou manipulés à des fins de désinformation soient totalement interdits ;
- la mésinformation susceptible de nuire à l'intégrité électorale soit totalement interdite ;
- les campagnes ne créent pas de *deepfakes* ou de chatbots pour imiter les interactions entre les candidats et le public.

Le règlement exige que les plateformes qui hébergent ou diffusent du contenu électoral adoptent des mesures pour empêcher la propagation de toute violation.

4.4. RÉGLEMENTATION DE L'IA DANS D'AUTRES PAYS

Plusieurs autres pays, dont l'Argentine, le Canada, le Chili, la Colombie, l'Inde, le Japon, la Nouvelle-Zélande, le Pérou, Singapour et bien d'autres encore, ont adopté des orientations relatives à l'IA ou sont en train d'élaborer des réglementations en la matière (IAPP, 2024). Nombre de ces réglementations adoptent des approches fondées sur les risques, en se concentrant sur les cas d'utilisation de l'IA les plus risqués dans les secteurs public et privé. Il est probable que, dans de nombreux pays, de nombreux cas d'utilisation de l'IA liés aux OGE, ainsi que de nombreux cas d'utilisation par des tiers qui affecteront les OGE, entreront dans des catégories à haut risque en raison de leur impact potentiel sur la démocratie.

Chapitre 5

CONCLUSION

Ce rapport fournit une vue d'ensemble des opportunités et des défis liés à l'IA pour les élections. Il illustre le potentiel des OGE à utiliser l'IA pour améliorer les processus électoraux tout au long du cycle électoral, notamment pour l'inscription des électeurs, la planification des élections, l'éducation civique, le suivi de la campagne et des médias, les opérations de vote, la surveillance des bureaux de vote, la compilation des votes et l'analyse des résultats. Les OGE qui envisagent une mise en œuvre rapide de l'IA peuvent également étudier l'utilisation d'outils d'IA généralistes à l'usage des employés, tels que l'application Copilot de Microsoft, pour les aider à rédiger ou à résumer des courriels et des contenus.

Bien que nombre de ces cas d'utilisation soient prometteurs, ils soulèvent tous des inquiétudes.

Bien que nombre de ces cas d'utilisation soient prometteurs, ils soulèvent tous des inquiétudes. Dans la pratique, les difficultés techniques liées à la mise en œuvre, au contrôle et à la maintenance de certains systèmes d'IA, ainsi que le manque de fiabilité de nombreux modèles, posent de sérieuses questions quant à la capacité des OGE à déployer et à gérer l'IA tout en préservant l'intégrité électorale. Les problèmes de fiabilité peuvent avoir des implications éthiques, l'utilisation de l'IA pouvant soulever des problèmes de partialité et de discrimination, en particulier pour les communautés traditionnellement marginalisées. L'utilisation de l'IA peut diminuer la confiance du public dans les élections, en particulier lorsqu'elle nécessite une surveillance accrue, ce qui peut avoir un effet dissuasif sur les droits humains.

Les OGE qui envisagent d'utiliser l'IA devraient se concentrer sur les principes de nécessité, de minimisation des données et de proportionnalité, en accordant une attention particulière aux coûts et aux avantages de l'utilisation de l'IA par rapport aux pratiques

existantes. La mise en œuvre de normes strictes en matière de transparence, de cybersécurité, de tests, d'audits et de supervision humaine peut contribuer à atténuer certaines des préoccupations liées à l'utilisation de l'IA, mais les OGE qui envisagent de la mettre en œuvre devraient commencer par s'intéresser en priorité aux cas d'utilisation présentant les risques potentiels les plus faibles. Dans presque tous les cas, les OGE devraient d'abord axer leurs efforts sur la mise en place de l'infrastructure, de l'expertise technique et des pratiques d'éthique et d'audit nécessaires pour utiliser l'IA en toute sécurité, avant de l'acquérir ou de la développer.

En ce qui concerne l'utilisation de l'IA par des acteurs autres que les OGE, il est essentiel que les OGE élaborent des plans pour répondre à l'impact que l'IA pourrait avoir sur la gestion des élections. Par exemple, il est probable que les OGE verront une augmentation de la quantité et de la qualité de la mésinformation liée aux élections. Bien que l'IA ne modifie pas radicalement le paysage de la mésinformation, elle pourrait affecter davantage la confiance dans les processus électoraux, et les OGE devraient prendre des mesures pour lutter contre la désinformation, en particulier la mésinformation ciblant les communautés marginalisées, notamment en travaillant avec les fonctionnaires locaux, les groupes communautaires, les entreprises d'IAg et les plateformes de réseaux sociaux.

Les chargés de campagnes et organisations politiques sont susceptibles d'utiliser l'IA pour influencer les élections en générant des contenus/publicités, des analyses de données et d'autres tâches liées à la campagne. Les OGE dont le mandat comprend la surveillance des organisations politiques devraient collaborer avec d'autres agences gouvernementales pour limiter la mésinformation provenant de chargés de campagnes, exiger l'apposition d'un filigrane sur les contenus générés par l'IA et prendre en compte les implications de l'utilisation de l'IA dans le cadre des campagnes en matière de protection de la vie privée.

Les OGE devraient être conscients de la menace accrue que représente l'IA pour la cybersécurité, tant lors de la mise en œuvre de l'IA que lors de son utilisation par des acteurs extérieurs. En particulier, les OGE doivent se préparer à des tentatives d'hameçonnage de meilleure qualité qui utilisent l'IAg pour manipuler les gens et les amener à partager des informations internes. Travailler en étroite collaboration avec des experts en cybersécurité, suivre les pratiques recommandées existantes en la matière et

former les employés à cette menace sont autant de mesures qui méritent d'être envisagées.

Les OGE devraient travailler en étroite collaboration avec leurs gouvernements pour comprendre les implications des différents cadres réglementaires et la manière dont ils peuvent influencer sur le travail des OGE. Par exemple, les OGE qui envisagent de mettre en œuvre l'IA au sein de l'UE peuvent voir leurs cas d'utilisation classés dans la catégorie « risque élevé », ce qui les oblige à respecter des normes plus strictes en matière de transparence, de responsabilité et de supervision humaine que pour d'autres technologies. Les OGE devront peut-être faire évoluer leurs propres mandats et structures réglementaires afin de préserver leur capacité à garantir l'intégrité des élections.

Enfin, l'IA et sa réglementation étant des domaines qui évoluent rapidement, les OGE doivent considérer le présent rapport comme un aperçu général et non exhaustif du rôle que l'IA pourrait jouer dans leurs élections. Les OGE doivent se tenir au courant du développement, des opportunités et des risques liés à l'IA, et collaborer étroitement avec des experts au sein et à l'extérieur du gouvernement afin d'actualiser en permanence leur compréhension du paysage. Avec ce rapport, nous espérons offrir un point de départ à ces discussions.

Références bibliographiques

- Akbar P., Jafar Loilatu M., Pribadi U. et Sudiar S., « Implementation of artificial intelligence by the General Elections Commission in creating a credible voter list » [Mise en œuvre de l'intelligence artificielle par la Commission des élections législatives pour établir un registre des électeurs crédible], *IOP Conference Series: Earth and Environment Science*, 717/1, 2021, <<https://doi.org/10.1088/1755-1315/717/1/012017>>
- Al-Haidary M., Ajlouni M. A., Talib M. A. Abbas S., Nasir Q. et Basaeed E., « Metaheuristic approaches to facility location problems: A systematic review » [Approche métaheuristique des problèmes d'implantation d'installations. Étude systématique], in *4th International Conference on Signal Processing and Information Security* [4^e conférence internationale sur le traitement des signaux et la sécurité de l'information], Institute of Electrical and Electronics Engineers, 2021, p. 49-52, <<https://doi.org/10.1109/ICSPIS53734.2021.9652430>>
- Ali M., Sapiezynski P., Bogen M., Korolova A., Mislove A. et Rieke A., « Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes » [Optimisation discriminatoire. Comment le ciblage publicitaire de Facebook peut aboutir à des résultats biaisés], ArXiv, 12 septembre 2019, <<https://doi.org/10.48550/arXiv.1904.02095>>
- Barretto S., Chown W., Meyer D., Soni A., Tata A. et Halderman J. A., « Improving the accuracy of ballot scanners using supervised learning » [Améliorer la précision des scanners de bulletins reposant sur l'apprentissage supervisé], in R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak et M. Germann (dir.), *Electronic Voting: 6th International Joint Conference, E-Vote-ID 2021, Virtual Event, October 5-8, 2021, Proceedings*, Springer International Publishing, 2021, p. 17-32, <https://doi.org/10.1007/978-3-030-86942-7_2>
- Bender S. M. L., « Algorithmic elections » [Élections algorithmiques], *Michigan Law Review*, 121/3, 2022, p. 489-524, <<https://doi.org/10.36644/mlr.121.3.algorithmic>>
- Bicu I., « The information environment around elections [L'environnement informationnel autour des élections], IDEA International, 2023, <<https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections>>, consulté le 15 avril 2024
- Bond S., « AI fakes raise election risks as lawmakers and tech companies scramble to catch up » [L'hypertrucage augmente les risques électoraux tandis les législateurs et les entreprises technologiques peinent à suivre], National Public Radio (NPR), 8 février 2024, <<https://www.npr.org/2024/02/08/1229641751/ai-deepfakes-election-risks-lawmakers-tech-companies-artificial-intelligence>>, consulté le 15 avril 2024
- Brynjolfsson E., Li D. et Raymond L. R., « Generative AI at Work' [L'IA générative au travail], National Bureau of Economic Research, Working Paper 31161, novembre 2023, <<https://doi.org/10.3386/w31161>>

- Calma J., « NYC Mayor Eric Adams uses AI to make robocalls in languages he doesn't speak » [Le maire de New York Eric Adams recourt à l'IA pour passer des appels téléphoniques automatisés dans des langues qu'il ne parle pas], *The Verge*, 17 octobre 2023, <<https://www.theverge.com/2023/10/17/23920733/nyc-mayor-eric-adams-ai-robocalls-spanish-mandarin>>, consulté le 15 avril 2024
- Carrasco M., Habib C., Felden F., Sargeant R., Mills S., Shenton S., Ingram J. et Dando G., « Generative AI for the public sector: The journey to scale » [L'IA générative pour le secteur public. Vers l'amplification], Boston Consulting Group, 26 mars 2024, <<https://www.bcg.com/publications/2024/gen-ai-journey-to-scale-in-government>>, consulté le 15 avril 2024
- Chee F. Y., « Europe one step away from landmark AI rules after lawmakers' vote » [L'Europe avance d'un pas par rapport aux grandes règles en matière d'IA après le vote des législateurs], Reuters, 14 mars 2024, <<https://www.reuters.com/technology/eu-lawmakers-endorse-political-deal-artificial-intelligence-rules-2024-03-13/>>, consulté le 15 avril 2024
- Clark A., « The cost of democracy: The determinants of spending on the public administration of elections » [Le coût de la démocratie. Les déterminants des dépenses de gestion publique des élections], *International Political Science Review*, 40/3, 2019, p. 354-369, <<https://doi.org/10.1177/0192512118824787>>
- Commission interaméricaine des droits de l'homme (CIDH), « Standards for a Free, Open and Inclusive Internet » [Normes pour un Internet libre, ouvert et inclusif], OEA/Ser.L/V/II., Organisation des États américains (OEA), 15 mars 2017, <https://www.oas.org/en/iachr/expression/docs/publications/internet_2016_eng.pdf>, consulté le 15 avril 2024
- Conceição L. H. M., « Brazilian judges regulate elections ... and AI » [Des juges brésiliens réglementent les élections ... et l'IA], *Verfassungsblog*, 15 mars 2024, <<https://doi.org/10.59704/612f31a89ce38fc6>>
- Crawford K., *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* [Atlas de l'IA. Pouvoir, politique et coûts de l'intelligence artificielle à l'échelle de la planète], New Haven (CT), Yale University Press, 2022, <<https://doi.org/10.12987/9780300252392>>
- Cybersecurity and Infrastructure Security Agency, « Risk in focus: Generative A.I. and the 2024 election cycle » [Le risque en ligne de mire. L'IA générative et les élections de 2024], 18 janvier 2024, <https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf>, consulté le 15 avril 2024
- Dhiman P., Kaur A., Iwendi C. et Mohan S. K., « A scientometric analysis of deep learning approaches for detecting fake news » [Analyse scientométrique des approches d'apprentissage profond pour détecter les fausses informations], *Electronics*, 12/4, 2023, p. 948, <<https://doi.org/10.3390/electronics12040948>>.
- Dommett K., « Data-driven political campaigns in practice: Understanding and regulating diverse data-driven campaigns » [Les campagnes politiques orientées données dans la pratique. Comprendre et réglementer diverses campagnes orientées données], *Internet Policy Review*, 8/4, 2019, <<https://doi.org/10.14763/2019.4.1432>>
- Eisen N., Lee N. T., Galliher C. et Katz J., « AI can strengthen U.S. democracy-and weaken it » [L'IA peut aussi bien renforcer la démocratie américaine que l'affaiblir], Brookings, 21 novembre 2023, <<https://www.brookings.edu/articles/ai-can-strengthen-u-s-democracy-and-weaken-it/>>, consulté le 15 avril 2024

- Electronic Registration Information Center, Technology and Security Brief 6.1, 8 mars 2024, <<https://ericstates.org/wp-content/uploads/documents/ERIC-Tech-Security-Brief.pdf>>, consulté le 15 avril 2024
- États-Unis, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence [Décret présidentiel sur le développement et l'utilisation sûre, sécuritaire et digne de confiance de l'intelligence artificielle], La Maison-Blanche, 20 octobre 2023, <<https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>>, consulté le 15 avril 2024
- Goel S., Meredith M., Morse M., Rothschild D. et Shirani-Mehr H., « One person, one vote: Estimating the prevalence of double voting in U.S. presidential elections » [Une personne, une voix. Estimer la prévalence des doubles votes aux élections présidentielles américaines], *American Political Science Review*, 114/2, 2020, p. 456-469, <<https://doi.org/10.1017/S000305541900087X>>
- Green J., « Anomaly detection in election data and its representation of U.S. infrastructure vulnerability » [La détection des anomalies dans les données relatives aux élections et leur représentativité de la vulnérabilité de l'infrastructure américaine], in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference*, Institute of Electrical and Electronics Engineers, 2021, p. 503-508, <<https://doi.org/10.1109/IEMCON53756.2021.9623111>>
- Gstrein O. J., Bunnik A. et Zwitter A., « Ethical, legal and social challenges of predictive policing » [Les défis éthiques, juridiques et sociaux de la prévision policière], *Católica Law Review, Direito Penal*, 3/3, 2019, p. 77-98, <<https://papers.ssrn.com/abstract=3447158>>, consulté le 15 avril 2024
- Gupta M., Akiri C., Aryal K., Parker E. et Praharaj L., « From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy » [De ChatGPT à ThreatGPT. L'impact de l'IA générative sur la cybersécurité et la protection de la vie privée], *IEEE Access*, 11, 2023, p. 80218-80245, <<https://doi.org/10.1109/ACCESS.2023.3300381>>
- Haenschen K., « The conditional effects of microtargeted Facebook advertisements on voter turnout » [Les effets de conditionnement des publicités Facebook microciblées sur la participation électorale], *Political Behavior*, 45/1, 2022, p. 1661-1681, <<https://doi.org/10.1007/s11109-022-09781-7>>
- Hajnal Z., Kuk J. et Lajevardi N., « We all agree: Strict voter ID laws disproportionately burden minorities » [Cela fait l'unanimité. Des législations strictes en matière d'identification des électeurs affectent les minorités de manière disproportionnée], *The Journal of Politics*, 80/3, 2018, p. 1052-1059, <<https://doi.org/10.1086/696617>>
- Hardyns W. et Rummens A., « Predictive policing as a new tool for law enforcement? Recent developments and challenges » [La prévision policière un nouvel outil pour l'application des lois ? Développements et défis récents], *European Journal on Criminal Policy and Research*, 24/3, 2018, p. 201-218, <<https://doi.org/10.1007/s10610-017-9361-2>>

- Haut-Commissariat des Nations Unies pour les réfugiés (HCR), Factsheet 4 : Types of Misinformation and Disinformation [Fiche d'information n° 4. Les types de mésinformation et de désinformation], février 2022, <<https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf>>, consulté le 22 avril 2024
- Hsu T., « New Hampshire officials to investigate A.I. robocalls mimicking Biden » [Des agents de l'État du New Hampshire vont enquêter sur les appels automatisés imitant la voix de Biden], *The New York Times*, 22 janvier 2024, <<https://www.nytimes.com/2024/01/22/business/media/biden-robocall-ai-new-hampshire.html>>, consulté le 15 avril 2024
- Hsu T., Thompson S. A. et Myers S. L., « Elections and disinformation are colliding like never before in 2024 » [Élections et désinformation se télescopent plus que jamais], *The New York Times*, 9 janvier 2024, <<https://www.nytimes.com/2024/01/09/business/media/election-disinformation-2024.html>>, consulté le 15 avril 2024
- Hussain R., Raza A., Siddiqi I., Khurshid K. et Djeddi C., « A comprehensive survey of handwritten document benchmarks: Structure, usage and evaluation » [Étude détaillée des référentiels de documents manuscrits. Structure, usage et évaluation], *EURASIP Journal on Image and Video Processing*, 1, 2015, <<https://doi.org/10.1186/s13640-015-0102-5>>
- International Association of Privacy Professionals (IAPP), « Global AI Law and Policy Tracker » [Législation mondiale sur l'IA et suivi des politiques], février 2024, <https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf>, consulté le 15 avril 2024
- Juneja P. et Floridi L., « Using Twitter to detect polling place issues on U.S. election days » [Détecer à l'aide de Twitter les problèmes sur les lieux de scrutin lors d'élections aux États-Unis], *SSRN*, 24 janvier 2023, <<https://doi.org/10.2139/ssrn.4334243>>
- Jungherr A., « Artificial intelligence and democracy: A conceptual framework » [Intelligence artificielle et démocratie. Cadre conceptuel], *Social Media + Society*, 9/3, 2023, <<https://doi.org/10.1177/20563051231186353>>
- Jungherr A. et Rauchfleisch A., « Negative downstream effects of alarmist disinformation discourse: Evidence from the United States » [Effets négatifs en aval du discours de désinformation alarmiste], *Political Behavior*, 2024, <<https://doi.org/10.1007/s11109-024-09911-3>>
- Kan H. J., Kharrazi H., Chang H.-Y., Bodycombe D., Lemke K. et Weiner J. P., « Exploring the use of machine learning for risk adjustment: A comparison of standard and penalized linear regression models in predicting health care costs in older adults » [Explorer l'utilisation de l'apprentissage automatique pour l'ajustement des risques. Comparaison de modèles de régression linéaire standard ou pénalisée dans la prévision des coûts de soins de santé chez les personnes âgées], *PLoS One*, 14/3, 2019, <<https://doi.org/10.1371/journal.pone.0213258>>
- Kennedy R., Wojcik S. et Lazer D., « Improving election prediction internationally » [Améliorer les prévisions électorales dans le monde], *Science*, 355/6324, 2017, p. 515-520, <<https://www.science.org/doi/10.1126/science.aal2887>>

- Kondamudi M. R., Sahoo S. R., Chouhan L. et Yadav N., « A comprehensive survey of fake news in social networks: Attributes, features, and detection approaches » [Étude détaillée des fausses informations sur les réseaux sociaux. Caractéristiques, composantes et détection], *Journal of King Saud University - Computer and Information Sciences*, 35/6, 2023, <<https://doi.org/10.1016/j.jksuci.2023.101571>>
- Kwon C., Moreno A. et Raman A., « The impact of input inaccuracy on leveraging AI tools: Evidence from algorithmic labor scheduling » [L'impact de l'imprécision des données d'entrée sur l'utilisation des outils d'IA. L'exemple de la planification algorithmique de la main d'œuvre], SSRN, 22 octobre 2023, <<https://doi.org/10.2139/ssrn.4602747>>
- Landemore H., « Fostering more inclusive democracy with AI » [Favoriser une démocratie plus inclusive avec l'IA], Fonds monétaire international (FMI), décembre 2023, <<https://www.imf.org/en/Publications/fandd/issues/2023/12/POV-Fostering-more-inclusive-democracy-with-AI-Landemore>>, consulté le 15 avril 2024
- Liu Z. et Hu S., « Predicting the fundraising performance of environmental crowdfunding projects: An interpretable machine learning approach » [Prédire le résultat des financements participatifs au bénéfice de projets pour l'environnement. Une approche d'apprentissage automatisé interprétable], *Information Processing & Management*, 61/2, 2024, <<https://doi.org/10.1016/j.ipm.2023.103587>>
- Livemint, « EC to start campaign to link voter ID with Aadhaar from August 1. Check details here » [La Commission électorale lance une campagne pour établir un lien entre la carte d'électeurs et l'identifiant biométrique Aadhaar à compter du 1^{er} août. Explications détaillées], *Mint*, 25 juillet 2022, <<https://www.livemint.com/news/india/ec-to-start-campaign-to-link-voter-id-with-aadhaar-from-august-1-check-details-here-11658748573098.html>>, consulté le 15 avril 2024
- Mann C. et Stein R. M., « The Impact of Polling Places on Voting » [L'impact des lieux de vote sur les scrutins], document préparé pour la conférence sur la réforme et l'administration de la science électorale, université de Pennsylvanie, Philadelphie (PA), juillet 2019, <<https://web.sas.upenn.edu/esra2019/files/2019/07/Mann-and-Stein-Polling-Place-Effect.pdf>>, consulté le 15 avril 2024
- Markay L., « AI becomes a political « super-weapon » [L'IA devient une « super-arme » politique], *Axios*, 7 octobre 2022, <<https://www.axios.com/2022/10/07/ai-becomes-a-political-super-weapon>>, consulté le 15 avril 2024
- MIT Election Data Science Lab, « Voting technology » [Les technologies en matière de scrutin], 21 avril 2023, <<https://electionlab.mit.edu/research/voting-technology>>, consulté le 15 avril 2024
- Mökander J. et Floridi L., « Ethics-based auditing to develop trustworthy AI » [L'audit fondé sur l'éthique pour développer une IA digne de confiance], *Minds and Machines*, 31/2, 2021, p. 323-327, <<https://doi.org/10.1007/s11023-021-09557-8>>
- Moses L. et Box-Steffensmeier J. M., « Considerations for Machine Learning Use in Political Research with Application to Voter Turnout » [Considérations sur le recours à l'apprentissage automatique dans la recherche politique, avec application à la participation électorale], 2021, <<https://polmeth.theopenscholar.com/files/polmeth/files/moses-box-steffensmeier-2020.pdf>>, consulté le 15 avril 2024

- Mughal N., « Deepfakes, Internet access cuts make election coverage hard, journalists say » [L'hypertrucage et les interruptions de la connexion à Internet rendent difficiles la couverture des élections], *Voice of America*, 22 février 2024, <<https://www.voanews.com/a/deepfakes-internet-access-cuts-make-election-coverage-hard-journalists-say-/7498917.html>>, consulté le 15 avril 2024
- Muppasani B., Pallagani V., Lakkaraju K., Lei S., Srivastava B., Robertson B., Hickerson A. et Narayanan V., « On safe and usable chatbots for promoting voter participation » [À propos des chatbots sûrs et exploitables pour favoriser la participation électorale], *AI Magazine*, 44/3, 2023, p. 240-247, <<https://doi.org/10.1002/aaai.12109>>
- National Cyber Security Centre, « The Near-Term Impact of AI on the Cyber Threat » [L'impact à court terme de l'IA sur les cybermenaces], 24 janvier 2024, <<https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>>, consulté le 15 avril 2024
- Norden L. et Ramachandran G., « Artificial intelligence and election security » [Intelligence artificielle et sécurité des élections], Brennan Center for Justice, 5 octobre 2023, <<https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-and-election-security>>, consulté le 15 avril 2024
- Noy S. et Zhang W., « Experimental evidence on the productivity effects of generative artificial intelligence » [Preuves empiriques de l'impact sur la productivité de l'intelligence artificielle générative], *Science*, 381/6654, 2023, p. 187-192, <<https://www.science.org/doi/10.1126/science.adh2586>>
- OpenAI, « How OpenAI is approaching 2024 worldwide elections » [Comment l'IA open source aborde les élections prévues en 2024 dans le monde] [blog], 15 janvier 2024, <<https://openai.com/blog/how-openai-is-approaching-2024-worldwide-elections>>, consulté le 15 avril 2024
- Organisation de coopération et de développement économiques (OCDE), Recommandation du Conseil sur l'intelligence artificielle, OECD/LEGAL/0449, adoptée le 22 mai 2019, <<https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449>>, consulté le 15 avril 2024
- Padmanabhan D., Simoes S. et MacCarthaigh M., « AI and core electoral processes: Mapping the horizons » [L'intelligence artificielle et les processus électoraux centraux. Cartographie des horizons], *AI Magazine*, 44/3, 2023, p. 218-239, <<https://doi.org/10.1002/aaai.12105>>
- Parkin B. et Bokhari F., « Imran Khan taps AI and TikTok to fight Pakistan election from jail » [Imran Kahn recourt à l'IA et à TikTok pour faire campagne au Pakistan depuis sa cellule de prison], *Financial Times*, 1^{er} février 2024, <<https://www.ft.com/content/7c3c5827-c965-453c-8bd1-d1312e90669a>>, consulté le 15 avril 2024.
- Parlement européen et Conseil de l'Union européenne, Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union européenne, 2021/0106 (COD), 2024, <<https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52021PC0206>>, consulté le 15 août 2024
- Pech L., « The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU » [Le concept d'effet inhibiteur. Son potentiel inexploité pour mieux protéger la démocratie, l'État de droit et les droits

- fondamentaux dans l'Union européenne], Open Society European Policy Institute, mars 2021, <<https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf>>, consulté le 15 avril 2024
- Perkowitz S., « The bias in the machine: Facial recognition technology and racial disparities » [Les biais dans la machine. La technologie de reconnaissance faciale et les disparités raciales], *MIT Case Studies in Social and Ethical Responsibilities of Computing*, Winter, 2021, <<https://doi.org/10.21428/2c646de5.62272586>>
- Rawte V., Sheth A. et Das A., « A survey of hallucination in large foundation models » [Étude de l'hallucination dans les grands modèles de fondation], ArXiv, 12 septembre 2023, <<https://doi.org/10.48550/arXiv.2309.05922>>
- Rayda N., « Indonesia elections 2024: How AI has become a double-edged sword for candidates and election officials » [Les élections indonésiennes de 2024. Comment l'IA est devenue une arme à double tranchant pour les candidats et les agents électoraux], CNA, 4 février 2024, <<https://www.channelnewsasia.com/asia/ai-disinformation-deepfakes-indonesia-elections-4091296>>, consulté le 15 avril 2024
- Richardson R., Schultz J. et Crawford K., « Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice » [Données douteuses, prédictions erronées. Comment les violations des droits civils influent sur les données sur la criminalité, les systèmes de police prédictive et la justice], *New York University Law Review Online*, 94/192, 2019, <<https://papers.ssrn.com/abstract=3333423>>, consulté le 15 avril 2024
- Simchon A., Edwards M. et Lewandowsky S., « The persuasive effects of political microtargeting in the age of generative artificial intelligence » [Les effets persuasifs du microciblage politique à l'ère de l'intelligence artificielle générative], *PNAS Nexus*, 3/2, 2024, p. 35, <<https://doi.org/10.1093/pnasnexus/pgae035>>
- Solender A. et Fried I., « Scoop: Congress bans staff use of Microsoft's AI Copilot » [Scoop : Le Congrès interdit l'utilisation par le personnel de l'assistant IA Copilot de Microsoft], *Axios*, 29 mars 2024, <<https://www.axios.com/2024/03/29/congress-house-strict-ban-microsoft-copilot-staffers>>, consulté le 15 avril 2024
- Stokel-Walker C., « AI chatbot models « think » in English even when using other languages » [Les modèles de chatbots basés sur l'IA « pensent » en anglais même lorsqu'ils utilisent une autre langue], *New Scientist*, 8 mars 2024, <<https://www.newscientist.com/article/2420973-ai-chatbot-models-think-in-english-even-when-using-other-languages>>, consulté le 15 avril 2024
- Suhenda D., « KPU insists on using Sirekap » [La commission électorale indonésienne déterminée à utiliser l'application Sirekap], *The Jakarta Post*, 22 février 2024, <<https://www.thejakartapost.com/indonesia/2024/02/22/kpu-insists-on-using-sirekap.html>>, consulté le 15 avril 2024
- Talarico L. et Maya Duque P. A., « An optimization algorithm for the workforce management in a retail chain » [Un algorithme d'optimisation pour la gestion du personnel dans la chaîne de vente au détail], *Computers & Industrial Engineering*, 82, 2015, p. 65-77, <<https://doi.org/10.1016/j.cie.2015.01.014>>

- Üçoğlu D., « Current machine learning applications in accounting and auditing » [Les applications d'apprentissage automatisé qui ont cours en comptabilité et en audit], *Pressacademia*, 12/1, 2020, p. 1-7, <<https://doi.org/10.17261/Pressacademia.2020.1337>>
- Valle-Cruz D., Fernandez-Cortez V. et Gil-Garcia J.R., « From e-budgeting to smart budgeting: Exploring the potential of artificial intelligence in government decision-making for resource allocation » [De la budgétisation électronique à la budgétisation intelligente. Une exploration du potentiel de l'intelligence artificielle dans les prises de décision du gouvernement concernant l'allocation des ressources], *Government Information Quarterly*, 39/2, 2022, <<https://doi.org/10.1016/j.giq.2021.101644>>
- Van Brakel R., « Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing » [La surveillance préemptive des mégadonnées et l'autonomisation (ou la perte) qu'elle entraîne. Le cas de la police prédictive], in B. van der Sloot, D. Broeders et E. Schrijvers (dir.), *Exploring the Boundaries of Big Data* [Explorer les limites des mégadonnées], La Haye, Amsterdam, Amsterdam University Press, 2016, p. 117-141, <<https://doi.org/10.2139/ssrn.2772469>>.
- Van der Staak S. et Wolf P., *Cybersecurity in Elections: Models of Interagency Collaboration*. [La cybersécurité dans les élections. Modèles de collaboration interagences] Stockholm, IDEA International, 2019, <<https://doi.org/10.31752/idea.2019.23>>
- Vandewalker I., « Digital Disinformation and Vote Suppression » [Désinformation numérique et exclusion du droit de vote], Brennan Center for Justice, 2 septembre 2020, <<https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression>>, consulté le 15 avril 2024
- Varna A., « Big data analytics and transformation of election campaign in India » [Analyse des mégadonnées et transformation de la campagne électorale en Inde], SSRN, 30 décembre 2019, <<https://doi.org/10.2139/ssrn.3511428>>
- Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser L. et Polosukhin I., « Attention is all you need » [L'attention est tout ce dont vous avez besoin], ArXiv, 6 décembre 2017, <<http://arxiv.org/abs/1706.03762>>, consulté le 15 avril 2024
- Wei A., Haghtalab N. et Steinhardt J., « Jailbroken: How does LLM safety training fail? » [Évasion. Comment l'entraînement des LLM en matière de sûreté échoue], ArXiv, 5 juillet 2023, <<https://doi.org/10.48550/arXiv.2307.02483>>
- Wolf P., Alim A., Kasaro B., Namugera P., Saneem M. et Zorigt T., *Introducing Biometric Technology in Elections* [Introduire les technologies biométriques dans les élections], Stockholm, IDEA International, 2017, <<https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections>>, consulté le 15 avril 2024
- Yamin K., Jadali N., Xie Y. et Nazzal D., « Novelty detection for election fraud: A case study with agent-based simulation data » [La détection de nouveauté appliquée à la fraude électorale. Étude de cas avec des données de simulation basée sur des agents IA], *AI Magazine*, 44/3 (2023), p. 255-262, <<https://doi.org/10.1002/aaai.12112>>

- Zhang M., Alvarez R. M. et Levin I., « Election forensics: Using machine learning and synthetic data for possible election anomaly detection » [Investigation numérique des élections. L'apprentissage automatique et les données synthétiques au service de la détection d'éventuelles anomalies], *PloS One*, 14/10 (2019), <<https://doi.org/10.1371/journal.pone.0223950>>
- Zhao, F., Zhang C., Saxena N., Wallach D. et Rabby A. S. A., « Ballot tabulation using deep learning » [La compilation des résultats de scrutins en recourant à l'apprentissage profond], in *2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science*, Institute of Electrical and Electronics Engineers, 2023, p. 107-114, <<https://doi.org/10.1109/IRI58017.2023.00026>>
- Zhou J., Zhan, Y., Luo Q., Parker A. G. et De Choudhury M., « Synthetic lies: Understanding AI-generated misinformation and evaluating algorithmic and human solutions » [Mensonges synthétiques. Comprendre la mésinformation générée par l'IA et évaluer les solutions algorithmiques et humaines], in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, New York (NY), Association for Computing Machinery, 2023, p. 1-20, <<https://doi.org/10.1145/3544548.3581318>>
- Zhuang Y., « Imran Khan's « victory speech » from jail shows A.I.'s peril and promise » [Le discours de victoire tenu par Imran Kahn depuis sa cellule de prison montre les dangers et promesses de l'IA], *The New York Times*, 11 février 2024, <<https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html>>, consulté le 15 avril 2024

Annexe A. Termes clés

Nous proposons ci-dessous quelques explications de termes techniques et non techniques liés à l'IA pour les besoins du présent rapport. Il ne s'agit pas de définitions exhaustives, mais plutôt d'une aide à la compréhension du texte.

Terme	Explication
Affiner et transférer l'apprentissage	Un processus dans lequel les modèles d'apprentissage profond peuvent être spécialisés pour une tâche spécifique tout en conservant les connaissances de leur formation initiale. Par exemple, on peut utiliser un LLM dans le but spécifique de classer les messages des réseaux sociaux comme discutant des élections en l'affinant avec un ensemble de données étiquetées de messages qui discutent des élections et qui n'en discutent pas.
Apprentissage automatique (<i>machine learning</i>)	Utilisé pour décrire des méthodes techniques développées plus récemment telles que les réseaux neuronaux, les transformateurs et les méthodes de <i>boosting/bagging</i> . Dans de nombreux cas, ces méthodes sont utilisées pour la prédiction, ce qui implique de prendre des décisions basées sur des données plutôt que d'expliquer des données antérieures.
Apprentissage non supervisé	Sous-ensemble de l'apprentissage automatique dans lequel les données de formation ne sont pas étiquetées et où l'objectif du modèle est de trouver des modèles dans les données. Un exemple serait le développement d'un modèle qui regroupe des échantillons d'écriture manuscrite similaires.
Apprentissage supervisé	Sous-ensemble de l'apprentissage automatique dans lequel les ensembles de données de formation sont étiquetés de manière que le modèle apprenne à associer les entrées à des sorties spécifiques. Un exemple serait de développer un modèle pour convertir l'écriture manuscrite en données textuelles en l'entraînant à partir d'un ensemble de données d'échantillons d'écriture manuscrite et des données textuelles correspondantes.
Apprentissage en profondeur (<i>deep learning</i>)	Sous-ensemble de l'apprentissage automatique qui utilise des réseaux neuronaux multicouches, généralement de grande taille, avec de grands ensembles de données, pour accomplir des tâches de prédiction. La plupart des exemples de progrès récents dans le domaine de l'apprentissage automatique, tels que les modèles de langage de grande taille (LLM), entrent dans cette catégorie.
Hallucination du LLM	Décrit la tendance de nombreux LLM à inventer en toute confiance des informations en réponse à des requêtes textuelles.

Terme	Explication
IA discriminante	Se réfère à un sous-ensemble de l'apprentissage automatique dans lequel les modèles sont utilisés pour classer ou séparer les données. Les LLM utilisés pour classer un texte en sentiment « positif » ou « négatif » sont des exemples d'IA discriminante.
IA générative (IAG)	Il s'agit d'un sous-ensemble de l'apprentissage automatique dans lequel les modèles sont utilisés pour générer du contenu, souvent du texte, de la vidéo ou de l'audio. Les LLM utilisés comme chatbots sont des exemples d'IA générative.
Interprétabilité	Se réfère à la capacité des gens à comprendre comment un modèle prend des décisions. Par exemple, la régression linéaire est un modèle généralement interprétable, car on peut facilement comprendre les coefficients que le modèle applique à chaque facteur. Avec un réseau neuronal multicouche, en revanche, il est beaucoup plus difficile d'interpréter pourquoi des entrées spécifiques conduisent aux sorties correspondantes.
Modèles de langage de grande taille (LLM)	Fait référence aux récentes avancées du <i>deep learning</i> dans le domaine du traitement du langage naturel, principalement dues au développement de l'architecture des transformateurs, qui ont permis d'obtenir des modèles entraînés sur de larges pans de texte. Les LLM, tels que ChatGPT, LLaMA et Gemini, peuvent être utilisés pour générer, interpréter et classer du texte.
Méthodes statistiques traditionnelles	Utilisé pour décrire des méthodes statistiques utilisées depuis longtemps, telles que les régressions linéaires et logistiques. Dans de nombreux cas, ces méthodes ont été utilisées pour l'inférence ou la formalisation de la compréhension des données.
Précision	Mesure du pourcentage d'entrées qu'un modèle classe correctement.

À propos de l'auteur

Prathm Juneja est doctorant et boursier Rhodes à l'Internet Institute de l'université d'Oxford, où son travail principal porte sur le rôle que l'IA et d'autres technologies numériques peuvent jouer dans l'amélioration de la fonction, de l'accès et de l'équité des élections. Ses autres recherches portent sur l'éthique de l'IA, la politique technologique, l'apprentissage automatique et le comportement électoral. Prathm conseille régulièrement des entreprises, des organisateurs, des gouvernements et des chargés de campagnes politiques sur l'utilisation de l'IA, la politique technologique et la politique de la technologie.

À propos d'IDEA International

L'Institut international pour la démocratie et l'assistance électorale (IDEA International) est une organisation intergouvernementale fondée en 1995, comptant 35 États Membres et avec pour mandat de soutenir la démocratie durable dans le monde entier.

QUE FAISONS-NOUS

Nous développons des recherches et des analyses politiquement neutres liées aux élections, aux parlements, aux constitutions, à la numérisation, aux changements climatiques, à l'inclusion et à la représentation politique, le tout sous l'égide des objectifs de développement durable des Nations Unies. Nous évaluons les performances des démocraties grâce à nos indices uniques sur l'état de la démocratie dans le monde et notre "Democracy Tracker".

Nous fournissons des services de renforcement des capacités et des conseils d'experts aux acteurs démocratiques, y compris aux gouvernements, parlements, agents électoraux et à la société civile. Nous développons des outils et publions des bases de données, des livres et brochures d'information dans plusieurs langues sur des sujets allant de la participation électorale aux quotas de genre.

Nous réunissons des acteurs étatiques et non étatiques pour des dialogues et partages de leçons. Nous nous consacrons à défendre, à promouvoir et à protéger la démocratie dans le monde entier.

OÙ NOUS TRAVAILLONS

Le siège d'IDEA International est situé à Stockholm et nous disposons de bureaux régionaux et de liaison en Afrique, en Asie-Pacifique, en Amérique latine, aux Caraïbes et en Europe. IDEA International a le statut d'observateur permanent auprès des Nations Unies et est également accrédité auprès des institutions de l'Union européenne.

NOS PUBLICATIONS ET BASES DE DONNÉES

Nous avons un catalogue avec plus de 1 000 publications et plus de 25 bases de données sur notre site Internet. La plupart de nos publications peuvent être téléchargées gratuitement.

<https://www.idea.int>

IDEA International
Strömsborg
SE-103 34 Stockholm
SUÈDE
+46 8 698 37 00
info@idea.int
www.idea.int



Le sujet de l'intelligence artificielle (IA) prenant de l'ampleur, et notamment le rôle qu'elle peut jouer pour influencer une élection, les organes de gestion des élections (OGE) doivent élaborer des plans pour répondre à l'IA et, dans certains cas, l'utiliser pour maintenir des élections libres, équitables et sûres. L'IA est une catégorie de technologies qui évolue rapidement et qui n'est pas réglementée, en grande partie. De plus, très peu de recherches ont été menées jusqu'à présent concernant son impact potentiel sur les élections.

Ce rapport vise à aider les organes de gestion électorale et les autres parties concernées à mieux comprendre les possibilités, les défis et les implications juridiques de l'utilisation de l'IA dans le cadre des élections.

ISBN: 978-91-7671-801-8 (édition PDF)