IVADO

Initiative IA + Société
AI + Society

Quando l'intelligenza artificiale interferisce con le elezioni

Quattro azioni per salvaguardare l'integrità elettorale e sostenere la democrazia[1]

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

Punti chiave

- Esempi recenti di Brasile, Romania, Gabon, Stati Uniti e altri Paesi mostrano come l'uso dell'IA da parte di attori politici possa danneggiare l'integrità elettorale e la democrazia.
- Le nazioni sono spesso impreparate ad affrontare le sfide legate all'IA: molte non hanno regole che disciplinino l'IA nelle elezioni, i partiti politici non si sono accordati su pratiche elettorali eque nell'era dell'IA e la maggior parte delle giurisdizioni non è in grado di contrastare efficacemente gli attacchi alle proprie istituzioni democratiche.
- Raccomandiamo quattro azioni: i governi dovrebbero aggiornare le norme elettorali (ad esempio, per proibire contenuti ingannevoli generati dall'IA); i partiti politici dovrebbero adottare un codice di condotta con linee guida chiare sull'uso politico responsabile dell'IA; le autorità elettorali dovrebbero istituire team indipendenti per prevenire e rispondere ai disagi causati dall'IA; a livello internazionale, i governi dovrebbero istituire dei fiduciari elettorali internazionali per l'IA e protocolli per affrontare le interferenze transfrontaliere.

Perché l'intelligenza artificiale e le elezioni sono un argomento essenziale

Le tecnologie hanno da tempo influenzato le elezioni, sia in positivo che in negativo, plasmandone gli esiti e la qualità del dibattito pubblico che le riguarda. Ad esempio, Internet permette ai cittadini di organizzarsi in modo più efficace che mai, consentendo loro di sostenere idee e cause specifiche, ma è anche un formidabile canale di disinformazione.

L'ascesa dell'intelligenza artificiale (IA) presenta nuove minacce significative, tra cui la moltiplicazione dei deepfake, l'aumento dei rischi per la sicurezza informatica, l'emergere di agenti persuasivi manipolatori e la proliferazione di dati sintetici e account falsi. Allo stesso tempo, l'IA offre agli attori politici un potente strumento per entrare in contatto con gli elettori, influenzare l'opinione pubblica e modellare il flusso di informazioni. Sfruttando le tendenze esistenti nelle elezioni, l'IA ha il potenziale per rimodellare profondamente il processo democratico e influenzare i risultati elettorali. Senza misure proattive, tuttavia, l'IA potrebbe esacerbare tendenze preoccupanti come la polarizzazione politica e il calo della fiducia nella democrazia.

I governi devono intraprendere un'azione decisiva per quanto riguarda l'IA, in particolare in un momento in cui le democrazie di tutto il mondo stanno affrontando sfide e attacchi crescenti alle loro elezioni. Agendo su vari fronti, essi rafforzeranno i sistemi democratici, miglioreranno la fiducia nella società e garantiranno che l'IA venga sfruttata in modo responsabile per migliorare l'integrità delle elezioni.

Come l'intelligenza artificiale rappresenta una minaccia per le elezioni e la democrazia

Ci sono molti modi in cui l'uso dell'IA da parte di attori politici, sia locali che stranieri, può finire per danneggiare l'integrità delle elezioni e della democrazia.

Ad esempio, nell'ottobre 2024 si sono tenute in Brasile le elezioni. Uno studio del Digital Forensic Research Lab ha rilevato che nei sei mesi precedenti il giorno delle elezioni, i politici locali o i loro sostenitori hanno utilizzato l'IA almeno 75 volte per produrre immagini sintetiche, contenuti audio o video per promuovere le loro candidature o indebolire gli avversari. In particolare, cinque candidate donne sono state vittime della pornografia deepfake[2], un fenomeno il cui impatto è spesso quello di scoraggiare le donne dall'assumere ruoli pubblici[3].

Nel dicembre 2024, il Servizio di intelligence estera della Romania ha riferito che la Russia ha preso di mira il Paese nel tentativo di influenzarne le elezioni presidenziali. In primo luogo, la Russia ha utilizzato la propaganda di estrema destra e pro-russa e contenuti generati dall'IA che ha diffuso attraverso una vasta rete di canali di social media e account generati dall'IA. In secondo luogo, con l'aiuto dell'intelligenza artificiale (che può aiutare a sviluppare malware in grado di eludere le difese di sicurezza informatica), si presume che la Russia abbia organizzato circa 85.000 attacchi contro l'Autorità elettorale permanente rumena per ottenere l'accesso ai suoi database. L'interferenza russa ha infine portato la Corte costituzionale rumena ad annullare il primo turno delle elezioni presidenziali[4].

Nella campagna elettorale del 2023 in Gabon, è scoppiata una controversia mentre gli elettori si preparavano a uno storico triplo voto, presidenziale, legislativo e locale. Verso la fine della campagna, sono emerse online delle registrazioni audio in cui due figure di spicco dell'opposizione avrebbero presumibilmente discusso di strategie, alleanze e sostegno esterno. Il presidente in carica ha accusato l'opposizione di "fomentare una rivolta popolare", mentre la coalizione di opposizione ha condannato le registrazioni come un "uso disonesto dell'IA". Il caso del Gabon evidenzia come l'ascesa dell'IA complichi il dibattito pubblico, rendendo sempre più difficile per gli elettori distinguere la realtà dalla finzione[5].

Infine, durante la campagna elettorale per le elezioni presidenziali statunitensi del 2024, gli esperti hanno testato i principali modelli di IA per verificare la loro capacità di fornire informazioni accurate sulle elezioni. Questi test hanno mostrato discrepanze per quanto riguarda le informazioni in diverse lingue e tra gli impegni dichiarati dalle aziende di IA per un'informazione elettorale precisa e le performance dei loro modelli[6]. Questi esempi mostrano come le nazioni e i governi spesso non siano preparati ad affrontare le sfide poste dall'ascesa dell'IA. Le nostre raccomandazioni suggeriscono modi per evitare o mitigare gli impatti negativi che le tecnologie emergenti hanno sulle elezioni.

Le elezioni locali sono particolarmente vulnerabili all'influenza dell'IA, poiché le democrazie locali spesso non hanno le risorse e le garanzie per contrastare efficacemente i suoi rischi.

Prima sfida
Molti governi non hanno ancora adottato regole che disciplinino l'uso dell'IA nelle elezioni

L'assenza di norme chiare e specifiche che regolino l'uso dell'IA nelle elezioni crea incertezza giuridica, rendendo difficile per le autorità attribuire responsabilità o intraprendere azioni efficaci contro gli abusi.

Molte leggi elettorali in tutto il mondo sono state adottate anni prima che l'IA generativa diventasse pubblicamente disponibile e ampiamente utilizzata. Di conseguenza, sono spesso troppo ampie per affrontare i rischi unici posti dall'IA. Ad esempio, molte legislazioni mancano di definizioni di "media sintetici" o "contenuti generati dall'IA" e non definiscono i limiti del loro utilizzo nel contesto delle elezioni.

Pochi organi legislativi hanno adottato o anche solo discusso proposte di norme elettorali che affrontino specificamente le sfide dell'IA nelle elezioni. Nel Regno Unito, ad esempio, le leggi esistenti sulla diffamazione si concentrano sulla protezione degli individui dalle dichiarazioni false, ma sono ambigue quando si tratta di immagini o video falsi[7].

Regole chiare e armonizzate sono essenziali per garantire la responsabilità, migliorare la trasparenza e consentire interventi tempestivi. Colmando queste lacune normative, i responsabili politici possono fornire solide garanzie per sostenere l'integrità dei processi democratici e ridurre la crescente insicurezza che circonda le sfide elettorali guidate dall'intelligenza artificiale.

Azione 1
I governi dovrebbero aggiornare le norme elettorali

I governi dovrebbero aggiornare le norme elettorali per garantire che i politici, i partiti politici e le aziende tecnologiche, così come gli elettori, sappiano con precisione:

- → **come i media sintetici possono essere utilizzati per le attività elettorali;**
- → **quali usi dei sistemi di IA sono vietati o limitati nel contesto delle elezioni; e**
- → **come deve essere attribuita la responsabilità in caso di violazione degli obblighi stabiliti dalle norme elettorali.**

Per garantire che la libertà di comunicazione politica non sia significativamente limitata, le nuove norme elettorali dovrebbero essere proporzionate al rischio che intendono prevenire. Le autorità indipendenti che vigilano l'IA nelle elezioni avranno bisogno di competenze tecniche e finanziamenti adeguati per applicare efficacemente queste regole.

Le giurisdizioni dovrebbero chiarire le definizioni di termini chiave, come dati sintetici, IA generativa, contenuti di IA generativa e informazioni fuorvianti o ingannevoli, e valutare la necessità di modificare aspetti particolari delle loro norme attuali. Inoltre, dovrebbero prendere seriamente in considerazione l'adozione delle seguenti norme obbligatorie:

- → **Dovrebbero essere introdotti divieti sull'uso, la pubblicazione, la proiezione o la circolazione di contenuti ingannevoli generati dall'IA per influenzare le elezioni. Ad esempio, i governi dovrebbero prendere in considerazione la possibilità di vietare l'uso di immagini, video o audio generati dall'IA che ritraggono candidati o campagne referendarie in modo falso o fuorviante, o che amplificano la disinformazione su un candidato, una campagna referendaria o sul processo elettorale;**
- → **I politici e i partiti politici dovrebbero essere tenuti a rispettare gli obblighi di trasparenza, come l'etichettatura delle immagini, dei clip audio e dei video generati dall'IA e utilizzati, pubblicati, proiettati o diffusi durante le elezioni. Per creare o migliorare queste etichette, i governi dovrebbero studiare la ricerca scientifica e raccogliere i suggerimenti del pubblico. Le etichette dovrebbero essere facilmente riconoscibili dai cittadini, tenendo conto di aspetti quali il design visivo, la formulazione, le dimensioni, la durata, la posizione e la tempistica;**
- → **I governi dovrebbero obbligare le piattaforme online a implementare politiche di etichettatura per gli annunci politici generati dall'IA e a creare e applicare rigorosamente regole di moderazione dei contenuti per frenare la diffusione di contenuti dannosi generati dall'IA.**

Le norme elettorali dovrebbero riguardare i chatbot, che possono produrre informazioni fuorvianti su elementi chiave di un'elezione, come l'ubicazione dei seggi elettorali, i documenti necessari per votare o i precedenti penali dei candidati [8]***.***

Seconda sfida
I partiti politici non hanno trovato un accordo su cosa si intenda per elezioni libere ed eque nell'era dell'intelligenza artificiale

I partiti politici e i candidati possono ora potenzialmente sfruttare gli strumenti di IA per creare sofisticati deepfakes, generare contenuti ingannevoli su larga scala, micro-targettizzare gli elettori con

disinformazione personalizzata o manipolare il discorso pubblico attraverso account automatizzati.

In assenza di una regolamentazione, di linee guida chiare o di principi etici, c'è il rischio che i partiti politici possano utilizzare l'IA in modo da contribuire a minare la fiducia degli elettori, a diffondere false informazioni e a influenzare ingiustamente i risultati delle elezioni.

Senza norme concordate, i partiti politici potrebbero sentirsi costretti a intensificare l'uso degli strumenti di IA in modi sempre più aggressivi per evitare di rimanere indietro rispetto agli avversari. La pressione politica potrebbe creare una spirale in cui i partiti danno la priorità all'uso dell'IA per vincere ad ogni costo rispetto al mantenimento dell'integrità elettorale.

Azione 2
I partiti dovrebbero adottare un codice di condotta come punto di partenza per assumersi la responsabilità del comportamento politico nell'era dell'IA

I codici di condotta mirano a far sì che gli attori politici accettino di impegnarsi per elezioni libere ed eque adottando determinati comportamenti o evitandone altri. I codici di condotta sull'IA sostengono generalmente la trasparenza e l'onestà nell'uso di questa tecnologia a fini elettorali.

Tali codici esistono già in alcune giurisdizioni. Ad esempio, nel 2023, cinque partiti svizzeri si sono impegnati a essere trasparenti nell'uso dell'IA e a non utilizzarla per scopi denigratori. Per le elezioni del Parlamento europeo del 2024, i partiti europei hanno approvato congiuntamente un codice di condotta con disposizioni specifiche sull'uso dell'IA. Paesi come il Regno Unito ed enti subnazionali si sono adoperati per sviluppare codici di questo tipo.

I codici di condotta sull'uso dell'IA a fini elettorali dovrebbero impegnare i partiti a:

- → **non utilizzare strumenti di IA per produrre contenuti materialmente fuorvianti o ingannare gli elettori;**
- → **etichettare chiaramente i contenuti quando le parti ricorrono all'IA in modo rilevante (date le lacune legislative identificate in precedenza e l'urgenza della questione);**
- → **non amplificare contenuti sintetici materialmente fuorvianti e segnalare comportamenti scorretti nella pubblicazione o nell'amplificazione di contenuti fuorvianti;**
- → **fornire linee guida chiare e una formazione adeguata al personale del partito, ai membri, agli attivisti e ai sostenitori sull'uso degli strumenti di IA per le campagne;**
- → **astenersi dal produrre, utilizzare o diffondere contenuti ingannevoli, compresi account falsi, bot automatici o chatbot, per manipolare le opinioni degli elettori;**
- → **introdurre "livelli di moderazione" nei loro chatbot in modo da indirizzare gli utenti di Internet verso le informazioni elettorali ufficiali; e**
- → **impegnarsi a monitorare, controllare e rivedere dopo le elezioni l'uso dell'IA e degli strumenti ad essa abilitati.**

Terza sfida
La maggior parte delle giurisdizioni non è preparata ad affrontare gli attacchi dell'IA alle elezioni e alle istituzioni democratiche

I governi hanno sviluppato strategie e meccanismi per far fronte a gravi crisi come disastri naturali, disordini civili o pandemie. Molti governi, tuttavia, non sono pronti ad affrontare attacchi guidati dall'intelligenza artificiale contro l'integrità delle loro elezioni e delle istituzioni democratiche.

Affrontare con successo le minacce all'integrità elettorale guidate dall'intelligenza artificiale è una sfida dalle molteplici sfaccettature.

In primo luogo, i governi spesso non dispongono di sistemi di monitoraggio completi per individuare la disinformazione generata dall'IA, i deepfake e altre campagne di influenza automatizzate che hanno come obiettivo i loro processi democratici. Questa carenza di conoscenze è aggravata dall'insufficienza dei meccanismi di collaborazione tra le parti interessate, come le agenzie governative, le piattaforme di social media, le organizzazioni giornalistiche e i gruppi della società civile. Quando vengono rilevate attività sospette, spesso non esiste un protocollo chiaro per condividere le informazioni o coordinare una risposta.

In secondo luogo, molti funzionari elettorali non possiedono adeguate conoscenze sull'intelligenza artificiale per riconoscere le minacce, e non sono quindi in grado di intervenire. Questa lacuna di conoscenza spesso si estende all'intero ecosistema democratico. Ad esempio, gli addetti ai seggi e gli osservatori elettorali, che sono i difensori in prima linea dell'integrità elettorale, in genere ricevono una formazione minima sulle minacce digitali e possono avere difficoltà a gestire le domande degli elettori sui contenuti generati dall'intelligenza artificiale o sui tentativi di manipolazione.

In terzo luogo, le agenzie governative spesso non dispongono delle infrastrutture tecniche, delle competenze umane e delle capacità necessarie per monitorare e contrastare efficacemente gli attacchi guidati dall'intelligenza artificiale. In mancanza di questi elementi, le giurisdizioni sono costrette a reagire agli incidenti su base occasionale piuttosto che implementare strategie di difesa proattive.

Azione 3
Le autorità elettorali dovrebbero istituire un team indipendente e interfunzionale incaricato di prevenire e rispondere alle perturbazioni elettorali causate dall'IA

Le autorità elettorali dovrebbero affidarsi a un team indipendente e interfunzionale che operi sotto la supervisione giudiziaria. Questo team dovrebbe essere supportato da tutte le parti interessate ai processi democratici ed elettorali di una giurisdizione. Dovrebbe avere collegamenti appropriati con gli attori dell'ambiente mediatico, le piattaforme online e altre entità regionali o internazionali pertinenti. Dovrebbe inoltre includere rappresentanti dei partiti politici per garantire che i protocolli di emergenza e di mitigazione siano considerati equi ed equilibrati.

Il team dovrebbe operare durante e al di fuori del ciclo elettorale per mantenere la vigilanza sugli attacchi alla democrazia. Sarebbe responsabile dello sviluppo di un piano di risposta pubblico e completo per le minacce dell'IA alle elezioni. Il Piano di Risposta Elettorale all'IA definirebbe quadri di valutazione chiari, responsabilità, approcci di comunicazione, ecc. Questo approccio si ispira alle strategie di preparazione alle emergenze già consolidate in settori come la gestione delle crisi della sanità pubblica, la risposta ai disastri naturali e la preparazione agli incidenti di cybersicurezza, che hanno implementato con successo sistemi di allerta precoce, protocolli di segnalazione, divulgazione obbligatoria degli incidenti, accordi di condivisione delle risorse e squadre di risposta rapida.

Tutti gli attori dell'ecosistema dei media e di Internet devono partecipare all'attuazione del piano di risposta per limitare la diffusione di un attacco e allertare i cittadini.

Le autorità elettorali dovrebbero condurre esercitazioni o simulazioni teoriche per consentire agli attori di capire come l'IA può essere impiegata e utilizzata, identificare e testare il piano di risposta e le reazioni concrete agli incidenti, nonché identificare le possibili vulnerabilità che gli attori disonesti potrebbero sfruttare.

Il Piano di Risposta Elettorale all'AI deve tenere conto dei diritti fondamentali dei cittadini a difendersi dalle minacce di sorveglianza o di controllo dell'espressione politica.

Per garantire che le perturbazioni elettorali causate dall'IA siano contrastate in modo efficace, è necessario fornire un'adeguata formazione in materia di IA e sicurezza informatica a tutti gli attori dell'ecosistema democratico ed elettorale, compresi i volontari dei seggi elettorali e gli osservatori.

Quarta sfida
L'interferenza elettorale supportata dall'IA spesso coinvolge attori occulti che operano in più giurisdizioni

La natura transnazionale di molti attacchi elettorali guidati dall'IA spiega perché è difficile per le singole giurisdizioni affrontarli da sole in modo efficace. Il problema è complicato dall'asimmetria di risorse e conoscenze tra i governi, in quanto alcuni non dispongono delle competenze, degli strumenti, delle risorse o delle capacità necessarie per individuare e contrastare adeguatamente le minacce elettorali guidate dall'IA.

Senza protocolli internazionali allineati, è difficile chiamare i responsabili a rispondere delle loro azioni a causa delle differenze nei sistemi giuridici, nelle capacità investigative e nei confini giurisdizionali.

Gli Stati democratici dovrebbero riconoscere che un attacco a una democrazia è un attacco ai principi che uniscono tutte le democrazie. L'azione collettiva è quindi essenziale per proteggere i valori democratici condivisi, aumentare la fiducia dei cittadini e garantire l'integrità delle elezioni in tutto il mondo.

Azione 4
I governi dovrebbero istituire degli International AI Electoral Trustkeepers e protocolli internazionali per l'assistenza legale reciproca in caso di interferenze elettorali legate all'AI

Gli Stati dovrebbero istituire una piattaforma e un'unità internazionale centralizzata per conoscere e reagire ai casi di interferenza elettorale legati all'IA: gli International AI Electoral Trustkeepers.

Questi ultimi comprenderebbero esperti multidisciplinari e istituzioni impegnate a rilevare, contrastare e mitigare le interferenze elettorali guidate dall'IA. Essi fungerebbero da risorsa tecnica per i Paesi vulnerabili alle interferenze elettorali tramite l'IA. Offrirebbero competenze, strumenti e collaborazione per affrontare le minacce elettorali transnazionali. Gli International AI Electoral Trustkeepers offrirebbero anche un supporto in caso di crisi, dispiegando squadre di pronto intervento per assistere durante eventi elettorali attivi e fornire strategie di monitoraggio e mitigazione in tempo reale in scenari ad alto rischio.

La creazione dell'International AI Electoral Trustkeepers potrebbe emergere o essere allineata con le iniziative esistenti che mirano a fornire assistenza elettorale o a proteggere i Paesi dai possibili danni dell'IA. Ad esempio, si potrebbero adottare misure per fornire risorse nuove o migliori in materia di IA (ad esempio, esperti ad hoc o specialisti permanenti) o competenze (ad esempio, tecniche o legali) alla Divisione di Assistenza Elettorale delle Nazioni Unite[9], che aiuta gli Stati membri a tenere elezioni che esprimano legittimamente la volontà del popolo e siano ritenute credibili dagli stakeholder nazionali. La nascente Rete internazionale degli Istituti di sicurezza dell'IA potrebbe essere sfruttata per questa iniziativa per formare i Trustkeepers elettorali e dispiegarli in tutto il mondo in missioni specifiche.

Quando è necessaria l'esperienza del settore, gli International AI Electoral Trustkeepers potrebbero essere supportati da operatori del settore privato, come le aziende di IA e di piattaforme che sono dietro al Tech Accord to Combat AI-Generated Election Interference[10].

Il ricorso a meccanismi di assistenza giudiziaria reciproca sarà essenziale anche per le indagini e i procedimenti giudiziari relativi a casi di interferenze elettorali causate dall'IA, in quanto faciliterà la cooperazione senza soluzione di continuità tra le varie giurisdizioni, aiuterà a raccogliere e condividere prove ammissibili provenienti da più Paesi e garantirà che gli autori di reati che utilizzano l'IA per manipolare le elezioni a livello transnazionale non possano sfruttare i confini giurisdizionali per eludere le proprie responsabilità. Tali meccanismi giudiziari hanno già affrontato efficacemente altre sfide transnazionali che richiedono cooperazione transfrontaliera e condivisione delle prove, come la lotta alla criminalità informatica, alle frodi digitali, al terrorismo, alla criminalità organizzata, alle violazioni dei diritti umani e ai crimini di guerra.

Questi meccanismi internazionali dovranno essere trasparenti per garantire la salvaguardia dei diritti fondamentali.

Conclusione

L'impatto dell'IA sulla democrazia non è definitivo.

Sebbene questo documento si sia concentrato sui rischi, l'IA potrebbe effettivamente rafforzare le democrazie. I funzionari elettorali potrebbero utilizzare strumenti di IA per gestire in modo efficiente compiti complessi. Questi strumenti potrebbero rendere il voto più accessibile e aumentare la partecipazione civica. Ad esempio, durante le contestate elezioni del 2024 in Pakistan, l'IA ha permesso al partito di un leader dell'opposizione incarcerato di trasmettere messaggi audio agli elettori e di mobilitarli nonostante le restrizioni[11]. In prospettiva, i sostenitori della democrazia dovrebbero studiare come l'IA possa migliorare i sistemi democratici.

Ora, però, la priorità è proteggere le democrazie da una minaccia pressante: gli attori disonesti, sia nazionali che stranieri, che abusano dell'IA.

Ciò richiede un'azione a due livelli.

All'interno dei Paesi, i governi devono aggiornare le loro leggi, i partiti politici devono collaborare e le autorità elettorali devono prepararsi a difendere l'integrità democratica contro coloro che abusano dell'IA.

Tra i Paesi, la cooperazione è essenziale. Nessuna nazione può affrontare le sfide dell'IA da sola. I Paesi devono allineare le loro leggi sulle interferenze elettorali consentite dall'IA. Questo rafforzerà le difese individuali e creerà una resistenza collettiva contro i tentativi di minare la democrazia in tutto il mondo.

Compiendo questi passi oggi, creeremo sistemi democratici più forti, più inclusivi e più affidabili per il domani.

Notes

1. La versione originale di questo testo è stata prodotta in inglese con il titolo AI in the Ballot Box. La traduzione in italiano è stata realizzata dalla Delegazione del Québec a Roma.
2. Farrugia, B. (2024, 26 novembre). La legge brasiliana sul *deepfake* elettorale è stata testata con contenuti generati dall'IA che hanno preso di mira le elezioni locali. DFRLab. https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes
3. Per maggiori informazioni su come l'IA presenti serie preoccupazioni per la sicurezza delle donne, si veda: Organizzazione delle Nazioni Unite per l'Educazione, la Scienza e la Cultura. (2023). *Technology-facilitated gender-based violence in an era of generative AI (World Trends in Freedom of Expression and Media Development Series).* https://unesdoc.unesco.org/ark:/48223/pf0000387483
4. Harward, C. (6 dicembre 2023). *Likely Kremlin-backed election interference against Romania threatens Bucharest's continued support for Ukraine and NATO. Institute for the Study of War.* https://understandingwar.org/backgrounder/likely-kremlin-backed-election-interference-against-romania-threatens-bucharests
5. RFI. (23 agosto 2023). *Élections au Gabon: polémique après des enregistrements supposés de candidats de l'opposition.* RFI. https://www.rfi.fr/fr/afrique/20230823-%C3%A9lections-au-gabon-pol%C3%A9mique-apr%C3%A8s-des-enregistrements-suppos%C3%A9s-de-candidats-de-l-opposition
6. Palta, R., Angwin, J., & Nelson, A. (27 febbraio 2024). *How we tested leading AI models performance on election queries.* Proof. https://www.proofnews.org/how-we-tested-leading-ai-models-performance-on-election-queries ; Impelli, M. (31 ottobre 2024). *Voting rights groups warn about AI generating unfounded claims in Spanish*. Newsweek. https://www.newsweek.com/2024-election-spanish-latino-voters-artifical-intelligence-concerns-1978170; Ott, H., & Lyons, E. (25 giugno 2024). *ChatGPT gave incorrect answers to questions about how to vote in battleground states.* CBS News. https://www.cbsnews.com/news/chatgpt-chatbot-ai-incorrect-answers-questions-how-to-vote-battleground-states
7. Stockwell, S., Hughes, M., Swatton, P., & Bishop, K. (2024). *AI-enabled influence operations: the threat to the UK general election.* CETaS Briefing Papers. https://cetas.turing.ac.uk/sites/default/files/2024-05/cetas_briefing_paper_-_ai-enabled_influence_operations_-_the_threat_to_the_uk_general_election.pdf
8 Kaye, R. (5 aprile 2023). *Australian mayor readies world's first defamation lawsuit over ChatGPT content.* Reuters. https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05
9. Dipartimento delle Nazioni Unite per gli Affari politici e di pace. (2023). Scheda informativa 2023: assistenza elettorale. https://dppa.un.org/sites/default/files/electoral_assistance.pdf
10. *AI Elections Accord (16 febbraio 2024). A tech accord to combat deceptive use of AI in 2024 elections*. https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL_.pdf
11. Zhuang, Y. (11 febbraio 2024). Il "discorso di vittoria" di Imran Khan dal carcere mostra i rischi e le promesse dell'A.I. The New York Times. https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html

I *Global Policy Brief on AI*

L'iniziativa Global Policy Brief on AI è un'iniziativa congiunta di IVADO, il principale consorzio canadese di ricerca e mobilitazione delle conoscenze sull'IA dell'Université de Montréal, e della initiative IA + Société, da Université d'Ottawa, con l'obiettivo di fornire ai responsabili politici delle linee guida basate su dati concreti per affrontare le principali sfide globali attuali in materia di IA.

Per questa prima edizione, i professori Catherine Régis e Florian Martin-Bariteau hanno riunito un gruppo di esperti di IA da tutto il mondo per sviluppare una guida politica orientata all'azione a livello globale sull'impatto dell'IA sulla democrazia e sull'integrità elettorale. Il documento è stato prodotto a seguito di un ritiro di una settimana ospitato dalla Società Italiana per l'Organizzazione Internazionale (SIOI) a Roma, Italia, nel dicembre 2024. È stato scritto con il supporto di Réjean Roy, direttore della Mobilitazione della conoscenza dell'IVADO.

Questo progetto è stato intrapreso grazie al contributo del Fonds de recherche du Québec, del CEIMIA, della Chaire Canada-CIFAR en IA et droits de la personne presso Mila, e della Chaire de recherche de l'Université d'Ottawa en technologie et société, e con l'aiuto della Delegazione del Québec a Roma e della SIOI per l'organizzazione del ritiro.

Le opinioni espresse in questo policy brief sono esclusivamente quelle degli autori.

Catherine Régis è professoressa di diritto all'Université de Montréal e direttrice dell'Innovazione sociale e politica internazionale di IVADO. Esperta di governance dell'IA, co-dirige i programmi di ricerca dell'Institut canadien de la sécurité de l'IA e detiene la Chaire Canada-CIFAR en IA et droits de la personne presso Mila.

Florian Martin-Bariteau è titolare della Chaire de recherche en technologie et société e professore associato di diritto presso l'Université d'Ottawa, dove dirige l'initiative AI + Société e il Centre de recherche en droit, technologie et société. È associato al Berkman-Klein Center dell'Università di Harvard.

Professore assistente presso la Lincoln Alexander School of Law della Toronto Metropolitan University, **Jake Okechukwu Effodu**h è specializzato in diritto dell'IA e diritti umani internazionali. Contribuisce allo sviluppo di quadri normativi sull'IA in diversi Paesi e dirige importanti progetti di ricerca Canada-Africa.

Juan David Gutiérrez, professore associato presso l'Universidad de los Andes di Bogotà, studia le intersezioni tra politiche pubbliche e tecnologie. In qualità di membro esperto della Global Partnership on Artificial Intelligence (GPAI), è co-responsabile del progetto sulla trasparenza algoritmica.

Gina Neff è professoressa di IA responsabile presso la Queen Mary University di Londra e dirige il Minderoo Centre for Technology and Democracy dell'Università di Cambridge. La sua ricerca analizza l'impatto degli ambienti digitali sul lavoro e sulla vita quotidiana.

Esperto legale specializzato in diritto digitale, **Carlos Affonso Pereira** è professore presso l'Universidade do Estado do Rio de Janeiro (UERJ) e dirige l'Instituto de Tecnologia e Sociedade (ITS Rio). Come professore di diritto e tecnologia, ha contribuito allo sviluppo delle leggi brasiliane su Internet e sulla protezione dei dati.

Professoressa di diritto privato all'Université Paris 1 Panthéon-Sorbonne, **Célia Zolynski** è specializzata in diritto digitale e proprietà intellettuale. In qualità di coordinatrice dell'Osservatorio sull'IA di Paris 1, si concentra sulla regolamentazione dell'IA e sui diritti fondamentali.

Un'iniziativa congiunta di

IVADO

uOttawa | Initiative IA + Société AI + Society

Con il supporto di

Fonds de recherche Québec

CIFAR

ceimia

Questa iniziativa è stata intrapresa grazie anche ai finanziamenti del *Fonds d'excellence en recherche Apogée Canada.*