KONRAD ADENAUER STIFTUNG

ANATOMIE DES TROUBLES DE L'INFORMATION EN AFRIQUE

Positionnement géostratégique et concurrence multipolaire à l'égard des technologies convergentes

Par Eleonore Pauwels

JUILLET 2020

ISBN: 978-3-95721-706-6

Table des matières

L’auteure

Eleonore Pauwels est experte internationale sur les implications sécuritaires, sociétales et de gouvernance suscitées par la convergence de l’intelligence artificielle et d’autres technologies à double usage, notamment la cybersécurité, la génomique et l’édition de génome.

Elle met son expertise au service de la Banque mondiale, de l’ONU et du Global Center on Cooperative Security à New York. Elle travaille aussi étroitement avec les gouvernements et avec les acteurs du secteur privé sur la scène de la prévention cyber-IA, de la nature changeante du conflit, de la prospective et de la sécurité mondiale. En 2018 et 2019, Eleanore Pauwels était chargée de recherche sur les cybertechnologies émergentes au Centre for Policy Research de l’Université des Nations Unies. Au Woodrow Wilson International Center for Scholars, elle a dirigé pendant 10 ans l’Anticipatory Intelligence Lab, au sein du programme Science and Technology Innovation.

Elle est aussi membre du Scientific Committee of the International Association for Responsible Research and Innovation in Genome-Editing (ARRIGE). Eleanore Pauwels a travaillé dans le passé à la direction « Science, économie et société » de la Commission européenne.

Elle témoigne régulièrement lors d’audiences en présence d’autorités américaines et européennes américaines et européennes, dont le Département d’État américain et les NAS, NIH, NCI, FDA et National Intelligence Council aux États-Unis, la Commission européenne et l’ONU. Ses écrits sont publiés dans Nature, The New York Times, The Guardian, Scientific American, Le Monde, Slate, UN News, The UN Chronicle et The World Economic Forum.

Avant-propos

Les élections sont une pierre angulaire de la démocratie. Faut-il cependant rappeler le sophisme de l'électoralisme[1] et la tentation de maints acteurs extérieurs de déclarer « démocratique » un système politique du simple fait d'exercices électoraux réguliers ? Souvent, la qualité des élections en soi est négligée, ou les écueils du processus électoral sont identifiés mais ils subsistent sans conséquences. À l'aune des normes internationales largement reconnues, les élections démocratiques doivent être libres, ce qui signifie que les droits des citoyens à participer et à concourir doivent être respectés et protégés en vertu de l'État de droit. Les élections démocratiques doivent aussi être justes, soumises à des règles équitables. Mais quel sens reste-t-il à ces normes minimales à l'ère de l'intelligence artificielle, de nouvelles technologies et de ce qu'Eléonore Pauwels, l'auteure de cette étude, qualifie de « troubles de l'information » ?

Pour une fondation politique telle que l'organisation Konrad-Adenauer-Stiftung, dont la mission embrasse le soutien des processus de démocratisation partout dans le monde, l'impact des nouvelles technologies sur les processus électoraux et l'état de nos démocraties revêt le plus grand intérêt.

Les démocraties consolidées aussi bien que celles émergentes sont concernées. Les menaces sont multiples et s'étendent bien au-delà de l'érosion des institutions. En particulier, elles affectent et changent radicalement la trame sociale et la culture politique de nos sociétés. La transformation n'est certes pas totalement dénuée d'avantages, pourvu que les effets négatifs et collatéraux en soient maîtrisés — et la tâche n'a jamais été aussi complexe.

Du côté de la défense de la démocratie, deux fronts se dessinent :

Il y a d'une part l'espace politique, où les candidats et les partis font campagne, cherchant à s'assurer le soutien populaire, et où la diffamation en ligne, le discours de la haine, les fuites de données, la désinformation et l'hypertrucage « deepfake » altèrent les règles du jeu. C'est ce niveau, la capture du cœur et de l'âme des citoyens, que l'étude présentée ici, « Anatomie des troubles de l'information en Afrique », dissèque et illustre,exemples du continent africain à l'appui.

Mais il y a aussi l'espace technique, où les organes de gestion des élections en particulier sont les institutions les plus vulnérables. Il s'agit d'une sphère où la manipulation des données par des acteurs locaux et étrangers peut perturber un processus électoral, et où les partis politiques concurrents doivent disposer d'une expertise suffisante pour comprendre les technologies employées et prévenir la fraude électorale.

Pour mieux cerner la vulnérabilité du cycle électoral à la menace de la technologie moderne, KAS New York s'est lancée avec l'auteure de cette étude dans un projet de recherche plus large qui, outre l'exploitation de l'intelligence artificielle (IA) dans la conduite de campagnes de désinformation hyperciblées, la manipulation des données et les suppress conflits cognitivo-émotionnels, se penche, entre autres questions pertinentes, sur celles de l'adaptation des lois électorales dans le contexte des capacités technologiques actuelles et sur la manière d'assurer, au mieux, la sécurité et la résilience de l'infrastructure électorale.

Le but ultime de ces analyses est d'aider les organes de gestion des élections, les législateurs, les représentants des partis politiques, les médias et la société civile et de les sensibiliser aux menaces émergentes qui remettent en cause le caractère démocratique des élections et dont les répercussions touchent au plus profond de la culture politique de nos sociétés.

Le projet s'adresse par ailleurs aux organisations internationales qui participent souvent à la gestion ou à l'observation des élections et qui doivent elles aussi tenir compte des distorsions possibles qui pourraient sinon passer facilement inaperçues.

KAS New York souhaite une excellente lecture à tous les intervenants et particuliers intéressés !

Andrea E. Ostheimer

Direction exécutive

Konrad-Adenauer-Stiftung, New York

[1] Terme inventé par la politologue Terry Lynn Karl.

Résumé

Nous sommes à l'ère de la « guerre d'émotions », où les réseaux algorithmiques de nos sphères médiatiques sociales électrisent des millions de cerveaux pour amplifier l'émotion, la haine et la méfiance.

Les guerres d'émotions sont lucratives. Déclenchées à coups de millions de dollars par des entreprises de consultance politique, elles se propagent vite, ciblant les attitudes de citoyens et populations partout dans le monde partout dans le monde. Aux États-Unis, le ressentiment des communautés afro-américaines face à la violence policière est alimentée par des usines à trolls russes délocalisées au Ghana[1] .Dans la région du Bengale occidental en Inde, les réfugiés Rohingya qui ont fui les exactions commises à leur encontre au Myanmar, sont aujourd'hui la proie d'un discours violent qui les diabolise et qui envahit rapidement WhatsApp[2] .En Afrique du Sud et au Kenya, la désinformation et le discours de haine fabriqués, en partie, par les élites politiques, ont enflammé les divisions raciales et socioéconomiques qui minent les deux pays depuis de nombreuses décennies[3].

Les guerres d'émotions posent une menace existentielle à la démocratie ; elles manipulent de plus en plus le cours des élections et minent le libre arbitre politique des populations. Au Kenya, lors des élections de 2013 et 2017, une propagande de division inflammatoire répandue en ligne, sans économie de violence graphique, a ciblé certains sous-groupes ethniques et socioéconomiques, s'imposant sur les réseaux de téléphonie mobile et des médias sociaux aussi bien que dans les médias traditionnels[4].

Chaque élection s'est vue le terrain de stratégies plus fines et précises pour le contrôle des sphères de l'information et l'exploitation d'un génie politique et émotionnel ciblé sur des communautés segmentées. Ces stratégies avaient été façonnées avec l'aide d'entreprises d'analyse de données étrangères, Cambridge Analytica et SCL Group[5], dans le but de profiler et d'influencer les comportements électoraux. Leurs cibles privilégiées étaient les jeunes Kenyans qui avaient grandi sous les forces virales et addictives des réseaux virtuels. Cela dit, les partis politiques en jeu, dont le Jubilee au pouvoir et son adversaire la National Super Alliance (NASA), avaient aussi construit et déployé une vaste architecture de communication ciblée sur certains segments de la population kenyane.

Voici donc où nous en sommes. Tout comme l'Internet a remodelé le commerce, la politique, les trames sociales et nos « récits », il s'ingère aujourd'hui plus directement que jamais dans la façon dont nous traitons et interprétons la connaissance et l'information. L'ère où nous vivons — où les technologies d'intelligence artificielle (IA) et de capture des données convergent pour analyser nos comportements et émotions — est celle d'une révolution épistémique aussi bien que technologique.

Nous cherchons dans ce rapport à cerner ce changement transformateur : à en analyser la nature, en identifier les règles et en comprendre les effets. L'accent est mis sur ce que l'érudition appelle les troubles de l'information et sur leur impact sur les élections dans différents pays d'Afrique, dont le Kenya, le Nigeria et l'Afrique du Sud. Définir l'anatomie des troubles de l'information[6] dans les pays d'Afrique représente un effort plutôt inédit mais non moins opportun à l'heure où les analystes se sont surtout penchés sur les opérations d'information de l'Occident.

Anatomie des troubles de l'information dans les élections africaines

Les sociétés africaines se trouveront sous peu face à une transformation sans précédent, alimentée par l'intégration des technologies d'IA et d'optimisation des données dans la politique, la vie quotidienne et les élections. Depuis le printemps 2019, les empreintes digitales et le visage de près de 40 millions de Kenyans ont été numérisés dans le cadre d'un nouveau système d'identification biométrique appelé à jouer un rôle fondamental dans les prochaines élections de 2022[7].

En 2020 et 2021, plusieurs nations d'Afrique se rendront aux urnes, à l'occasion d'élections législatives et présidentielles [Carte 1]. Ces nations comprennent le Ghana, l'Éthiopie, la République centrafricaine, ainsi que des pays du Sahel en proie à une agitation grandissante, à des menaces terroristes, à des migrations et à une ingérence potentielle russe dans le processus électoral. Les régimes autoritaires d'Égypte, du Burundi et de Tanzanie doivent tenir leurs élections en 2020, et ceux d'Ouganda et de Zambie, en 2021. Peut-être le scrutin sera-t-il perturbé par la pandémie qui sévit depuis le début de l'année 2020. Ce contexte d'instabilité mondiale et de méfiance ne fera qu'amplifier la menace à l'intégrité du processus politique des nations.

Ce rapport entend expliquer pourquoi et comment les troubles de l'information contaminent les élections en Afrique, en érodant la confiance du citoyen dans les institutions de l'État, et nous préparer aux défis sur le point d'émerger.

Le programme du développement mondial cherche à réaliser les promesses de l'économie numérique, porteuse de prospérité, d'inclusion et d'habilitation/autonomisation. L'avance des systèmes d'identification biométrique et numérique est exponentielle sur le continent africain, où de nombreuses nations ont entrepris l'enregistrement des données biométriques de leurs populations dans des bases de données nationales centralisées [Carte 2]. Les autorités exploitent chaque jour davantage d'autres technologies convergentes — de la reconnaissance du visage et de l'affect aux outils de surveillance du contenu des médias sociaux — pour suivre le comportement des populations, en prenant littéralement le pouls de l'électorat. Ainsi, en février 2019, l'entreprise française Gemalto annonçait une collaboration de police intelligente avec la Police ougandaise, en vue du déploiement de dispositifs biométriques portables faisant appel à l'IA pour confirmer une correspondance sur le champ[8].

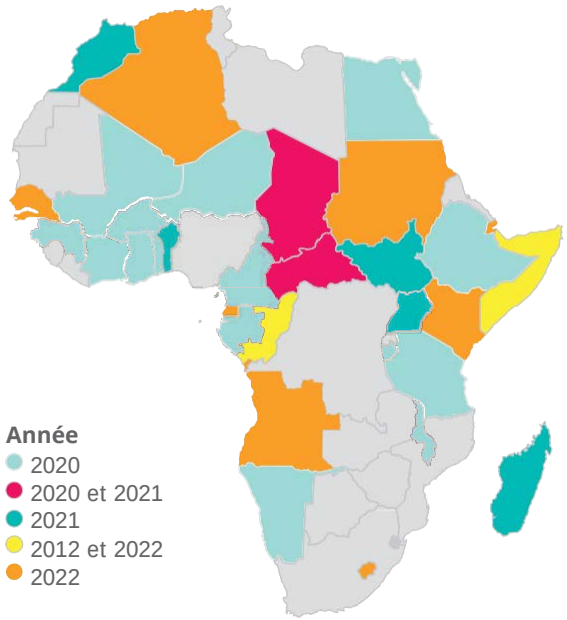
L'étude de l'impact des troubles de l'information sur les élections tend à sous-estimer gravement combien les technologies convergentes sont de plus en plus conçues pour anticiper et encourager les attitudes et les comportements humains, avec un potentiel immense de manipulation et de restriction du libre arbitre politique.

La convergence de l'IA avec la reconnaissance omniprésente du visage, des données biométriques et émotions favorise en somme de nouvelles formes d'ingénierie politique, sociale et comportementale.

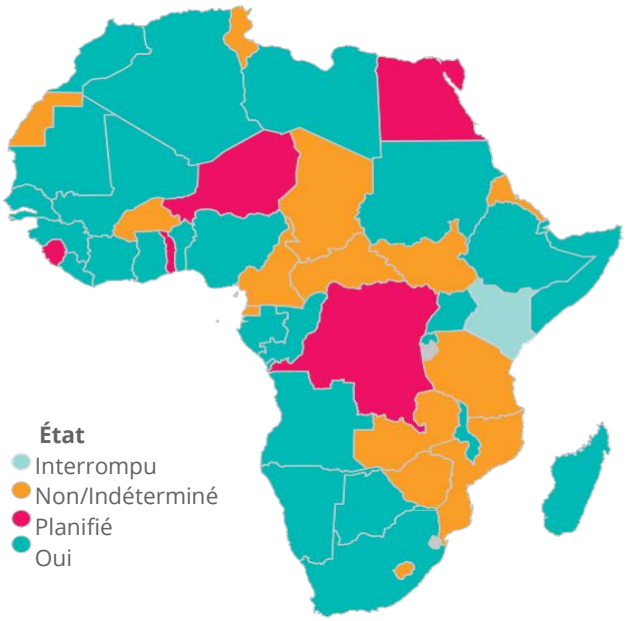
Les technologies convergentes surveillent et analysent les données biométriques et comportementales des individus, imposant graduellement un contrôle social et politique sur leur vie. Ce « pouvoir sur la vie » trouve son écho dans ce que le philosophe français Michel Foucault a appelé le biopouvoir : « [un] pouvoir qui exerce une influence positive sur la vie, qui cherche à l'administrer, à l'optimiser et à la multiplier, en l'assujettissant à des contrôles précis et à une réglementation exhaustive »[11]. À l'heure de la convergence technologique, les algorithmes amplifient essentiellement ce biopouvoir, en gonflant le potentiel des technologies à réglementer le corps collectif des sociétés.

Dans plus d'un pays d'Afrique, ces nouvelles formes de contrôles politiques et sociaux sont nées de l'alliance complexe entre différents acteurs, de nations étrangères à la pointe de la technologie aux élites dirigeantes intérieures et aux entreprises occidentales championnes de l'analyse des données et la consultance politique. Leurs pratiques collusoires prospèrent dans les sociétés où les données et la gouvernance technologique souffrent de l'absence de solides mécanismes de réglementation et de surveillance. Faute de renforcement des capacités normatives et de redevabilité utile, les populations et la société civile de plusieurs pays d'Afrique sont devenus vulnérables à la dynamique de la capture du pouvoir, des données et des ressources.

Carte 1 | Élections présidentielles ou législatives prévues[9]



Carte 2 | Mise en œuvre du système national d'identification biométrique[10]



Quatre fortes tendances technologiques, politiques et géostratégiques contribuent à la prolifération et à l'amplification des troubles de l'information dans les scrutins d'Afrique. Ces tendances constituent l'anatomie de ce que nous appelons les « conflits cognitivo-émotionnels » ou les « guerres d'émotions » dans notre rapport, de nouvelles formes d'ingénierie politique et sociale, qui exploitent les données et les technologies numériques pour contrôler et manipuler les populations.

- La première tendance se révèle dans la capacité et la disposition accrues des gouvernements au pouvoir en Afrique d'instrumentaliser les réseaux numériques pour enflammer les divisions raciales, sociales et économiques entre les sous-populations. Au Kenya, au Nigeria et en Afrique du Sud, les campagnes de « suivi et d'influence du pouls » de l'électorat n'ont fait qu'aggraver ces clivages.

- La deuxième tendance est étroitement liée à l'exploitation des tensions raciales, ethniques et économiques. Dans les pays où les lois sur la protection de la vie privée et des données ne s'accompagnent pas de robustes mécanismes opérationnels, les acteurs étatiques comme privés peuvent extraire les données personnelles sensibles de différentes bases de données démographiques en ligne pour cibler les groupes ethniques et socioéconomiques de leur choix. En s'appuyant sur les campagnes agressives et incendiaires de firmes de relations publiques telles que Cambridge Analytica, les partis politiques d'un pays peuvent exploiter le profil personnel des citoyens et leurs réseaux d'information pour répandre des rumeurs, une propagande ciblée, un discours de haine, la mésinformation et la désinformation[12]. La motivation à la base de cette architecture de désinformation sophistiquée est la volonté de plonger les citoyens dans une réalité virtuelle parallèle, où ils deviennent eux-mêmes producteurs de manipulation numérique. En Afrique, la capacité de manipuler les populations et l'information est de plus en plus imposée par « l'Internet des corps et des esprits »[13].

- En troisième lieu, le suivi et le contrôle des populations humaines est le résultat d'un programme de sécurisation où les technologies convergentes aident les acteurs de l'État à imposer la surveillance et la répression. Les tactiques et les instruments de la surveillance numérique peuvent être exploités aux deux niveaux, alimentant les troubles de l'information lors des élections et réprimant les groupes professionnels qui y opposent leur résistance, comme la presse traditionnelle et la société civile.

  Pour plusieurs pays d'Afrique confrontés à une pression intérieure grandissante, la capacité de contrôler les sphères de cyberinfluence et les infrastructures de l'information s'inscrit dans une « stratégie de survie » conçue pour préserver la stabilité des régimes. Ces gouvernements ont un intérêt direct à surveiller et à censurer le contenu et l'information qui pourrait affaiblir, voire mettre en danger, la stabilité intérieure et la légitimité du régime. Ces dernières années, une série de lois sur la cybersécurité ont été proposées et adoptées au Kenya, au Nigeria et dans d'autres États au nom de la défense et de la protection de l'intérêt national dans la lutte contre le terrorisme, même si, parfois, ces législations violent les droits individuels[14] .Au-delà des infractions aux droits humains et à la liberté d'expression, ces mesures de sécurité nationale ont progressivement donné lieu à un rétrécissement de l'espace civique. Aujourd'hui, le risque pour les populations est la fermeture de « l'espace civique virtuel ».

- Quatrièmement, enfin, lorsque des entreprises ou des pays étrangers se mettent à perturber l'information dans des nations fragiles lointaines, elles sont souvent guidées par une motivation à long terme de capture du pouvoir et des ressources[15] .La tendance paraît évidente dans les pays d'Afrique où quantités d'entreprises étrangères s'associent aux élites politiques et économiques pour influencer les résultats électoraux. Ces entreprises reçoivent la promesse d'un accès aux marchés et aux industries en expansion, partant, aux données, au pétrole, aux ressources génétiques et de biodiversité, aux minéraux de terres rares et aux métaux. De plus en plus, l'ingérence d'intérêts étrangers dépasse les confins de l'influence électorale. Depuis de nombreuses années, dans des dizaines de pays d'Afrique, des entreprises de lobbying et des courtiers en données tels que le SCL Group, analysent les données relatives aux populations africaines, de la santé et de la nutrition à l'assainissement, à l'armement et à la jeunesse militarisée.[16] .Ces firmes de consultance politique font partie de ce que le rapport appelle les « chaînes logistiques mondiales de la surveillance ». Les données sensibles qu'elles collectent leur donnent, ainsi qu'à d'autres entreprises auxquelles elles vendent leur produit au plus offrant, une plus grande influence dans la course au positionnement stratégique qui se déroule actuellement en Afrique.

Les quatre tendances ainsi décrites constituent l'anatomie des troubles de l'information. Elles sont en fait observées dans la plupart des pays — Kenya, Nigeria, Afrique du Sud, Inde, Malaisie et Brésil — ciblés par les entreprises de consultance politique.

Ce rapport n'en demeure pas moins un appel urgent à l'examen des profondes implications géopolitiques auxquelles nous nous trouvons confrontés, au carrefour de multiples changements transformateurs : une concurrence multipolaire pour la maîtrise des technologies convergentes ; l'essor de la cybersouveraineté comme modèle de gouvernance émergent des nations, qui se distancient ainsi de plus en plus de l'Occident ; l'importance cruciale du continent africain en tant que marché géostratégique pour le positionnement et le contrôle des technologies convergentes du future; et le défi du leadership normatif et, en fin de compte, la pertinence du système multilatéral et de sa capacité à établir les normes.

Importance géostratégique de l'Afrique au cœur d'une concurrence multipolaire

Le rapport dépeint par conséquent la scène plus large de l'instrumentalisation des troubles de l'information dans les élections en Afrique. Il s'agit d'une pièce en trois actes, dont les ramifications touchent au pouvoir de l'État, à la cybersouveraineté et à la géostratégie.

- Tels des métastases sur la carte du monde, les troubles de l'information semblent contaminer rapidement l'hémisphère Sud, où ils affectent les élections dans les démocraties fragiles aussi bien que sous les régimes autoritaires. Pourtant, les outils de la manipulation épistémique et émotionnelle ne se propagent pas aléatoirement à travers les veines câblées de plateformes mondiales connectées. Dans les nations d'Afrique, la convergence des technologies d'IA et de capture des données est exploitée par le pouvoir étatique, pour manipuler le comportement électoral des populations, certes, mais aussi pour renforcer les régimes en place par le biais d'une surveillance algorithmique omniprésente, de la répression et du contrôle. Les plateformes algorithmiques et biométriques — « l'assemblage biométrique » — sont mises au service de puissants objectifs de sécurisation.

  De plus en plus, au Kenya, au Nigeria et en Afrique du Sud, les populations et la société civile s'interrogent sur les tensions alentour du contrat social de l'économique numérique : Où se trouve l'équilibre entre les droits individuels et le commandement étatique de la sécurité collective et de la prospérité dans l'économie numérique ? Partout dans le monde, les décideurs politiques se trouvent confrontés à cette question, mais dans plusieurs pays d'Afrique où des projets d'identification biométrique des populations ont été entrepris sans une solide surveillance de la protection des données, elle se pose avec urgence.

Au Kenya, au Nigeria et en Afrique du Sud, l'année 2019 aura vu naître quelques efforts normatifs concernant la vie privée et la protection des données[17]. L'enjeu en est la concurrence entre les valeurs des démocraties libérales et de nouvelles formes d'autoritarisme numérique. La marchandisation de flux massifs de données relatives aux populations implique que, dans le futur, les gouvernements pourront non seulement surveiller et contrôler le comportement des personnes, des groupes, des professions et des communautés médiatiques, mais encore en produire une valeur économique à redistribuer. Le risque est que des régimes autoritaires numériques deviennent les modèles qui permettent d'assurer la préservation de l'élite dirigeante — avec sa dynamique de capture des ressources — et apportent, à la fois, croissance et sécurité sous un ordre social répressif.

Il est intéressant de noter que la question de la protection des données renvoie à la scène internationale car, dans l'économie numérique mondiale, les flux de données de population ne connaissent pas de frontières. Un souci grandissant pour les décideurs politiques, les diplomates et les chefs d'entreprises d'envergure mondiale, tient au risque de se retrouver face à un plus grand nombre de visions concurrentes de la gouvernance et à une balkanisation d'un cyberespace soumis à des normes divergentes sur la vie privé, la sécurité, la liberté d'expression et les transferts de données transfrontaliers. Avec l'émergence de lois sur la protection des données dans les pays d'Afrique, les gouvernements risquent d'imposer un contrôle national plus strict de l'Internet, en adoptant par exemple les principes de localisation des données prônés par la Chine, qui exigent le stockage des données dans le pays d'origine. Ceci explique la course à laquelle nous assistons aujourd'hui entre les plateformes technologiques américaines et chinoises pour l'établissement de centres de données et d'infrastructures informatiques sur les territoires stratégiques — villes côtières et points chauds de ressources — des pays d'Afrique.

En février 2019, Huawei inaugurait son premier centre de données en Égypte, en bordure, à point nommé, du corridor qui relie l'Afrique orientale à l'Europe. La société de télécommunications chinoise a par ailleurs signé un contrat avec le gouvernement d'Algérie pour la construction d'un centre de données destiné à ses autorités douanières et frontalières. Forte des accords BRI conclus avec le Maroc, l'Algérie, la Tunisie et l'Égypte, la Chine a établi sa présence en Méditerranée[18].

Les mesures réglementaires prises en faveur de la localisation des données et de la cybersouveraineté compliqueraient d'autant la tâche des Nations Unies et de leurs organismes (l'OMS, notamment), qui dépendent du partage mondial des données dans leur recherche de solutions aux problèmes communs tels que l'atténuation des conséquences d'une pandémie, par exemple. Il s'agit là d'un autre problème complexe de gouvernance, que l'ONU devra résoudre si elle veut garder sa pertinence dans la prévention des crises et le développement mondial.

- De plus en plus, les élections nationales peuvent être influencées pour définir le modèle de cybersouveraineté qui prévaudra sur la scène mondiale. Naguère un moment principalement stratégique dans le processus politique national d'un pays, chaque élection donne désormais aux nations étrangères à la pointe de la technologie l'occasion de façonner leurs modèles technologiques et de gouvernance des données et de jouer ainsi un rôle dans la définition historique mondiale du cyberespace.

  Dans les pays d'Afrique en particulier, les troubles de l'information pendant les élections commencent à montrer des signes d'approbation du modèle sino-russe de cybernationalisme à l'échelle normative. Cette influence normative repose de plus en plus sur des liens étroits avec la Chine, qui aide à construire et, surtout, à contrôler les infrastructures technologiques, de l'information et des ressources. Sans disposer de la puissance économique et de la cyberdiplomatie chinoises, la Russie s'appuie sur l'ingénierie politique ponctuelle de campagnes qui dégradent la cohésion des populations africaines, suscitent l'instabilité et découpent des secteurs spécifiques de capture des ressources. L'ingérence russe la plus manifeste et la mieux réussie en Afrique aura ciblé l'île lointaine de Madagascar[19]. L'opération a été orchestrée pour le Kremlin par des agents russes liés à Evgueni Prigojine, l'oligarque accusé d'ingérence dans les élections américaines de 2016.

  Bien que déployant d'ores et déjà, avec succès, des services financiers transformateurs dans l'économie numérique, les pays tels que le Kenya, l'Afrique du Sud et le Nigeria n'en restent pas moins confrontés à de longs défis économiques et de capacité et, plus important encore, à des faiblesses sur le plan de la gouvernance. Ils sont par conséquent susceptibles de s'associer à des nations à la pointe de la technologie pour bâtir les infrastructures d'information requises et importer l'expertise des technologies convergentes dont ils ont besoin pour poursuivre leur intégration dans l'économie numérique mondiale. Les pays qu'ils choisiront comme partenaires amèneront inévitablement et imposeront peut-être des normes techniques précises, des accords de propriété et une gouvernance normative.

  Dans le même temps, sur la scène mondiale, le Kenya, le Nigeria et l'Afrique du Sud représentent un véritable Eldorado de marchés numériques en expansion, donnant accès et contrôle sur les données de vastes populations, sans compter les ressources en énergie et en minerais nécessaires à l'alimentation de l'économie numérique. Mieux encore, ces pays représentent différents corridors territoriaux géostratégiques où établir les architectures numériques 5G de demain et implanter des centres d'informatique en nuage et de données satellitaires. Dans le contexte d'une concurrence multipolaire grandissante, les gouvernements du Kenya, du Nigeria et d'Afrique du Sud vont déterminer le modèle de gouvernance qui pourra les aider à s'assurer une croissance économique et une autonomie relatives sans mettre en péril la stabilité de leur régime. Le modèle de cybersouveraineté chinois se révèle une option potentielle, appliquant la cybersurveillance pour préserver la légitimité du régime et prévenir les menaces extérieures.

Autonomiser les sociétés africaines et l'avenir du multilatéralisme

Dans un monde où les États et les entreprises s'associent chaque jour davantage pour surveiller le comportement des populations et leurs réseaux d'information, comment l'ONU peut-elle se poser en leader normatif au soutien de la protection des données des populations et, par conséquent, des droits humains ? En particulier, les organismes onusiens pourront-ils obtenir le soutien des États membres pour éviter la montée de formes de collecte et de manipulation des données politiques qui impactent les populations en semant des troubles de l'information et le dysfonctionnement électoral ?

Faute de législations, de politiques et de pratiques commerciales adéquates ancrées dans les principes internationalement reconnus des droits humains, les données les plus intimes que nous partageons peuvent servir à miner les processus démocratiques au préjudice des citoyens, en particulier, les plus vulnérables.

Un diagnostic opportun et crucial serait que, dans la course à la réalisation des promesses de l'économie numérique, nous nous trouvons face à un écart omniprésent et préjudiciable entre nos cadres normatifs et l'instauration d'une redevabilité effective. Il s'agit essentiellement d'un échec, d'une incapacité à traduire les déclarations éthiques de haut niveau en mécanismes normatifs viables qui puissent assurer cette redevabilité, pour différentes populations, présentant toutes leurs vulnérabilités particulières mais aussi leurs contextes socioculturels normatifs.

En 2020, 24 pays d'Afrique sur 53 travaillaient à l'adoption ou à la mise à jour de lois et de réglementations appelées à protéger les données personnelles de leurs citoyens[20]. L'Union africaine (UA) et l'ONU pourraient assumer ici un rôle unique de leadership normatif. Les deux institutions offrent un forum où les acteurs du secteur public et privé, en collaboration avec la société civile, pourraient procéder à ce que l'auteure qualifie de « prospective normative ». L'initiative porterait sur l'établissement de collaborations multipartites qui traduisent les hauts principes législatifs de la protection des données personnelles en mécanismes et pratiques opérationnels engageant la redevabilité. Il faudra aussi tester ces pratiques normatives à l'effort dans le contexte de différents scénarios où il pourrait y avoir infraction à la vie privée et abus de données personnelles, donnant lieu à des violations des droits humains. Des acteurs de la société civile, des décideurs politiques et des experts en matière de protection des données originaires du Kenya et du Nigeria pourraient être les partenaires indispensables à inclure dans cet effort de guidance normative.

Dans un rapport important réalisé en 2019 pour l'Université des Nations Unies, l'auteure proposait de doter l'ONU d'un observatoire de prospective mondiale, chargé de définir une approche de gouvernance responsable qui exploite l'IA et les technologies convergentes au bénéfice du programme onusien de prévention des conflits et de l'autonomisation sociale[21]. Cet observatoire mondial pourrait encourager une collaboration sur mesure au soutien des organisations de la société civile, des laboratoires de droits numériques et des jeunes innovateurs d'Afrique dans leur effort d'élaborer des modèles de redevabilité et de gouvernance conformes aux besoins éthiques des démocraties africaines.

En cette capacité d'intermédiaires, différentes entités du système onusien pourraient assumer un rôle qui fait cruellement défaut au niveau international, offrant : 1) un support à la négociation de cadres normatifs adéquats concernant la protection des données, la vie privée et les droits numériques des populations, 2) une prospective normative plus utile à la mise en œuvre des mécanismes de protection des données, lesquels devront être adaptés aux défis particuliers des pays d'Afrique et 3) la mise au point d'une capacité de suivi stratégique et de planification de crise qui permette aux organes de gestion des élections d'atténuer l'impact des troubles de l'information dans le processus électoral et les risques de manipulation de leurs propres données.

Le risque n'en est pas moins, pour l'avenir proche, que les nations à la pointe de la technologie et leurs partenaires commerciaux cherchent à instrumentaliser davantage la mission onusienne de renforcement des capacités normatives et techniques pour cristalliser leur avantage concurrentiel (par voie de normes et de technologies exclusives) et augmenter leur contrôle sur les infrastructures du cyberespace transnational.

Les Etats qui dominent la convergence technologique cherchent aussi à amplifier leurs sphères d'influence normative par leur pouvoir discursif. La course au leadership leadership mondial, par le récit et l'action, est claire en ces temps de pandémie déclenchée au début de l'année 2020. La Chine, par exemple, a tenté d'éclipser les craintes et le ressentiment étrangers concernant le terrible impact mondial de la COVID-19 à coups de « pouvoir doux » (*soft power*), en envoyant du matériel médical aux pays d'Europe par trop débordés pour partager leurs fournitures au sein des frontières de leur marché interne[22]. En Chine même, les vidéos d'hôpitaux construits à la hâte étaient censées offrir une consolation virtuelle aux populations chinoises affectées[23].

L'ONU ne sera pas à l'abri des tentatives croissantes de recours recours au pouvoir discursif, au soft power et aux troubles de l'information pour affaiblir aux troubles de l'information pour affaiblir les normes et les valeurs traditionnelles du multilatéralisme. L'ère des troubles de l'information et des « guerres d'émotions » met à mal la confiance dans l'ordre multilatéral et dans la capacité de leadership de l'ONU à protéger les populations du monde, non seulement contre les menaces technologiques et biologiques, mais encore de la surveillance et de la manipulation numérique et épistémique. Pour l'ONU, la seule marche à suivre pour préserver sa pertinence est d'offrir un leadership normatif solide et tourné vers l'avenir, en partenariat avec la nouvelle génération d'acteurs de la société civile et du secteur privé, dans le but d'habiliter toutes les populations du monde. La cause appelle à un leadership normatif visionnaire.

Nous traversons une époque où les technologies de l'intelligence artificielle augmentent le potentiel de la « biopolitique » de Foucault[24], cet interventionnisme et ce contrôle réglementaire destinés à surveiller en permanence l'information relative à de vastes populations. La suprématie de l'utilisation de réseaux d'information algorithmiques pour manipuler les croyances, les attitudes et les comportements des populations au sein et au-delà de vos frontières représente aujourd'hui le moyen le plus stratégique d'acquérir le pouvoir matériel et mondial.

MESSAGES

STRATÉGIQUES ET POINTS À RETENIR

Les sociétés africaines se trouvent face à une révolution sans précédent, alimentée par l'intégration des technologies d'IA et d'optimisation des données au sein de la politique et de la société.

Les acteurs étatiques et privés impliqués dans les élections en Afrique exploitent la combinaison de l'IA et des données de population sensibles pour exercer de nouvelles formes d'ingénierie politique et sociale.

Dans un nombre grandissant de pays d'Afrique, le suivi et le contrôle des populations servent une intention de sécurisation dans laquelle les technologies convergentes aident les acteurs étatiques à imposer la surveillance et la répression.

Le risque géopolitique est que ces nations africaines adoptent le modèle de gouvernance chinois basé sur la cybersouveraineté. Dans le positionnement géostratégique de la Chine, l'Afrique se situe au cœur d'une concurrence multipolaire grandissante visant à s'assurer le contrôle de l'infrastructure informatique transnationale de l'économie numérique mondiale.

Pour conserver leur pertinence dans la résolution des problèmes communs, de la prévention des pandémies à l'atténuation du changement climatique, les institutions multilatérales se doivent d'exercer un leadership normatif qui aide à autonomiser et à protéger les populations africaines au sein de l'économie numérique.

Motivation et contenu du rapport

Ce rapport cherche à analyser l'anatomie des troubles de l'information et leur impact sur les élections dans différents pays d'Afrique, y compris le Kenya, le Nigeria et l'Afrique du Sud. Y sont aussi démontrés pourquoi et comment l'influence sur les élections en Afrique joue un rôle essentiel dans le positionnement géostratégique en ces temps de concurrence multipolaire grandissante. Le contexte géopolitique plus large présente d'importantes ramifications sur le plan du pouvoir étatique, de la cybersouveraineté et de l'avenir du multilatéralisme.

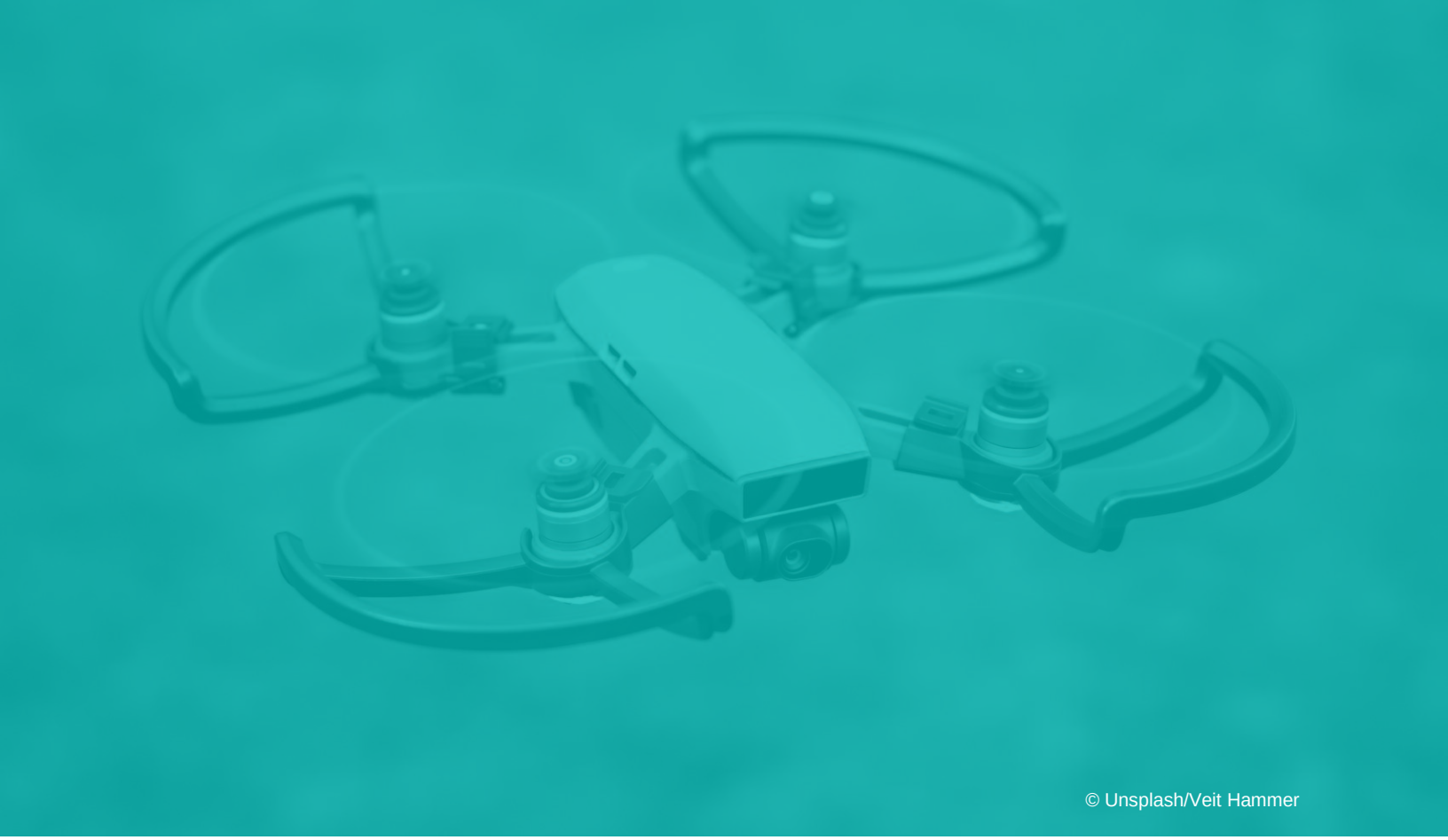
La **1re partie** du rapport présente une analyse succincte de quelques-unes des tendances technologiques, politiques et géostratégiques générales qui contribuent à la prolifération et à l'amplification des troubles de l'information dans les élections africaines. Ces tendances constituent l'**anatomie des troubles de l'information** – ou « conflits cognitivo-émotionnels » ou encore « guerres d'émotions » –, de nouvelles formes d'ingénierie politique et sociale, qui exploitent les données et les technologies numériques pour suivre et contrôler les comportements de populations.

Cette partie propose aussi un bref aperçu de l'impact des quatre tendances identifiées sur les élections au Kenya. Les parties suivantes présentent des analyses d'études de cas plus approfondies, concernant le Kenya, le Nigeria et l'Afrique du Sud.

La **2e partie** examine un paradigme important – **« l'Internet africain des corps et des esprits »** – dans lequel les sociétés africaines se trouvent confrontées à un bouleversement sans précédent, alimenté par l'intégration des technologies d'IA et d'optimisation des données dans la politique, la vie quotidienne et les élections. Dans de nombreux pays d'Afrique, des systèmes biométriques, algorithmiques et d'identification numérique centralisent les données sensibles des populations, ouvrant un créneau d'accès aux services publics essentiels. À défaut d'une solide protection des droits de l'homme et des données, toutefois, ces systèmes posent des risques omniprésents, de la consolidation de la discrimination à l'exploitation de l'information personnelle à des fins de gain électoral. Pire, il n'existe aucune forme de redevabilité et de responsabilité des risques, en particulier lorsque ces technologies interviennent dans le processus électoral. Les implications sur le plan de la vie privée et du libre arbitre des populations pourraient être graves. Équipés d'outils technologiques qui leur permettent d'analyser et de contrôler les réactions humaines à l'information et à la connaissance, les gouvernements et les entreprises impliquées dans les élections en Afrique peuvent de plus en plus surveiller et influencer les attitudes des populations, offrant un potentiel considérable de manipulation et de restriction du libre arbitre politique.

La **3e partie** part d'études de cas relatives au Kenya, au Nigeria et à l'Afrique du Sud pour examiner la machine de manipulation numérique qui sous-tend la **« fabrication et propagation des guerres d'émotions » :** 1) élaboration de profils d'électeurs sur la base de données divulguées, vendues ou décryptées originaires de vastes bases de données gouvernementales ou privées ; 2) création d'une propagande vive, voire graphiquement violente qui exploite les tensions ethniques et socioéconomiques pour cibler des segments d'électorat définis en fonction de leur ethnie, de leurs tendances politiques et de leur âge ; 3) recours aux réseaux de substitution pour inonder les sphères de l'information telles que les applications de messagerie privée, ainsi que la télévision, la radio et les médias sociaux ; 4) vigoureuses campagnes publicitaires numériques et modification du moteur de recherche algorithmique et de la réglementation de contenu algorithmique sur les plateformes médiatiques sociales ; 5) Réduction au silence de toutes formes de résistance par la répression des structures de médias traritionnels.

La **4e partie** illustre le rôle des troubles de l'information dans le programme plus large de la sécurisation. Cette section présente en détail la manière dont les États d'Afrique exploitent les technologies convergentes, y compris l'IA et la biométrie, la reconnaissance du visage et de l'affect, à des fins de contrôle politique et social. Elle dévoile aussi l'influence du crédit social de la Chine sur les sociétés africaines et décrit les **chaînes logistiques mondiales de la surveillance**. En suivant constamment les « corps et les esprits traçables », ces forces biopolitiques exercent et amplifient la dynamique de l'exclusion et de la discrimination imposée aux populations déjà vulnérables.



© Unsplash/Veit Hammer

« Les élections nationales peuvent être influencées pour définir le modèle de cybersouveraineté qui prévaudra sur la scène mondiale.

La **5e partie** démontre en quoi les troubles de l'information sont symptomatiques d'une concurrence multipolaire plus large visant l'influence normative dans le cyberespace. Les gouvernements du Kenya, du Nigeria et d'Afrique du Sud doivent décider quel modèle de cybergouvernance les aidera à projeter leur souveraineté, tout en poursuivant l'autonomie économique et sécuritaire. Leurs options de gouvernance dépendent de plus en plus de la nation à la pointe de la technologie qu'ils choisiront comme partenaire. Cette section présente une analyse approfondie du **analyse approfondie des collaborations Sino-Africaines pour la convergence technologique**, suivant l'exemple de l'initiative chinoise Belt and Road Initiative (BRI).

La conclusion propose un programme de recherche future à l'intention de l'ONU et des organes de gestion des élections. Elle s'achève sur une réflexion concernant le rôle que pourrait assumer le système multilatéral pour aider les sociétés africaines à éviter la manipulation numérique et électorale : 1) support à la négociation de cadres normatifs adéquats concernant la protection des données, la vie privée et les droits numériques des populations ;
2) prospective normative plus utile à la mise en œuvre des mécanismes de protection des données, lesquels devront être adaptés aux défis particuliers des pays d'Afrique et 3) mise au point d'un suivi stratégique et d'une planification de crise qui permettent aux organes de gestion des élections d'atténuer l'impact des troubles de l'information dans le processus électoral.

Konrad-Adenauer-Stiftung e. V.

Andrea E. Ostheimer
Executive Director
www.kas.de/newyork

andrea.ostheimer@kas.de