



BOITE À OUTILS DE L'OBSERVATOIRE

DES DROITS NUMÉRIQUES
EN PERIODE ELECTORALE EN
AFRIQUE

BOITE À OUTILS DE L'OBSERVATOIRE DES DROITS NUMÉRIQUES EN PERIODE ELECTORALE EN AFRIQUE (DREAMT)

(PREMIÈRE ÉDITION)

Août 2025

Chercheurs :

**Thobekile Matimbe and
Sani Suleiman**

Expert en sécurité numérique :

Angela Onyegbuna

Conception et mise en page

Kenneth Oyeniya

Publié par
Paradigm Initiative

Avec le soutien de
Privacy International

BOITE À OUTILS DE L'OBSERVATOIRE DES DROITS NUMÉRIQUES EN PERIODE ELECTORALE EN AFRIQUE (DREAMT)

Remerciements

Ce guide est une publication de Paradigm Initiative soutenue par Privacy International. Le projet remercie ces derniers pour leur soutien financier et leur collaboration.



À qui s'adresse cette boîte à outils?

Ce guide peut aider les personnes ou les organisations qui s'identifient comme observateurs ou surveillants électoraux à évaluer la situation avant, pendant et après une élection. Les surveillants électoraux sont des personnes qui ont pour mandat d'observer le processus électoral et d'intervenir si les lois ou les procédures standard sont violées ou ignorées.¹ *Les observateurs électoraux* sont des personnes indépendantes et non partisans accréditées qui ont pour mandat d'observer un processus électoral sans toutefois intervenir dans celui-ci.² La période électorale (la période) mentionnée dans cette boîte à outils pour la surveillance des droits numériques et des élections couvre les phases suivantes :

- Phase préélectorale (0 à 6 mois).
- Jours d'élection
- Phase postélectorale (jusqu'à 3 mois).



Comment utiliser la boîte à outils?

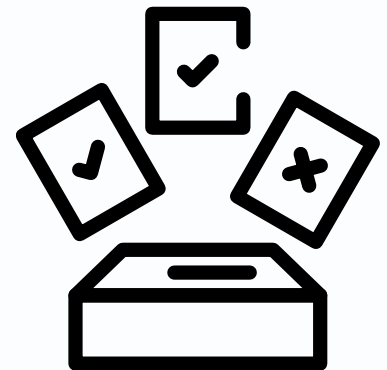
Cette boîte à outils est simple, pratique et facile à utiliser. Vous pouvez la lire pour comprendre les enjeux clés des élections et utiliser les outils et ressources de surveillance pour documenter et signaler les menaces et violations des droits numériques. Si vous êtes formateur, vous pouvez adapter cette boîte à outils au contexte national, en citant des exemples pertinents tirés du pays. Faites référence à Paradigm Initiative (PIN) lorsque vous dispensez une formation à l'aide de cet outil et fournissez des commentaires de suivi via les différentes plateformes de PIN.³

¹ https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf

² https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf

³ <https://paradigmhq.org/>

LES DROITS NUMÉRIQUES DANS LES ÉLECTIONS



Aperçu

Les Nations unies ont établi que les droits numériques sont des droits humains en ligne, comme indiqué dans l'encadré ci-dessus. Il s'agit de droits humains exercés et jouis grâce à l'utilisation des technologies numériques. Les droits numériques sont transversaux et leur violation peut affecter les droits civils, politiques et socio-économiques.

La 32^e session du Conseil des droits de l'homme des Nations Unies en 2016 a établi sa position comme suit :

‘« 1. Affirme que les mêmes droits dont jouissent les personnes hors ligne doivent également être protégés en ligne, en particulier la liberté d'expression, qui s'applique sans considération de frontières et par le biais de tout média de son choix, conformément à l'article 19 de la Déclaration universelle des droits de l'homme et au Pacte international relatif aux droits civils et politiques ; »,'

Les périodes électorales sont des moments critiques où les citoyens d'un pays exercent leurs droits civils et politiques, en exprimant leur choix par le vote. Les périodes électorales sont des moments où la non-discrimination, la liberté d'expression, la liberté de réunion et d'association pacifiques, la vie privée et l'accès à l'information sont des droits humains vulnérables dans des contextes répressifs, qui peuvent être violés, entre autres. Certains pays africains ont désormais adopté des technologies d'enregistrement biométrique des électeurs, permettant aux citoyens de s'inscrire sur les listes électorales. Directement ou indirectement, les élections sont désormais alimentées par Internet. Certains pays qui ne dépendent pas largement des technologies numériques sont néanmoins liés à la technologie sous une forme ou une autre. Le discours politique s'exerce désormais au-delà des espaces hors ligne, ayant également migré vers des plateformes en ligne telles que Facebook et X. Les acteurs politiques peuvent désormais

accéder à l'électorat via WhatsApp et d'autres plateformes de communication.

L'ère numérique a apporté d'immenses avantages, en améliorant l'accès à l'information pendant les élections grâce aux médias en ligne, en particulier lorsque certains pays sont encore confrontés au défi de ne pas disposer de médias pluralistes. Alors que dans le passé, les partis politiques au pouvoir monopolisaient les médias nationaux traditionnels, les plateformes médiatiques en ligne offrent aujourd'hui une solution pour faire progresser la liberté des médias en Afrique. L'éventail des menaces numériques pesant sur les élections ne cesse de s'élargir. Dans le cadre de cette boîte à outils, nous examinons les thèmes clés suivants :

1. Coupures d'Internet
2. Protection des données
3. Intégrité de l'information
4. Liberté d'expression
5. Accès à l'information

NORMES RÉGIONALES ET INTERNATIONALES APPLICABLES

Traités	Articles
Pacte international relatif aux droits civils et politiques	17. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. a) Toute personne a droit à la protection de la loi contre de telles ingérences ou atteintes. 19.2. Toute personne a droit à la liberté d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix. 19.3. L'exercice des droits prévus au paragraphe 2 du présent article comporte des devoirs et des responsabilités spéciaux. Il peut donc être soumis à certaines restrictions, mais celles-ci ne peuvent être que celles prévues par la loi et qui sont nécessaires : (a) au respect des droits ou de la réputation d'autrui ; (b) Fa la protection de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques. » 25. Tout citoyen a le droit et la possibilité, sans aucune des distinctions mentionnées à l'article 2 et sans restrictions déraisonnables : (a) De prendre part à la direction des affaires publiques, directement ou par l'intermédiaire de représentants librement choisis ; (b) De voter et d'être élu lors d'élections périodiques authentiques, au suffrage universel et égal, au scrutin secret, garantissant la libre expression de la volonté des électeurs ;
Charte africaine de la démocratie, des élections et de la bonne gouvernance	3. 1 Respect des droits de l'homme et des principes démocratiques 3.4. Tenue d'élections régulières, transparentes, libres et équitables ; 4.1 Les États parties s'engagent à promouvoir la démocratie, le principe de la primauté du droit et les droits de l'homme. 6.1 Les États parties veillent à ce que les citoyens jouissent des libertés fondamentales et des droits de l'homme, en tenant compte de leur universalité, de leur interdépendance et de leur indivisibilité.
Charte africaine des droits de l'homme et des peuples	9.1 Toute personne a le droit de recevoir des informations. 9.2. Toute personne a le droit d'exprimer et de diffuser ses opinions dans le respect de la loi. »
Convention africaine sur la protection des données personnelles et des données électroniques	8.1 Chaque État partie s'engage à établir un cadre juridique visant à renforcer les droits fondamentaux et les libertés publiques, en particulier la protection des données physiques, et à punir toute violation de la vie privée sans préjudice du principe de libre circulation des données à caractère personnel.

NORMES RÉGIONALES ET INTERNATIONALES APPLICABLES

Soft Law

[Commission africaine des droits de l'homme et des peuples Déclaration de principes sur la liberté d'expression et l'accès à l'information](#)

Principe 40(1)

Toute personne a droit à la vie privée, y compris à la confidentialité de ses communications et à la protection de ses informations personnelles.

[Résolution 573 de la CADHP sur le déploiement de la surveillance massive et illégale des communications ciblées et son impact sur les droits de l'homme en Afrique](#)

i. *Veiller à ce que toutes les restrictions aux droits à la vie privée et aux autres libertés fondamentales, telles que la liberté d'expression, la liberté d'association et la liberté de réunion, soient nécessaires et proportionnées, et conformes aux dispositions du droit international et aux normes internationales en matière de droits de l'homme ;*

ii. *Aligner les approches en matière de réglementation de la surveillance des communications sur le droit international et les normes internationales pertinents en matière de droits de l'homme, en tenant compte de garanties telles que l'obligation d'obtenir l'autorisation préalable d'une autorité judiciaire indépendante et impartiale et la nécessité d'un contrôle efficace et d'un examen régulier par des mécanismes de surveillance indépendants ;*

iii. *Ne recourir qu'à une surveillance ciblée des communications qui soit autorisée par la loi, conforme au droit international et aux normes internationales en matière de droits de l'homme, et fondée sur des soupçons raisonnables qu'un crime grave a été ou est en train d'être commis ;*

[ACHPR Résolution 580 de la CADHP sur les coupures d'Internet et les élections en Afrique](#)

Compte tenu de l'utilisation croissante de l'internet et des plateformes de médias sociaux pour la diffusion d'informations aux électeurs, aux observateurs électoraux, aux organes de gestion des élections et aux autres parties prenantes, en particulier pendant les élections ;

La Commission invite les États parties à :

(i) Veiller au respect de la Charte africaine, de la Charte africaine de la démocratie, des élections et de la bonne gouvernance et des instruments régionaux et internationaux pertinents relatifs aux droits de l'homme pendant le processus électoral ;

(ii) *Prendre les mesures législatives et autres nécessaires pour garantir un accès ouvert et sécurisé à Internet avant, pendant et après les élections, notamment en veillant à ce que les fournisseurs de services de télécommunications et d'Internet prennent les mesures adéquates pour fournir un accès sans restriction et ininterrompu ;*

(iii) *s'abstenir d'ordonner l'interruption des services de télécommunications, la fermeture de l'Internet et/ou la perturbation de l'accès à toute autre plateforme de communication numérique avant, pendant ou après les élections ;*

(iv) *Exiger des fournisseurs de services de télécommunications et d'Internet qu'ils informent les utilisateurs des perturbations potentielles et qu'ils fassent preuve de diligence raisonnable pour résoudre rapidement toute perturbation.*

NORMES RÉGIONALES ET INTERNATIONALES APPLICABLES

[Lignes directrices sur l'accès à l'information et les élections en Afrique](#)

3. Le principe est que toutes les informations détenues par les acteurs électoraux concernés doivent être divulguées dans leur intégralité. En conséquence, les acteurs électoraux concernés sont tenus de publier les informations clés d'intérêt public concernant leur structure, leurs fonctions, leurs pouvoirs, leurs processus décisionnels, leurs décisions, leurs recettes et leurs dépenses en rapport avec le processus électoral.

26. L'organisme chargé de réglementer les médias audiovisuels et tout autre organisme national de sécurité, public ou privé, impliqué dans la fourniture de services de télécommunications doit s'abstenir de fermer l'Internet ou tout autre type de média pendant le processus électoral.

27. Dans les cas exceptionnels où une coupure peut être autorisée en vertu du droit international, les raisons de cette coupure doivent être divulguées de manière proactive. Une telle restriction doit :

- (a) être autorisée par la loi ;
- (b) servir un objectif légitime ;
- (c) être nécessaire et proportionnée dans une société démocratique

28. Toute décision de l'organisme de régulation des médias ou de l'Internet est soumise à un contrôle judiciaire, qui doit être effectué dans les plus brefs délais.

[Résolution 620 de la CADHP sur la promotion et l'exploitation de l'accès aux données comme outil pour faire progresser les droits de l'homme et le développement durable à l'ère numérique](#)

1. Exhorte les États parties à :

- a) Veiller à ce que les pratiques en matière de collecte, de traitement, de stockage et d'accès aux données soient transparentes, responsables et conformes aux normes régionales et internationales à l'ère de la numérisation et de l'utilisation croissante de l'IA ;

SURVEILLANCE DES COUPURES D'INTERNET



Les coupures d'Internet sont courantes pendant les élections dans les pays où les gouvernements cherchent à entraver la libre circulation de l'information. Elles prennent diverses formes, mais constituent des perturbations intentionnelles de l'Internet ou des communications électroniques, les rendant inaccessibles ou inutilisables.⁴ Telles peuvent être mises en œuvre pour des populations spécifiques ou affecter des plateformes de médias sociaux spécifiques telles que X ou Telegram.⁵ Les coupures d'Internet sont également appelées « kill switch » (interrupteur d'arrêt) en raison de leur capacité inhérente à empêcher des communautés d'accéder à Internet, une pratique délibérée d'exclusion numérique.

1. Amnesty International Togo et Ors c. République togolaise (ECW/CCJ/JUD/09/20)

La Cour communautaire de justice de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) estime que la liberté d'expression est un droit dérivé et que le gouvernement togolais a violé le droit à la liberté d'expression des requérants en coupant l'accès à Internet en septembre 2017. La Cour rend une décision qui garantit la « non-occurrence » des coupures d'Internet et ordonne le versement d'une indemnité d'un montant de 2 000 000 CFA (environ 3 500 USD).

2. Coupure d'Internet en [Guinée-Conakry](#)

Dans une affaire similaire à celle d'Amnesty c. Togo mentionnée ci-dessus, la Cour de la CEDEAO, à la suite d'une [affaire](#) dans laquelle le gouvernement de la Guinée-Conakry avait coupé l'accès à Internet en mars et octobre 2020, a estimé que cette mesure violait la liberté d'expression et l'accès à l'information, et que la liberté d'expression était un droit dérivé.

Étapes de surveillance

Pour savoir s'il y a une coupure totale d'Internet, vous pouvez vous fier aux outils développés par les organisations de la communauté de mesure, tels que NetBlocks⁶ et Ooni.⁷

Indicateurs de coupures d'Internet

- Impossibilité d'accéder aux principaux sites web
- Ralentissement de la connectivité lors d'événements majeurs tels que les rassemblements politiques, les manifestations électorales, les jours d'élection et les dates d'annonce des résultats électoraux.

4 <https://www.accessnow.org/issue/internet-shutdowns/>

5 <https://www.mediadefence.org/>

6 <https://netblocks.org/>

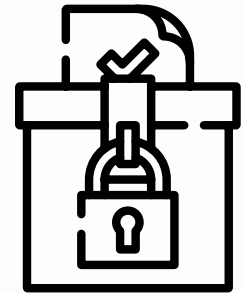
7 <https://ooni.org/install/>

Comment rester connecté pendant les élections ?

- Utilisation de réseaux privés virtuels (VPN), voir [Ayeta](#)⁸ pour obtenir des conseils.
- Installez OONI Probe au moins 6 mois avant les élections afin de permettre la collecte de données pour recueillir des preuves de la censure d'Internet, car cet outil montre comment, quand et où elle est mise en œuvre. Vous trouverez des informations sur les tendances en matière de censure d'Internet sur OONI's Detection Analysis (IODA), qui surveille Internet et détecte les coupures de connexion en temps réel sur un tableau de bord interactif, permettant aux utilisateurs de suivre les coupures d'Internet à l'échelle mondiale.

- Y a-t-il un ralentissement de l'accès à Internet ou une coupure totale ?
- Quand cela a-t-il commencé et quand cela s'est-il terminé ? (Si cela est toujours en cours, vous pouvez indiquer que cela est toujours en attente. Signalez également cet incident sur Ripoti.)
- Si oui, quels sites web sont concernés ? (Tous les sites web ou certaines plateformes spécifiques comme X ou Facebook ?)
- Le gouvernement a-t-il communiqué ou ordonné un blocage de l'accès à Internet ?
- Si oui, pouvez-vous partager un lien vers la communication/l'ordre ?
- Quelle agence gouvernementale l'a ordonné ?
- Sur quelle loi s'est-elle appuyée ?
- Les fournisseurs d'accès à Internet (FAI) ont-ils communiqué leur intention de bloquer l'accès à Internet ?
- Si oui, pouvez-vous fournir des liens à ce sujet ?

PROTECTION DES DONNÉES ET ÉLECTIONS



Privacy International a publié une [liste de contrôle sur les données et les élections](#)⁹ qui souligne l'importance du droit à la vie privée, y compris la protection des données personnelles pendant les élections. La plupart des constitutions nationales protègent le droit à la vie privée et la majorité des États ont adopté une législation sur la protection des données. Cependant, dans des pays comme le Kenya¹⁰ et le Zimbabwe,¹¹ des violations de la vie privée ont été constatées, les partis politiques accédant aux numéros de téléphone des électeurs et leur envoyant des SMS pour solliciter des votes ou leur demander d'assister à des rassemblements politiques. Cette pratique est contraire à la plupart des lois sur la protection des données en vigueur dans les pays où elles existent.

Quelques questions à se poser:

- Les citoyens reçoivent-ils des messages politiques non sollicités par SMS ou d'autres technologies de communication ?
- À partir de quels réseaux ces messages sont-ils envoyés ?
- Y a-t-il eu des violations des données relatives aux listes électorales ou d'autres données personnelles lors d'élections en ligne ?

Technologies biométriques

La biométrie consiste à mesurer et à analyser des caractéristiques physiques ou comportementales uniques, notamment pour vérifier et identifier un individu. Les caractéristiques biométriques pouvant être mesurées sont nombreuses : empreintes digitales, empreintes palmaires, scans de la rétine et de l'iris, empreintes vocales et profils ADN.¹² Les caractéristiques biométriques les plus couramment utilisées à des fins électorales sont les empreintes digitales pour les systèmes d'identification automatique des empreintes digitales (AFIS), les images faciales des électeurs pour les systèmes de reconnaissance faciale (FRS) et, parfois, les signatures numérisées. Les données biométriques sont un type de données personnelles particulièrement sensibles, car elles révèlent les caractéristiques et l'identité d'une personne et, à ce titre, elles peuvent faire l'objet d'abus graves. Une réglementation est nécessaire concernant les fins auxquelles les données biométriques peuvent être utilisées et les personnes auxquelles ces données peuvent être divulguées. Les citoyens dont les données sont collectées devraient pouvoir obtenir des informations sur la manière dont ces données seront utilisées et avoir la possibilité d'accéder à leurs données et de corriger toute inexactitude.

9 https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Fi-nal_21Nov_Reduced.pdf

10 <https://privacyinternational.org/sites/default/files/2018-06/Biometric%20Technology-Elections-Privacy.pdf>

11 <https://www.techzim.co.zw/2018/07/econet-denies-selling-customers-data-to-3rd-parties-refutes-zecs-allegations-so-who-sold-data-to-zanu-pf/>

12 <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

Des pays comme [Kenya](#) utilisent plusieurs technologies dans le processus électoral, notamment des systèmes d'enregistrement biométrique des électeurs (BVR), ce qui soulève des préoccupations en matière de protection des données pour le droit à la vie privée. Au Malawi, la Commission électorale du Malawi [a acheté](#) à Smartmatic de nouvelles technologies destinées à être utilisées lors des élections de 2025, ce qui a suscité des inquiétudes quant à l'intégrité des systèmes de gestion des élections. Au ¹³ [Nigeria](#), l'absence de communication des résultats électoraux a donné lieu à des manifestations lors des élections de 2023. Le portail de consultation des résultats de la Commission électorale nationale indépendante (INEC) (IREV) n'a pas réussi à télécharger rapidement les résultats de l'élection présidentielle du 25 février 2023, malgré le bon fonctionnement du système bimodal d'accréditation des électeurs (BVAS), ce qui a suscité des inquiétudes quant à l'existence de biais et de manipulations. Outre les préoccupations liées à la protection des données, la désinformation et la mésinformation prospèrent lorsqu'il n'y a pas d'informations adéquates sur l'utilisation des technologies biométriques pendant les élections. Voir ci-dessous un extrait concernant le [Zimbabwe](#).

« Heal Zimbabwe, par l'intermédiaire de ses observateurs des droits de l'homme (HRM) formés, a surveillé l'environnement électoral avant l'opération d'inscription des électeurs et a constaté une augmentation des cas de violations des droits de l'homme, certains militants politiques trop zélés affirmant que le système BVR permet aux partis politiques de voir comment les électeurs votent. »

Extrait d'un rapport de surveillance de Heal Zimbabwe sur l'enregistrement biométrique des électeurs (BVR) lors des élections au Zimbabwe.¹⁴

L'utilisation de la biométrie pour l'inscription et l'identification des électeurs ne supprime pas la nécessité de mesures de transparence liées à l'inscription des électeurs. Il est nécessaire de sensibiliser en permanence les parties prenantes afin de renforcer leur confiance dans la biométrie et d'éviter les perceptions erronées. Des informations sur les systèmes utilisés doivent être fournies tout au long de la période et du cycle électoraux. Lorsque les technologies biométriques sont adoptées en l'absence d'une loi solide sur la protection des données, le droit à la vie privée et à la sécurité personnelle est menacé.¹⁵

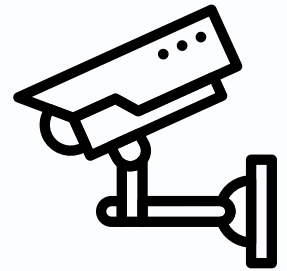
Quelques questions à poser en tant qu'observateur électoral

- Existe-t-il dans votre pays une loi sur la protection des données qui traite de l'utilisation des technologies biométriques pendant les élections ?
- L'organe de gestion des élections communique-t-il suffisamment d'informations sur l'utilisation des technologies biométriques afin d'éviter la désinformation et les fausses informations ?
- Y a-t-il des informations erronées ou de la désinformation concernant l'utilisation des technologies biométriques ?
- Existe-t-il des liens vers les rapports ?

¹³ <https://www.investigativeplatform-mw.org/show-story/mecs-controversial-it-partner>

¹⁴ <https://kubatana.net/2017/09/08/voter-educators-diffuse-myths-suspicious-biometric-voter-registration/>

¹⁵ <https://privacyinternational.org/report/2066/investigating-privacy-implications-biometric-voter-registration-kenyas-2017-election>



SURVEILLANCE

La surveillance pendant les élections désigne le contrôle secret des communications, des activités, des déplacements et des données personnelles des citoyens. Elle est effectuée sans consentement et vise généralement les journalistes, les militants, les candidats de l'opposition et parfois les électeurs. L'ingérence dans le droit à la vie privée est réglementée par la loi, qui doit être accessible au public, claire, précise, exhaustive et non discriminatoire, et cette ingérence ne doit pas être arbitraire ou illégale, en tenant compte de ce qui est raisonnable pour la poursuite d'objectifs légitimes ¹⁶. La surveillance peut prendre différentes formes, telles que :

- Le piratage de téléphones ou de courriels pour espionner des conversations privées.
- Suivre l'activité sur les réseaux sociaux pour surveiller les détracteurs ou les opposants.
- La surveillance des espaces publics et des rassemblements à l'aide de technologies de reconnaissance faciale et d'autres technologies telles que les logiciels espions.

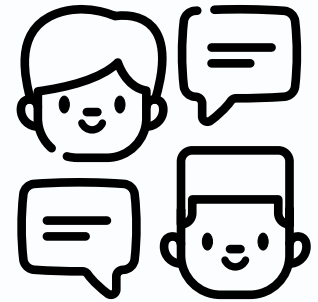
- A-t-on fait mention d'une surveillance ciblée des communications de masse pendant les élections ?
- Y a-t-il eu une surveillance ciblée sur des individus ou des groupes spécifiques ?
- Si oui, où cela a-t-il été communiqué ?
- Quels sont les organismes gouvernementaux responsables de cette surveillance ?
- Y a-t-il eu acquisition ou déploiement d'outils de surveillance ?
- Des outils de surveillance des espaces publics ont-ils été déployés pendant cette période ?
- Y a-t-il eu des saisies arbitraires de technologies numériques appartenant à des électeurs, des journalistes, des défenseurs des droits humains, des observateurs/moniteurs électoraux, des organisations de la société civile, etc. ?
- Des liens ?

¹⁶ Check PI's Guide to International Law and Surveillance here <https://privacyinternational.org/sites/default/files/2024-09/2024%20GILS%20version%204.0.pdf>

Pourquoi est-ce un problème lors des élections ?

- **Réduit les voix au silence** : les gens peuvent avoir peur de s'exprimer ou de participer s'ils se sentent surveillés.
- **Violates the right to privacy** : Surveillance
- **Violation du droit à la vie privée** : la surveillance peut exposer des données privées, des plans de campagne ou les choix des électeurs.
- **C'est de l'intimidation** : les informations issues de la surveillance peuvent être utilisées pour menacer ou discréditer les opposants et rendre les élections injustes.
- **C'est un abus de pouvoir de la part des partis au pouvoir** : elle permet à ceux qui détiennent le pouvoir d'en abuser et de cibler l'opposition.

LIBERTÉ D'EXPRESSION



La liberté d'expression est considérée comme fondamentale pendant les élections. Tout moyen visant à restreindre cette liberté ne doit pas porter atteinte de manière injustifiée au droit des individus de participer au débat politique et de partager leurs opinions en ligne.

L'article 21 de la Déclaration universelle des droits de l'homme et l'article 25 du Pacte garantissent le droit de participer aux affaires publiques. Le Comité des droits de l'homme a affirmé que, pour garantir la pleine jouissance des droits protégés par l'article 25, « la libre communication d'informations et d'idées sur les questions publiques et politiques entre les citoyens, les candidats et les représentants élus est essentielle. Cela implique une presse libre et d'autres médias capables de commenter les questions publiques sans censure ni restriction et d'informer l'opinion publique. [Assemblée générale des Nations unies A/77/287](#) (paragraphe 19)

La Déclaration de la CADHP¹⁷ définit, dans son principe 23.1, les discours interdits comme tout discours qui prône la haine nationale, raciale, religieuse ou toute autre forme de haine discriminatoire constituant une incitation à la discrimination, à l'hostilité ou à la violence. Le principe 23.3 stipule que les États ne doivent pas interdire les discours qui manquent simplement de civilité ou qui offensent ou dérangent. Le discours politique ne doit pas être criminalisé.

Que faut-il surveiller ?

- Y a-t-il des arrestations d'individus pour des discours politiques en ligne ?
- Qui est spécifiquement visé/affecté ?
- Les accusations portées contre elles ont-elles été rendues publiques ?
- Les arrestations sont-elles fondées sur une loi du pays (lois sur les insultes, les fausses nouvelles, l'incitation à la violence publique, la diffamation criminelle, etc.) ?
- Quelle loi et quelle disposition permettent l'arrestation, si elles sont connues ?

Suivi des informations erronées et de la désinformation

Troubles de l'information

Voici les formes courantes de troubles de l'information pendant les élections :

1. La désinformation consiste à partager des informations fausses, mais sans intention de nuire.¹⁸
2. La désinformation désigne le partage délibéré d'informations fausses dans l'intention de nuire.¹⁹
3. La malinformation désigne le partage d'informations authentiques dans l'intention de nuire, souvent en divulguant des informations relevant de la sphère privée dans la sphère publique.²⁰

À surveiller :

- *La diffusion d'informations fausses ou trompeuses visant des candidats, des institutions ou des électeurs.*
- *L'utilisation des réseaux sociaux, des robots ou des réseaux pour amplifier les discours.*
- *Présence (ou absence) de mécanismes de vérification des faits.*

Si la diffusion de désinformation pendant ces périodes peut exacerber les effets négatifs sur les droits humains, les coupures d'Internet ont des répercussions importantes sur toute une série de droits et peuvent même contribuer à des violations et à des abus des droits humains, notamment en limitant leur visibilité. Compte tenu de leur portée indiscriminée et de leurs répercussions négatives importantes, les coupures d'Internet répondent très rarement aux exigences de nécessité et de proportionnalité en matière de droits humains. [Assemblée générale des Nations unies A/77/287](#) ((paragraphe 45(e))²¹

De nombreux pays africains traitent la désinformation lors des élections en termes vagues et généraux, ce qui conduit à des violations des droits humains. Voici quelques-unes des approches adoptées par certains États :

- Définitions vagues des fausses informations dans les codes ou lois pénaux.
- Coupures d'Internet
- Déploiement d'une surveillance ciblée des communications de masse à l'aide de la technologie

À l'ère numérique, les technologies telles que l'intelligence artificielle (IA) et d'autres technologies émergentes peuvent être utilisées à des fins bonnes ou mauvaises lors des élections. L'essor des deepfakes, par exemple, est problématique car il induit les électeurs en erreur. Ces contenus ont pour effet de tromper les électeurs, et les observateurs électoraux devraient être en mesure de surveiller les plateformes de réseaux sociaux telles que Facebook, X et WhatsApp afin d'évaluer les éléments suivants :

¹⁸ <https://firstdraftnews.org/long-form-article/understanding-information-disorder/>

¹⁹ Abid

²⁰

²¹ UN General Assembly <https://documents.un.org/doc/undoc/gen/n22/459/24/pdf/n2245924.pdf>

- Y a-t-il eu utilisation de deepfakes à caractère politique et de contenus trompeurs générés par l'IA en ligne avant, pendant et après les élections ?
- Qui a généré les deepfakes ou autres contenus faux générés par l'IA ?
- Les plateformes de réseaux sociaux ont-elles signalé ces contenus comme étant faux ou générés par l'IA ?
- Le retrait de contenus par les plateformes de réseaux sociaux (SMP) a-t-il été signalé comme une violation des normes communautaires des SMP ?
- Y a-t-il des liens vers ces contenus ?

Divulgations proactives

Pour lutter contre la désinformation et la désinformation et remédier à leur impact, les divulgations proactives constituent une stratégie essentielle que les États devraient utiliser pendant les élections. Lorsque toutes les parties prenantes aux élections divulguent de manière proactive des informations, cela jette les bases d'un processus démocratique et réduit l'incidence des troubles liés à l'information. Cette démarche doit s'accompagner d'une sensibilisation des électeurs et de la promotion des pratiques de vérification des faits. Les autorités chargées de nommer les membres des OGE, les OGE, les partis politiques, les candidats, les forces de l'ordre, les observateurs électoraux, les médias et les plateformes de médias sociaux ont un rôle à jouer dans la divulgation proactive d'informations. Ils peuvent tirer parti de la technologie pour garantir un flux constant et libre d'informations vers l'électorat. Le fait de ne pas divulguer les informations de manière proactive nuit à la réputation d'une élection et conduit à une conclusion d'injustice.

Paragraphe 27.

*Dans sa résolution 76/227, l'Assemblée générale a souligné la nécessité de « diffuser des informations factuelles, opportunes, claires, accessibles, multilingues et fondées sur des preuves » et a insisté sur « la nécessité pour toutes les parties prenantes concernées de relever le défi de la désinformation ». Maximiser la transparence et l'accès à l'information est une condition essentielle pour instaurer la confiance dans les institutions publiques, la gouvernance et les processus. Lorsque les gouvernements, les responsables politiques et les fonctionnaires agissent de manière transparente, communiquent régulièrement avec les citoyens qu'ils servent, fournissent des informations opportunes et fondées sur des preuves et se soumettent à un contrôle, ils contribuent à la mise en place d'institutions légitimes, responsables et efficaces, qui peuvent renforcer la confiance du public dans le système d'information et réduire la vulnérabilité des personnes et des communautés à la désinformation.*²² [UN General Assembly A/77/287](#)

Les [lignes directrices](#)²³ invitent les organismes chargés de la gestion des élections (OGE) à divulguer de manière proactive des informations à toutes les étapes du processus électoral, en précisant certaines catégories d'informations qui doivent être divulguées avant, pendant et après les élections. Pour suivre les divulgations proactives d'informations, veuillez consulter ci-dessous les éléments à surveiller de la part des OGE :

- Quand l'EMB a-t-il annoncé la date des élections ?
- Quelles plateformes l'EMB a-t-il utilisées pour divulguer ces informations ?
- Quelles plateformes ont été principalement utilisées pour les divulgations liées aux élections ?
- Quelles informations ont été divulguées explicitement et en temps utile ?
- À quelle fréquence l'OGE a-t-il divulgué des informations ?
- Dans quelle mesure les informations divulguées étaient-elles précises (clarté des informations divulguées/absence d'imprécision) ?

L'opacité du processus et l'absence de diligence raisonnable et de contrôle indépendant ont été particulièrement préoccupantes. Pour suivre les divulgations proactives d'informations, veuillez consulter ci-dessous les éléments à surveiller de la part des agences gouvernementales :

- Le gouvernement utilise-t-il la technologie dans le cadre des élections ?
- Quelle technologie est utilisée ou déployée ?
- À quelles fins la technologie est-elle déployée dans le cadre de l'élection ?
- Y a-t-il une divulgation proactive des informations relatives à l'acquisition de la technologie utilisée ?
- Une entreprise privée est-elle impliquée dans le processus ?
- Sur la technologie de quelle entreprise privée s'appuie l'administration électorale ? (par exemple, kits d'enregistrement/de vérification biométriques)
- Les informations relatives au processus d'acquisition et à la technologie utilisée sont-elles suffisamment rendues publiques pour permettre au public et aux autorités de contrôle d'examiner le processus et la technologie ?
- À quelles données personnelles l'entreprise privée fournissant la technologie a-t-elle accès ?
- Quelle justification est fournie pour le traitement de ces données ?
- Quelles garanties ou limites, le cas échéant, sont imposées au fournisseur de technologie privé pour le traitement des données ?
- Existe-t-il des conditions claires précisant qui conserve la propriété de l'ensemble de données produit/maintenu par une entreprise privée ?

Mécanismes de responsabilité

Outre la surveillance des droits numériques pendant les élections, il est essentiel d'identifier les mécanismes de signalement à des fins de responsabilité. Voici quelques moyens de garantir que les violations des droits numériques soient traitées en temps réel.

- Signalez les violations à l'institution nationale des droits de l'homme de votre pays. rights institution in your country.
- Signalez-les à des organisations de défense des droits humains réputées qui peuvent répondre à vos préoccupations par des actions de sensibilisation et des poursuites judiciaires.
- Soumettez des rapports pour une action immédiate à Paradigm Initiative via la plateforme de signalement- [Ripoti](#).
- Soumettez un rapport de surveillance à Paradigm Initiative et à tout partenaire collaborateur au format Annexe A su partners@paradigmhq.org .

RESOURCES

1. [Déclaration de principes de la CADHP sur la liberté d'expression et l'accès à l'information en Afrique](#)
2. [GUIDE DE PI SUR LE DROIT INTERNATIONAL ET LA SURVEILLANCE](#)
3. [Résolution 580 de la CADHP sur les coupures d'Internet et les élections en Afrique](#)
4. **Charte africaine de la démocratie, des élections et de la bonne gouvernance**
https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf
5. **Netblocks**
<https://netblocks.org/> et suivez-nous sur https://x.com/netblocks?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor .
6. [Boîte à outils Ayeta sur les droits numériques](#)
Boîte à outils Paradigm Initiative sur la sécurité numérique – Ayeta présente les droits numériques et les solutions de sécurité numérique
7. Signalez toutes les violations des droits numériques sur [Ripoti](#).
8. Si vous avez besoin d'un VPN, envoyez une demande à vpn@paradigmhq.org.
9. Open Observatory of Network Interference ([OONI](#)) Probe —Testez le blocage des sites web et des applications et mesurez la vitesse et les performances de votre réseau à l'aide d'OONI.
10. **Liste de contrôle de Privacy International sur les données et les élections**
https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Final_21Nov_Reduced.pdf

ANNEXE 1 : FORMULAIRE DE SURVEILLANCE

Nom :

Organisation/affiliation:.....

Rôle/secteur (journaliste/OSC/chercheur, etc.).....

Période couverte par le rapport (par exemple, juin 2025 ou juin-juillet 2025) :

NB : Vous pouvez répondre de l'une des manières suivantes :

- ☐ Oui - Fournissez des détails sur votre réponse, y compris des liens, si possible.
- ☐ Non - Fournissez des détails lorsque cela est pertinent pour plus de clarté.
- ☐ Aucune information disponible — Lorsqu'il n'y a aucun moyen de vérifier ce qui est demandé, vous pouvez répondre de cette manière et fournir des détails pour plus de clarté.

Coupures d'Internet

- Y a-t-il un ralentissement de l'accès à Internet ou une coupure totale ?
- Quand cela a-t-il commencé et quand cela s'est-il terminé ? (Si cela est toujours en cours, vous pouvez indiquer que cela est toujours en attente. Signalez également cet événement sur Ripoti.)
- Si oui, quels sites web sont concernés ? (Tous les sites web ou des plateformes spécifiques comme X ou Facebook ?)
- Le gouvernement a-t-il communiqué ou ordonné un blocage de l'accès à Internet ?
- Si oui, pouvez-vous partager un lien vers cette communication/ce ordre ?
- Quelle agence gouvernementale l'a ordonné ?
- Sur quelle loi s'est-elle appuyée ?
- Les fournisseurs d'accès à Internet (FAI) ont-ils communiqué leur intention de bloquer l'accès à Internet ?
- Si oui, pouvez-vous fournir des liens à ce sujet ?

Protection des données

- Y a-t-il des signalements d'utilisation abusive ou d'accès non autorisé ?
- Les citoyens reçoivent-ils des messages politiques non sollicités par SMS ou d'autres technologies de communication ?
- À partir de quels réseaux ces messages sont-ils envoyés ?
- Y a-t-il eu des violations de données concernant les listes électorales ou d'autres données personnelles liées aux élections en ligne ?
- Existe-t-il dans votre pays une loi sur la protection des données qui régit l'utilisation des données personnelles et des technologies biométriques pendant les élections ?
- L'organisme chargé de la gestion des élections partage-t-il des informations adéquates sur l'utilisation des données et des technologies biométriques afin de prévenir la désinformation et la mésinformation ?
- Y a-t-il des informations erronées ou de la désinformation concernant l'utilisation des technologies biométriques ?
- Existe-t-il des liens vers les rapports ?

Piratage, surveillance et harcèlement en ligne

- Existe-t-il des rapports faisant état de piratage ou de surveillance à l'encontre de journalistes, de militants et de membres de l'opposition ?
- Rapports sur le déploiement de logiciels espions ou de technologies de suivi.
- Existe-t-il des rapports sur des cas de harcèlement ou d'intimidation coordonnés en ligne ?
- Y a-t-il eu mention d'une surveillance ciblée des communications de masse pendant les élections ?
- Y a-t-il eu une surveillance ciblée sur des individus ou des groupes spécifiques ?
- Si oui, où cela a-t-il été communiqué ?
- Quels sont les organismes gouvernementaux responsables de cette surveillance ?
- Y a-t-il eu des achats ou des déploiements d'outils de surveillance ?
- Des outils de surveillance des espaces publics ont-ils été déployés pendant cette période ?
- Quels outils ont été déployés, le cas échéant ?
- Y a-t-il eu des saisies arbitraires de technologies numériques appartenant à des électeurs, des journalistes, des défenseurs des droits humains, des observateurs/moniteurs électoraux, des organisations de la société civile, etc. ?
- Y a-t-il des liens ?

Rapport sur la liberté d'expression

- Y a-t-il eu des arrestations d'individus pour des discours politiques en ligne ?
- Qui est spécifiquement visé/concerné ?
- Les accusations portées contre ces personnes ont-elles été rendues publiques ?
- Les arrestations sont-elles fondées sur une loi du pays (lois sur les insultes, les fausses nouvelles, l'incitation à la violence publique, la diffamation criminelle, etc.) ?
- Quelle loi et quelle disposition permettent l'arrestation, si elles sont connues ?

Intégrité de l'information

- Y a-t-il eu utilisation de deepfakes à caractère politique et de contenus trompeurs générés par l'IA en ligne avant, pendant et après les élections ?
- Qui a généré les deepfakes ou autres contenus faux générés par l'IA ?
- Les plateformes de réseaux sociaux ont-elles signalé ces contenus comme étant faux ou générés par l'IA ?
- Le retrait de contenus par les plateformes de réseaux sociaux (SMP) a-t-il été signalé comme une violation des normes communautaires des SMP ?
- Y a-t-il des liens vers ces contenus ?

Rapport sur la divulgation proactive des technologies utilisées lors des élections

- Quand l'organe de gestion des élections a-t-il annoncé la date des élections ?
- Quelles plateformes l'organisme de gestion des élections a-t-il utilisées pour effectuer la divulgation ?
- Quelles plateformes ont été principalement utilisées pour les divulgations liées aux élections ?
- Quelles informations ont été spécifiquement divulguées et l'ont-elles été en temps opportun ?
- À quelle fréquence l'organisme de gestion des élections a-t-il divulgué des informations ?
- Dans quelle mesure les informations divulguées étaient-elles précises (clarté des informations/absence d'ambiguïté) ?

Technologie de suivi et élections

- Le gouvernement utilise-t-il la technologie dans le cadre des élections ?
- Quelle technologie est utilisée ou déployée ?
- À quelles fins cette technologie est-elle déployée lors des élections ?
- Y a-t-il une divulgation proactive des informations relatives à l'acquisition de la technologie utilisée ?
- Le gouvernement a-t-il divulgué de manière proactive aux principaux acteurs électoraux et aux électeurs les informations relatives à l'acquisition et à l'utilisation de cette technologie ?

ANNEXE B : SÉCURITÉ DES OBSERVATEURS ET DES SURVEILLANTS ÉLECTORAUX

	Avant les élections	Pendant les élections	Après les élections
Conseils de sécurité	Maintenez vos appareils à jour. Installez un logiciel antivirus et assurez-vous que les pare-feu sont activés. Utilisez des mots de passe forts et activez l'authentification à deux facteurs (2FA) pour vos comptes sur les plateformes numériques. Pour sécuriser vos communications, utilisez des applications de messagerie cryptées de bout en bout telles que Signal pour les communications sensibles. Utilisez des phrases de passe plutôt que des mots de passe. Activez le chiffrement au repos/le chiffrement complet du disque sur tous vos appareils. Ne cliquez pas sur des liens suspects. Vérifiez bien qui vous a envoyé des e-mails et des fichiers.	Évitez d'utiliser le Wi-Fi public. Utilisez les données mobiles ou un réseau privé virtuel (VPN) fiable. Pour protéger vos données, sauvegardez régulièrement vos documents (photos, rapports) sur un espace de stockage cloud sécurisé ou des disques cryptés. Désactivez le partage de position en direct sur les applications et évitez de publier votre position en temps réel.	Chiffrez et stockez en toute sécurité toutes les données collectées. Ne les conservez pas sur des appareils partagés ou publics. Utilisez des plateformes sécurisées pour les réunions de compte rendu et de débriefing. Modifiez les mots de passe de tous les comptes ou appareils utilisés pendant les élections.
Conseils pour la sécurité physique	Évaluation des risques : identifiez les zones à haut risque et planifiez les itinéraires des observateurs en conséquence. Il est essentiel de disposer d'une carte d'identité officielle d'observateur valide et accessible. Enregistrez le numéro d'urgence sur votre appareil et dans un carnet. Communiquez votre emplacement et votre emploi du temps à des contacts de confiance. N'utilisez pas la biométrie pour déverrouiller des appareils qui sont par ailleurs sécurisés, car celle-ci peut être très facilement contournée (déverrouillage par reconnaissance faciale/empreinte digitale)	Évitez d'utiliser le Wi-Fi public. Utilisez les données mobiles ou un réseau privé virtuel (VPN) fiable. Pour protéger vos données, sauvegardez régulièrement vos documents (photos, rapports) sur un espace de stockage cloud sécurisé ou des disques cryptés. Désactivez le partage de position en direct sur les applications et évitez de publier votre position en temps réel.	Chiffrez et stockez en toute sécurité toutes les données collectées. Ne les conservez pas sur des appareils partagés ou publics. Utilisez des plateformes sécurisées pour les réunions de compte rendu et de débriefing. Modifiez les mots de passe de tous les comptes ou appareils utilisés pendant les élections.

CONSEILS SUPPLÉMENTAIRES POUR LA SÉCURITÉ NUMÉRIQUE

Google Authenticator (vous pouvez utiliser cet outil pour générer des codes d'authentification à deux facteurs (2FA) pour sécuriser vos connexions)

Mode d'emploi :

- Sur votre appareil mobile, installez Google Authenticator depuis le Google Play Store ou l'App Store. Cliquez sur ce lien pour en savoir plus sur Google Authenticator et son installation [Android](#) et [iPhone / iPad](#)
- Ouvrez l'application et scannez les codes QR 2FA de vos comptes en ligne.
- Utilisez les codes générés pour vous connecter.

Signal (pour une communication plus sécurisée, vous pouvez utiliser cette plateforme pour envoyer des messages cryptés et passer des appels vocaux et vidéo)

Mode d'emploi:

1. Rendez-vous sur signal.org et téléchargez l'application pour votre appareil (Android, iOS ou ordinateur de bureau).
2. Installez l'application et vérifiez votre numéro de téléphone.
3. Définissez un code PIN et commencez à envoyer des messages en toute sécurité.

Navigateur Tor (pour la confidentialité, l'anonymat et une navigation sécurisée)

Mode d'emploi :

- Téléchargez-le sur torproject.org.
- Installez et ouvrez le navigateur.
- Naviguez en toute sécurité sans révéler votre identité ni votre emplacement.

ProtonMail (Envoie des e-mails sécurisés et cryptés de bout en bout)

Mode d'emploi :

- Rendez-vous sur proton.me.
- Créez un compte de messagerie crypté gratuit.
- Utilisez l'application web ou mobile pour envoyer des e-mails protégés.

Proton Drive (Stockage cloud crypté de bout en bout proposé par les créateurs de ProtonMail)

- Rendez-vous sur proton.me/drive.
- Créez un compte Proton gratuit (ou connectez-vous si vous en avez déjà un).
- Utilisez l'interface web ou installez l'application pour télécharger vos fichiers.
- Les fichiers sont automatiquement cryptés. Vous pouvez les organiser dans des dossiers et les partager en toute sécurité.
- Activez l'authentification à deux facteurs dans les paramètres de votre compte Proton pour une protection supplémentaire.

VeraCrypt (Il crée des volumes cryptés sur votre ordinateur ou votre clé USB.)

Mode d'emploi :

- Téléchargez VeraCrypt depuis veracrypt.fr
- Installez et ouvrez l'application
- Cliquez sur « Créer un volume », suivez l'assistant et choisissez un mot de passe fort.

Have I Been Pwned (vérifie si votre adresse e-mail ou votre numéro de téléphone ont été exposés à des violations de données)

Mode d'emploi :

- Rendez-vous sur haveibeenpwned.com.
- Saisissez votre adresse e-mail ou votre numéro de téléphone.
- Recevez les résultats et modifiez vos mots de passe si nécessaire.

Utilisez un gestionnaire de mots de passe pour générer, stocker et saisir des mots de passe sécurisés pour vos services. Vous pouvez également stocker votre TOTP/deuxième facteur dans l'entrée correspondante. Proton en propose un, ou KeePassXC pour une utilisation hors ligne.

