Les élections et la démocratie
à l'ère du numérique

Une initiative de la Fondation Kofi Annan

PROTÉGER L'INTÉGRITÉ ÉLECTORALE À L'ÈRE DU NUMÉRIQUE

Rapport de la Commission Kofi Annan sur les élections et la démocratie à l'ère du numérique

Janvier 2020

TABLE DES MATIÈRES

À propos de la Commission Kofi Annan sur les élections et la démocratie à l'ère du numérique 1

Les membres de la Commission 5

Avant-propos 9

Résumé 14
Renforcement des capacités 17
Renforcement des normes 18
Actions à mener par les pouvoirs publics 20
Actions à mener par plateforme 22

I. Les élections : un pilier de la lutte pour la démocratie 25

II. Polarisation affective, réseaux sociaux et intégrité électorale 31
Réseaux sociaux et polarisation 35
Actions à envisager 38

III. Discours de haine et intégrité électorale 41
Approches de réglementation des discours de haine 44
Actions à envisager 49

IV. Protection de l'intégrité électorale contre la désinformation 55
Mesure de la fréquence de la désinformation 58
La désinformation comme arme politique 61
Actions à envisager 62

V. La publicité à des fins politiques à l'ère du numérique 71
Actions à envisager 76

VI. Protection des processus électoraux contre l'ingérence étrangère 81
Émergence d'acteurs transnationaux spécialisés dans la manipulation électorale 83
Protection des infrastructures électorales 84
Actions à envisager 86

VII. Synthèse des recommandations 91
Renforcement des capacités 91
Renforcement des normes 93
Actions à mener par les pouvoirs publics 94
Actions à mener par plateforme 96

Remerciements 97

À propos de la Fondation Kofi Annan 99

Bibliographie 101

LISTE DES FIGURES

Encadré 1 Les réseaux sociaux, une arme contre les femmes 43

Encadré 2 Coupures du réseau Internet en Asie et en Afrique 47

Encadré 3 Initiatives en faveur de la diversité dans le codage 52

Encadré 4 Surveillance citoyenne des discours de haine au Kenya, 2012-2013 53

Encadré 5 Lutte contre la désinformation au Mexique 66

Encadré 6 Lutte contre la désinformation en Indonésie, 2018-2019 68

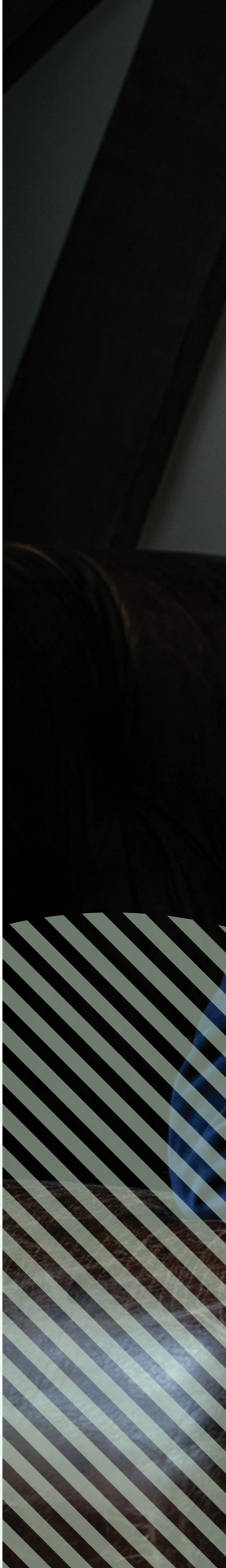
Encadré 7 Accord d'Abuja sur la conduite des élections au Nigéria, 2015 77

À PROPOS DE LA COMMISSION KOFI ANNAN SUR LES ÉLECTIONS ET LA DÉMOCRATIE À L'ÈRE DU NUMÉRIQUE

(KACEDDA)

Pendant toute sa vie, Kofi Annan a défendu le droit des citoyens à choisir la forme de leur gouvernement et leurs gouvernants. Il était fermement convaincu que la gouvernance démocratique et l'autonomisation des citoyens sont indispensables à la mise en œuvre du développement durable, dans un contexte de sécurité et de paix durable. Ce principe guide pour grande partie l'action de la Fondation et, tout particulièrement, son initiative en faveur de l'intégrité électorale.

En 2018, il lançait l'un de ses derniers projets majeurs, à savoir la Commission sur les élections et la démocratie à l'ère du numérique. Pendant 12 mois, ses membres, issus de la société civile, des pouvoirs publics, du secteur technologique, du monde universitaire et des médias, ont étudié et passé en revue les possibilités et les défis que présentent les innovations technologiques pour l'intégrité électorale.



> « La technologie évolue, la démocratie doit faire de même. »
>
> **- Kofi Annan**

Avec l'assistance d'un secrétariat restreint hébergé par l'université de Stanford et de la Fondation Kofi Annan, la Commission a mené de nombreuses consultations dans le but d'émettre des recommandations sur l'utilisation des nouvelles technologies, des plateformes de réseaux sociaux et des outils de communication pour impliquer, autonomiser et sensibiliser les électeurs ainsi que pour renforcer l'intégrité des élections.

Principales questions ayant guidé la réflexion de la Commission :

- Quels éléments fondamentaux de la technologie numérique auront un impact spécifique (négatif ou positif) sur la démocratie et les processus électoraux ?

- Quel est le potentiel des technologies numériques en matière de renforcement et d'affaiblissement de l'intégrité de l'environnement électoral ?

- Comment tirer parti de la technologie pour assurer la transparence des élections et la responsabilisation des pouvoirs publics ?

- Quelles perspectives et incitations à participer aux processus démocratiques la technologie numérique offre-t-elle aux électeurs, notamment aux jeunes ?

- Quels sont le rôle et l'impact du financement politique dans le déploiement et l'adoption de stratégies et d'instruments électoraux fondés sur le numérique ?

Objectifs de la Commission :

1. Identifier et circonscrire les défis que pose l'expansion mondiale des technologies numériques et des plateformes de réseaux sociaux vis-à-vis de l'intégrité électorale.

2. Élaborer des politiques aptes à surmonter ces défis et à mettre en lumière les pistes de renforcement de l'intégrité électorale et de participation à la vie politique qu'offre l'innovation technologique.

3. Définir et formuler un plaidoyer visant à diffuser largement les messages clés élaborés par la Commission et à en débattre dans le monde entier.

Déclaration de la Présidente de la Commission

« À l'ère du numérique qui est la nôtre, les nouvelles technologies et les plateformes de réseaux sociaux modifient en profondeur les démocraties et les processus démocratiques aux quatre coins de la planète. Susceptibles, plus que tout autre outil, de contribuer à la gouvernance démocratique à laquelle aspirent les citoyens, elles engendrent aussi de nouveaux risques et enjeux s'agissant des processus démocratiques et des droits politiques.

Avec l'équipe de Stanford et la Fondation Kofi Annan, les membres de la Commission et moi-même sommes déterminés à faire honneur à l'héritage de M. Annan en octroyant à la Commission un rôle de premier plan dans la défense et le renforcement des processus électoraux qui constituent le cœur même de la démocratie. »

- Laura Chinchilla

PRÉSIDENTE DE LA COMMISSION KOFI ANNAN SUR LES ÉLECTIONS ET LA DÉMOCRATIE À L'ÈRE DU NUMÉRIQUE

LES MEMBRES DE LA COMMISSION

La Commission Kofi Annan sur les élections et la démocratie à l'ère du numérique réunit plusieurs des figures les plus éminentes du secteur technologique, du monde universitaire et de la vie politique dans le but de répondre à une question simple : comment atténuer les risques que fait courir l'ère numérique à l'organisation de nos élections tout en en exploitant ses apports et en renforçant, *in fine*, la démocratie dans le monde ?

Kofi Annan ǂ Président de séances
(Ghana)

Lauréat du prix Nobel de la paix, Secrétaire général des Nations Unies de 1997 à 2007 et Président fondateur de la Fondation Kofi Annan

Laura Chinchilla – Présidente
(Costa Rica)

Vice-présidente du Club de Madrid, ancienne Présidente du Costa Rica

Yves Leterme – Vice-président
(Belgique)

Ancien Secrétaire général de l'Institut international pour la démocratie et l'assistance électorale, ancien Premier ministre de la Belgique

Stephen Stedman – Secrétaire général de la Commission
(États-Unis)

Chercheur principal du Freeman Spogli Institute for International Studies et professeur de sciences politiques à l'université de Stanford

Noeleen Heyzer
(Singapour)

Ancienne Secrétaire exécutive de la Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique

Toomas Hendrik Ilves
(Estonie)

Collaborateur émérite, Hoover Institution, ancien Président de l'Estonie

Ory Okolloh

(Kenya)

Directrice de Luminate pour la zone Afrique

Nate Persily

(États-Unis)

James B. McClatchy, professeur de droit
à la Stanford Law School

Alex Stamos

(États-Unis)

Professeur-chercheur à l'université de Stanford, ancien responsable en chef de la sécurité chez Facebook

William Sweeney

(États-Unis)

Ancien président et directeur général de la Fondation internationale pour les systèmes électoraux (IFES)

Megan Smith

(États-Unis)

Fondatrice et directrice générale de Shift7, ancienne responsable technologique en chef (États-Unis)

Ernesto Zedillo

(Mexique)

Directeur du Yale Center for the Study of Globalization, ancien Président du Mexique

AVANT-PROPOS

La consolidation démocratique se heurte actuellement à des difficultés majeures partout dans le monde. Les menaces qui pèsent sur la démocratie sont devenues plus insidieuses, notamment du fait de la manipulation des procédures juridiques et constitutionnelles – conçues initialement pour protéger la démocratie contre les dérives arbitraires et abusives. Pierre angulaire de la légitimité démocratique, la tenue d'élections libres et justes subit la pression considérable des mouvements populistes et des courants post-vérité, qui exploitent les nouvelles technologies de communication numériques pour semer la confusion dans l'esprit des citoyens et les tromper. Aujourd'hui, les élections libres et justes, principale expression de la volonté démocratique de gouverner collectivement, sont loin d'être garanties dans de nombreux pays. Afin d'y remédier, il incombera aux responsables des plateformes technologiques, gouvernements et citoyens d'adopter de nouvelles politiques et de mener de nouvelles actions.

La vulnérabilité de l'intégrité électorale dans le monde constitue un symptôme des processus d'érosion démocratique plus larges observés autant dans les démocraties historiques que récentes : progression de la polarisation politique, sentiment de méfiance grandissant entre concitoyens mais aussi entre citoyens et institutions gouvernementales, attaques systématiques contre la presse et les médias indépendants, déclin des partis politiques en tant que véhicules légitimes de regroupements d'intérêts et mécontentement croissant né du sentiment que les gouvernements démocratiques ne satisfont pas aux besoins et aux aspirations élémentaires des populations.

Le recours aux technologies de communication numériques, souvent considérées comme la source de cette érosion démocratique, occupe une place centrale à cet égard. Selon certains, les réseaux sociaux polarisent le débat public et poussent les gens vers les partis extrêmes.

D'autres affirment que les réseaux sociaux créent des « bulles de filtrage » et des « chambres d'écho », qui réduisent l'accès à des sources d'information et des points de vue diversifiés nécessaire à la réflexion démocratique. Parce que les équipes de campagnes politiques envoient sur les réseaux sociaux des appels personnalisés à de petits groupes d'électeurs ciblés, certains observateurs avancent que les réseaux sociaux affaiblissent le débat public et l'esprit de dialogue propres aux campagnes électorales traditionnelles. De fait, les débats actuels sur les causes et les effets de l'érosion démocratique doivent s'intéresser au rôle des technologies de communication numériques, faute de quoi ils risquent de ne pas couvrir l'ensemble du problème.

C'est la raison pour laquelle Kofi Annan a créé la Commission sur les élections et la démocratie à l'ère du numérique. Profondément inquiet des effets des technologies de l'information et de la communication (TIC) sur la démocratie et les élections, M. Annan a jugé – à l'issue de consultations menées avec des experts du monde entier – que la création d'une nouvelle commission pourrait éclairer plusieurs enjeux fondamentaux en lien avec ces sujets. Il a assigné à la Commission un mandat en vue i) d'identifier et cerner les défis que pose l'expansion mondiale des technologies numériques et des réseaux sociaux à l'égard de l'intégrité électorale et ii) d'élaborer des politiques visant à les surmonter.

M. Annan a demandé à la Commission d'adopter une perspective internationale et de s'efforcer de comprendre les diverses manifestations de ces problématiques sur différents continents, notamment dans les démocraties du Sud. Pour ce faire, la Commission a consulté experts et pouvoirs publics au Brésil, au Mexique, au Kenya, en Côte d'Ivoire, en Afrique du Sud et en Inde et commandité plusieurs études en Amérique latine, en Afrique et en Asie. Elle a également rencontré des représentants de la Commission européenne et consulté des acteurs de premier plan du secteur d'Internet et des réseaux sociaux.

Son rapport émet plusieurs recommandations visant à renforcer les capacités des autorités en charge de l'intégrité électorale, à élaborer des normes fondées sur un consensus concernant l'utilisation acceptable des technologies numériques dans les élections et à encourager les actions consolidant l'intégrité électorale qui sont menées par les pouvoirs publics et les entreprises high-tech. Ces recommandations découlent de l'une des principales conclusions du rapport : toutes les parties prenantes compétentes (plateformes technologiques et numériques, gouvernements, autorités électorales, médias traditionnels et citoyens) ont un rôle crucial à jouer dans le renforcement de l'intégrité électorale.

Je remercie Yves Leterme, Vice-président de la Commission, et les autres membres de la Commission pour leur contribution et leur dévouement tout au long du projet. Je souhaite notamment exprimer mes sincères remerciements au Secrétaire général de la Commission, Stephen Stedman, qui a supervisé l'étude et les consultations pour le compte de la Commission, et qui a joué un rôle central dans la rédaction du présent rapport. Je suis également profondément reconnaissante à la Fondation Kofi Annan, pour son appui précieux, et à son Président, Alan Doss, sous les auspices duquel la Commission a été réunie.

M. Annan est décédé brutalement avant que la Commission ne débute ses travaux. Les questions d'intégrité électorale lui tenaient particulièrement à cœur, faisant écho à son expérience de médiateur après les élections kenyanes frauduleuses de 2007, qui ont conduit le pays au bord de la guerre civile et se sont traduites par la mort de milliers de Kenyans et le déplacement forcé de centaines de milliers de personnes. En hommage à sa vision, à sa défense de la démocratie et à ses efforts permanents déployés en faveur de l'état de droit et de la paix internationale, nous dédions le présent rapport à sa mémoire. Protecteur et défenseur de l'intégrité électorale, Kofi Annan laisse

derrière lui un riche héritage. Nous espérons que ce rapport lui fait honneur et portera sa voix dans les débats et les échanges futurs, mais plus encore dans les actions qui viseront à renforcer l'intégrité des élections dans le monde.

- Laura Chinchilla

PRÉSIDENTE, COMMISSION KOFI ANNAN SUR LES ÉLECTIONS ET LA DÉMOCRATIE À L'ÈRE DU NUMÉRIQUE

RÉSUMÉ

Les nouvelles technologies de l'information et de la communication (TIC) posent des problèmes ardus quant au respect de l'intégrité électorale. Ces dernières années, des gouvernements étrangers ont exploité les réseaux sociaux et Internet pour s'ingérer dans les élections un peu partout dans le monde. La désinformation s'est transformée en arme afin de discréditer les institutions démocratiques, de semer la méfiance au sein de la société et d'attaquer les adversaires politiques. Les réseaux sociaux ont été prisés par les groupes extrémistes pour envoyer des messages de haine et inciter à la violence. Les gouvernements démocratiques s'efforcent de réagir au phénomène inédit des publicités à visée politique, favorisé par l'essor des TIC. L'intégrité électorale fait l'objet d'attaques potentielles portant sur la nature même du processus électoral mais aussi sur la qualité de la délibération démocratique.

La corrélation entre Internet, les réseaux sociaux, les élections et la démocratie est complexe, systémique et en constante mutation. Le refus opposé par les grandes plateformes de réseaux sociaux s'agissant de la communication des données aux chercheurs limite notre capacité à évaluer quelques-unes des hypothèses marquantes. Certaines conclusions semblent néanmoins irréfutables :

- Un grand nombre des maux dont Internet et les réseaux sociaux ont été accusés (polarisation extrême du jeu politique démocratique, déclin de la confiance envers les gouvernements, médias traditionnels et la société en général, médias partisans et désinformation) existaient avant leur apparition même.

- Bien que les réseaux sociaux n'engendrent pas nécessairement une polarisation politique à grande échelle, ils l'exacerbent et l'intensifient. Ils constituent également un outil à la disposition de toute personne cherchant à saper l'intégrité électorale et à polluer la délibération démocratique.

- La vulnérabilité des démocraties face à la désinformation varie en fonction de l'existence antérieure des phénomènes mentionnés (polarisation, méfiance et tendances partisanes des médias traditionnels). Les démocraties du Sud (nouvelles ou en devenir) sont particulièrement exposées.

- À moyen terme, les élections dans les démocraties du Sud deviendront une caisse de résonnance de la désinformation et des discours de haine sur les réseaux, tout en étant le réceptacle des ingérences extérieures et manipulations intérieures.

- Nombreux sont les acteurs à porter une responsabilité certaine dans la dérive observée sur les réseaux sociaux qui les transforme en menaces pour le respect de l'intégrité électorale :

    - Les grandes plateformes ont autorisé la diffusion virale des discours de haine et de la désinformation et n'ont pas anticipé l'usage qui serait fait de leurs technologies dans les pays connaissant une transition démocratique (ou proto-démocraties) dont les sociétés sont fracturées et hantées par des explosions de violences ethniques et religieuses. Elles ont par ailleurs rejeté les preuves attestant que leurs services sapaient la démocratie et encourageaient la violence. Elles ont enfin lancé des campagnes de dénigrement contre les critiques et ont tardé à réagir de façon constructive.

    - Les candidats et les élus, quant à eux, se sont servis des réseaux sociaux pour fomenter la haine, diffuser la désinformation et compromettre la confiance des citoyens à l'égard des institutions civiles et gouvernementales.

- Certains consultants politiques ont cherché à manipuler les processus électoraux afin de gagner à tout prix, et ont fait de la manipulation électorale un fonds de commerce transnational qui menace l'intégrité électorale sur l'ensemble du globe.

- Les médias traditionnels ont souvent amplifié la désinformation et la propagande au lieu de la combattre.

La défense de l'intégrité électorale contre le mauvais usage des réseaux sociaux dépendra des choix et du comportement des entreprises et des grandes plateformes technologiques tout autant que de l'attitude des gouvernements, des personnalités politiques, des médias traditionnels, des organes de gestion des élections, et des citoyens. Pour protéger l'intégrité électorale à l'ère numérique, nous devrons renforcer les capacités de ses défenseurs et élaborer des normes communes sur l'utilisation acceptable des technologies numériques lors de la tenue d'élections. Les plateformes technologiques et les pouvoirs publics doivent prendre des mesures pour soutenir l'intégrité électorale.

RENFORCEMENT DES CAPACITÉS

Recommandation 1

Il faut impérativement consacrer davantage d'attention et de ressources à la promotion de l'intégrité électorale. Les pouvoirs publics, les organisations internationales, les fondations philanthropiques et la société civile doivent investir dans le recours à des spécialistes en technologie et le renforcement des capacités numériques, tout en favorisant les initiatives auprès des médias et en appuyant la constitution d'organes de gestion des élections qui protègent et promeuvent le principe d'intégrité. Toutes les parties prenantes intéressées doivent coopérer, collaborer et partager rapidement les informations relatives aux menaces pesant sur l'intégrité électorale. Ces efforts prendront les formes suivantes :

- Création d'un indice de la vulnérabilité électorale déterminant les élections qui nécessitent une étroite surveillance contre une éventuelle ingérence, les comportements en ligne usurpateurs coordonnés, la mésinformation ou encore la désinformation.

- Renforcement des capacités des partenariats nationaux de défense de l'intégrité des élections luttant contre la désinformation et soutien à l'amélioration de l'évaluation et du partage des bonnes pratiques.

- Financement des organisations de la société civile qui combattent les discours de haine, le harcèlement ciblé et l'incitation à la violence, notamment dans les périodes pré-électorales.

- Dispense d'une expertise à l'adresse des organes de gestion des élections en matière de bonnes pratiques liées à la cybersécurité.

- Soutien apporté aux démocraties dans l'élaboration de programmes technologiques civiques par le biais de l'enseignement du codage, notamment aux femmes et aux minorités, et de l'intégration de spécialistes techniques au sein des équipes gouvernementales.

Recommandation 2

Certains organes de gestion des élections pourront nécessiter une assistance technique à court terme afin de réagir aux menaces que font peser les ingérences étrangères – ainsi que le piratage et les discours de haine incitant à la violence en contexte électoral – sur l'intégrité des élections. Dans ce type de cas, l'assistance technique internationale requise pour les aider à assurer le bon déroulement des élections devra être dispensée aussitôt après réception de la demande. Afin de permettre cette réactivité, nous conseillons la mise en place d'équipes permanentes de cybersécurité électorale pouvant être déployées immédiatement sur demande. Ces équipes pourraient être basées dans des organisations internationales existantes telles que la Division de l'assistance électorale des Nations Unies, des organisations régionales ou une nouvelle institution internationale. La rotation des postes techniques constituerait une bonne pratique de gouvernance numérique au sein de ces instances.

RENFORCEMENT DES NORMES

Recommandation 3

Nous adhérons à l'appel de la Commission transatlantique sur l'intégrité des élections invitant les candidats, partis et groupes politiques à s'engager par écrit à rejeter les pratiques de campagnes politiques numériques trompeuses, à savoir : utilisation de données ou de documents volés, recours à des supports visuels altérés déformant les propos d'une personnalité à un degré de réalisme plus ou moins élevé (« shallow fakes » et « deep fakes »), publication de fausses images de nus (« deep nudes »), production, utilisation ou diffusion de documents falsifiés ou faux, ou encore collusion avec des gouvernements étrangers et leurs agents dans le but de manipuler une élection.

Recommandation 4

Les gouvernements démocratiques doivent joindre leurs forces afin d'élaborer une convention internationale sur le rôle des gouvernements étrangers et de leurs agents dans les élections d'autres pays. Il serait notamment judicieux qu'ils établissent des normes internationales opérant la distinction entre assistance transfrontière légitime et interventions illicites ou illégales.

Recommandation 5

Les gouvernements démocratiques doivent considérer les technologies électorales électroniques (TEE) comme des infrastructures cruciales et soutenir la norme approuvée par le G20, à savoir : Les États ne doivent pas mener ou soutenir en connaissance de cause une quelconque activité relevant des technologies de l'information et de la communication (...) qui endommagerait intentionnellement les infrastructures cruciales.

Recommandation 6

Les fournisseurs d'équipements et de services électoraux devraient s'engager à respecter un code de conduite afin de garantir que leurs produits sont sécurisés, que leurs pratiques commerciales protègent les droits, la vie privée et les données des citoyens des pays clients, et que leurs pratiques d'achat sont honnêtes et transparentes. La communauté internationale en faveur de l'intégrité électorale devrait s'engager quant à elle à conditionner l'assistance électorale dispensée aux pays à la signature et au respect de ce code par les fournisseurs. L'élaboration de ce code de conduite devrait se dérouler dans le cadre d'une initiative multipartite impliquant a minima la communauté en faveur de l'intégrité électorale, le Réseau mondial d'observateurs nationaux des élections et des partenaires internationaux.

Recommandation 7

Il conviendrait que la communauté en faveur de l'intégrité électorale élabore des normes applicables aux cabinets transnationaux de conseil spécialisés dans les campagnes politiques, y compris aux sociétés de relations publiques et de communication stratégique, ainsi qu'aux experts en marketing numérique. Les réglementations devraient établir des procédures de certification régissant l'activité de ces consultants, et interdire aux sociétés qui violent les normes et les règles de consulting en campagnes électorales de poursuivre leurs missions.

ACTIONS À MENER PAR LES POUVOIRS PUBLICS

Recommandation 8

Les pays doivent adapter leurs réglementations sur la publicité politique à l'environnement en ligne. Les autorités publiques compétentes doivent :

- définir en droit la nature des publicités à visée politique ;
- obliger les plateformes de réseaux sociaux à rendre publiques toutes les informations relatives à l'achat de publicités, notamment l'identité réelle de l'annonceur, les montants dépensés, les critères de ciblage et l'identité des créateurs effectifs de l'annonce ;
- préciser en droit la taille minimale du segment de la population ciblée par les publicités ;
- légiférer sur l'arrêt de la diffusion des publicités numériques à visée politique au moins 48 heures avant la tenue d'élections.

Recommandation 9

Les pouvoirs publics doivent obliger les grandes plateformes Internet à communiquer à des tiers indépendants des données pertinentes concernant l'impact des réseaux sociaux sur la démocratie. Les plateformes doivent notamment :

- communiquer des données sécurisées (et respectant les règles de confidentialité) à des institutions universitaires certifiées afin qu'elles étudient les questions suivantes : existence éventuelle de biais favorables aux opinions extrémistes dans les algorithmes, impact des réseaux sociaux sur la polarisation politique et la consommation d'informations, décryptage de la corrélation entre discours de haine en ligne et violence hors ligne, etc. ;

- tenir à jour leurs comptes rendus sur la transparence afin de fournir au public des données sur le nombre de signalements de discours de haine et d'abus en ligne. Les données en question devraient porter, entre autres, sur les cas d'abus ciblés (selon des critères ethniques, de genre, d'orientation sexuelle ou d'affiliation religieuse) et la fréquence à laquelle ils visent différentes communautés ;

- déclarer les comptes ayant recours à des pratiques d'automatisation. Les plateformes doivent être passibles de pénalités financières en cas de comptes automatiques non déclarés comme tels (bots, etc.).

Recommandation 10

Les pouvoirs publics devraient promouvoir l'éducation aux usages numériques et aux médias dans les écoles ainsi que dans le cadre de programmes d'intérêt public destinés à l'ensemble de la population.

ACTIONS À MENER PAR PLATEFORME

Recommandation 11

Les plateformes devraient assurer la transparence accrue des publicités à visée politique :

- Les plateformes devraient laisser le choix aux utilisateurs d'accepter ou de refuser la publicité à des fins politiques.

- Les plateformes ne devraient accepter de vendre des espaces publicitaires qu'aux candidats, aux partis et aux groupes s'étant formellement engagés à éviter les pratiques de campagne trompeuses. Cet engagement deviendrait alors la norme contractuelle régissant l'approbation ou le refus d'une publicité donnée.

- Afin d'éviter que les financeurs ne se cachent derrière des noms d'organisations frauduleux, les plateformes devraient exiger la divulgation publique de l'identité des personnes finançant la publicité politique, quelle qu'elle soit.

Recommandation 12

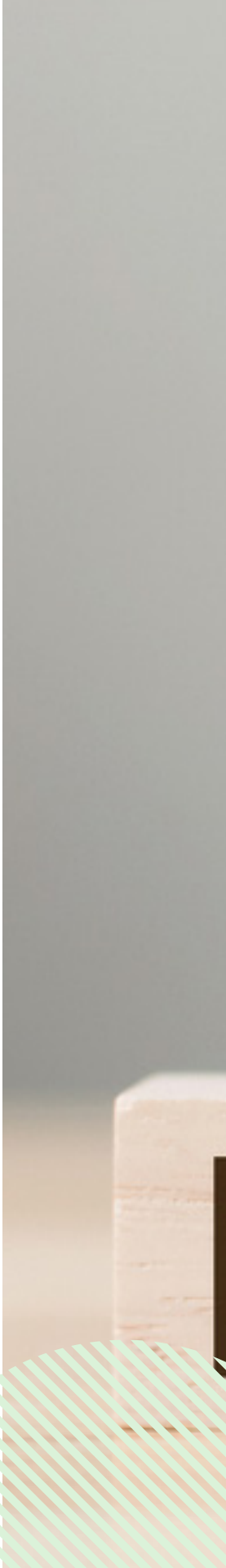
Les plateformes de réseaux sociaux doivent élaborer des systèmes d'alerte précoce prenant en compte la désinformation en rapport avec des élections, les ingérences étrangères, les crimes et délits motivés par la haine, les menaces proférées à l'encontre des femmes, la violence et les dissuasions à se rendre aux bureaux de vote :

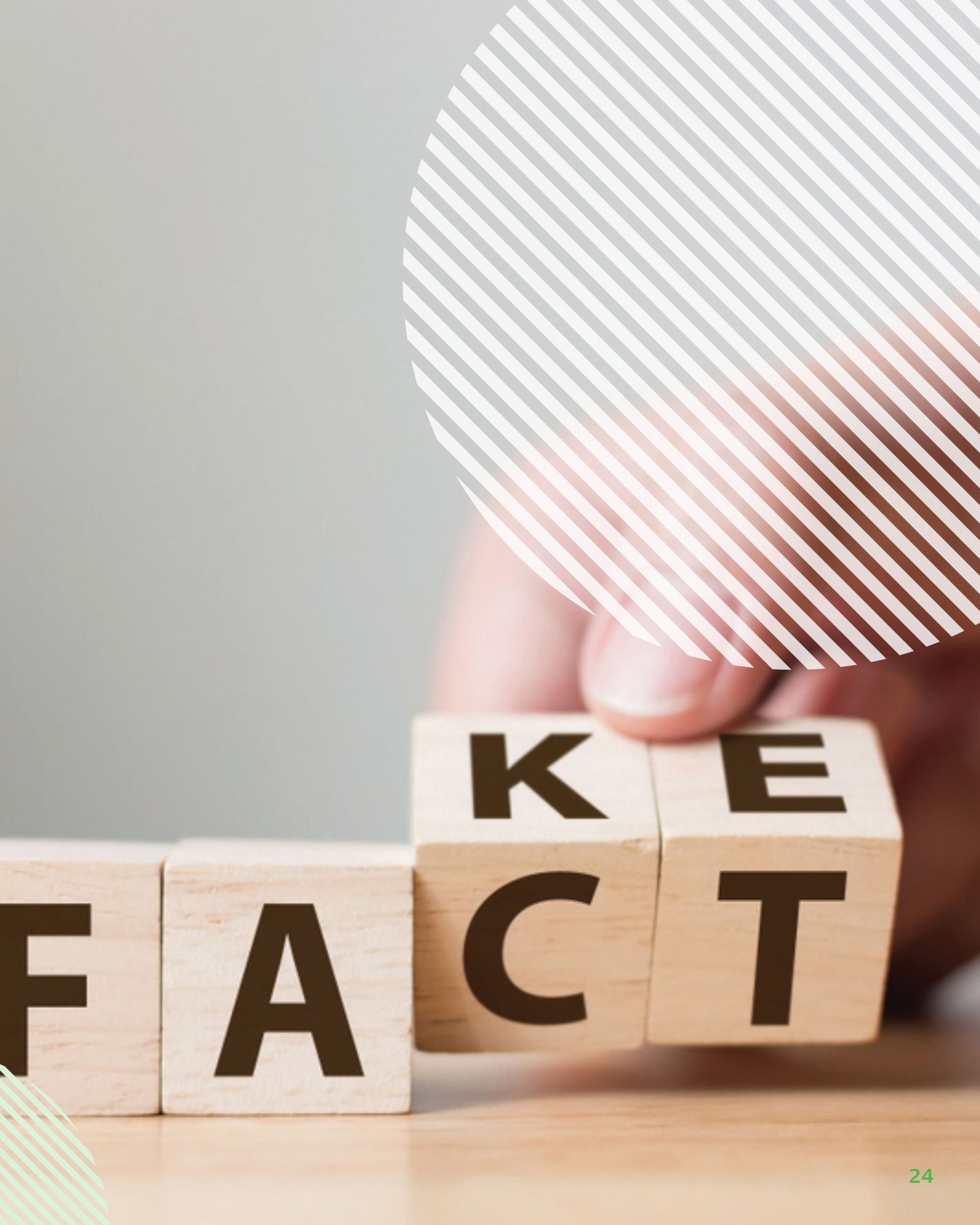
- Les plateformes doivent employer davantage de locuteurs de langues locales, sensibles au contexte culturel des régions où ils opèrent.

- Afin de prévenir la diffusion virale des messages malveillants, des systèmes d'alerte précoce doivent permettre une intervention humaine afin de détecter les comptes et publications représentant une menace potentielle pour la bonne tenue des élections. Les contenus qui atteignent un certain degré de viralité devraient être modérés et examinés par des intervenants humains.

Recommandation 13

Les plateformes de réseaux sociaux devraient former une coalition visant à combattre les menaces numériques à l'encontre de la démocratie et de l'intégrité électorale, à l'instar des mesures prises pour lutter contre le terrorisme et l'exploitation des enfants. Les membres de la coalition se réuniraient à intervalles réguliers et élaboreraient des stratégies trans-plateformes pour détecter et limiter la portée de la désinformation et des discours de haine.




FAKE
FACT

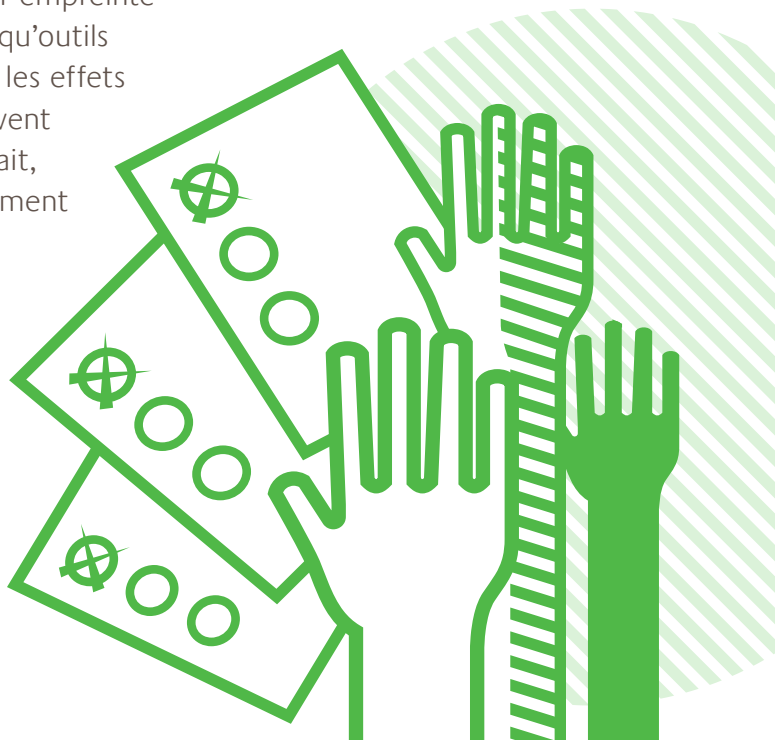
I. LES ÉLECTIONS : UN PILIER DE LA LUTTE POUR LA DÉMOCRATIE

Les technologies de communication numériques donnent – à ceux qui exploitent les failles de nos démocraties – les outils pour saper la tenue des élections et des délibérations démocratiques. Des partis, des candidats, des conseillers en campagnes politiques et des gouvernements étrangers ont transformé les réseaux sociaux en armes de désinformation et d'incitation à la haine et à la violence, ou encore en instruments d'ingérence dans les élections nationales et étrangères. Dans un contexte mondial caractérisé par une polarisation et une méfiance croissantes, les élections sont désormais aux avant-postes de la lutte pour la démocratie.

Les propriétés des nouvelles technologies de l'information et de la communication (viralité, vélocité, anonymat, regroupement en communautés d'intérêts et portée transnationale) engendrent des défis inédits pour la démocratie, qui ont gagné le monde entier[1]. Avant que l'élection présidentielle américaine de 2016 se trouve sous le feu des projecteurs (avec son cortège de bots politiques et de trolls russes amplifiant la désinformation afin de semer la méfiance et d'affaiblir certains candidats), les mêmes tactiques avaient été élaborées, affinées et utilisées au Kenya, aux Philippines et au Nigéria, entre autres. Plusieurs années avant de s'attaquer aux États-Unis et au Royaume-Uni, des cabinets de conseil peu scrupuleux comme Cambridge Analytica ont déployé des tactiques de guerre de l'information en contexte électoral en Afrique, en Asie et en Amérique latine. De la même manière, des partis politiques et des candidats se sont servis des réseaux sociaux pour nourrir le sentiment nationaliste, prêchant la haine et l'intolérance, et imposer leur projet politique périphérique dans les débats dominants. Cependant, les recherches actuelles suggèrent que les effets de ces

technologies ne constituent pas un bloc monolithique et qu'ils ne sont pas tous négatifs. Les technologies numériques peuvent indéniablement exacerber le chaos politique dans les pays où sévissent déjà la polarisation et la méfiance. Comme le conclut notre analyse sur la démocratie et les réseaux sociaux en Amérique latine, ces derniers « amplifient des schémas préexistants davantage qu'ils n'en créent de nouveaux »[2]. Les travaux consacrés à l'Afrique et à l'Amérique latine ont également mis en lumière des effets positifs incrémentiels sur l'engagement politique tels que l'augmentation de la participation aux scrutins, l'adhésion à des mouvements sociaux et la coordination de l'action politique[3]. En Afrique, les plateformes numériques constituent de puissants catalyseurs pour la multiplication des mouvements sociaux. Ce sont des vecteurs importants, voire fondamentaux, du dialogue politique, du partage d'informations et du débat démocratique[4].

Alors que les réseaux sociaux marquent de leur empreinte la vie politique du XXIe siècle, à la fois en tant qu'outils de campagne et plateformes de débat public, les effets de la technologie sur l'intégrité électorale doivent faire l'objet d'un examen tout particulier. De fait, les technologies numériques affectent directement la manière dont les citoyens participent à la démocratie et les élections constituent des périodes cruciales pendant lesquelles ils sont particulièrement attentifs au discours public. Les élections sont des tests à nul autre pareils de la légitimité démocratique et la perception de leur intégrité peut avoir des effets considérables sur la stabilité et la performance démocratiques.



Nous avons pour mission d'identifier les défis que présentent les nouvelles TIC pour l'intégrité électorale et d'élaborer des politiques mettant en avant les perspectives offertes par les technologies numériques en matière de renforcement de l'intégrité électorale, tout en atténuant les risques engendrés par l'innovation technologique. L'intégrité électorale est définie comme suit : « Toute élection reposant sur les principes démocratiques de suffrage universel et d'égalité politique tels qu'ils figurent dans les normes et accords internationaux, et menée de façon professionnelle, impartiale et transparente dans sa préparation et dans sa gestion, tout au long du cycle électoral »[5]. Nos travaux s'intéressent non seulement à l'impact potentiel des réseaux sociaux sur la conduite d'une élection, mais aussi à leur impact sur la *perception de l'intégrité d'une élection*. Comme l'observe une ONG : « Si les électeurs et les candidats croient qu'une élection est frauduleuse ou défaillante dans son organisation, ils n'en accepteront pas le résultat. Au mieux, cela se traduira par le mécontentement ou le désintérêt du public, au pire par la violence, une gouvernance inefficace et une instabilité à long terme »[6].

Deux des composantes de l'intégrité électorale auxquelles nous prêtons une attention particulière sont les suivantes : le contexte dans lequel les élections se déroulent d'une part, et la mesure dans laquelle les participants (candidats, partis et partisans) se sentent mutuellement en sécurité d'autre part[7]. L'intégrité électorale requiert l'assurance des citoyens quant à la régularité et la tenue des élections sur le long terme. Dans de nombreuses proto-démocraties, les candidats craignent d'être définitivement écartés du pouvoir s'ils perdent une élection. Les candidats, les partis et leurs partisans doivent être assurés i) que la perte d'une élection ne les empêchera pas d'en organiser d'autres et de s'y présenter et ii) que les gagnants ne seront pas en position d'user de leur pouvoir pour les priver de leurs droits. Ils doivent également être convaincus que s'ils remportent une élection, ils pourront former un gouvernement et appliquer leur programme politique et que les perdants ne recourront pas à la violence et ne feront pas obstruction à leur mandat électoral.

Les TIC – notamment les réseaux sociaux – présentent des risques potentiels pour l'intégrité électorale (polarisation, discours de haine, désinformation, nouvelles formes de publicité à visée politique et ingérences étrangères) que nous aborderons successivement. Bien que nous orientions notre action sur nombre de défis que présentent les TIC en matière d'intégrité électorale, les diverses consultations que nous avons menées dans le monde ont fait apparaître deux préoccupations principales concernant la gouvernabilité démocratique.

Premièrement, de l'Europe à l'Amérique latine, les législateurs ont fait valoir que la rapidité et l'ubiquité des réseaux sociaux poussent à réagir immédiatement aux demandes, aux nouvelles, aux doléances et aux accusations et fragilisent le mandat des parlements pour délibérer et définir l'agenda politique. Certains parlementaires ont le sentiment que la nature même de la représentation politique se délite en raison de l'intense mobilisation de l'opinion en ligne et de la propension des militants des réseaux sociaux à passer à la loupe la vie quotidienne des élus. Dans certains pays, la toxicité des attaques personnelles et des menaces en ligne a conduit certains députés à quitter la vie politique – les femmes étant concernées de façon disproportionnée. Bien que les effets des réseaux sociaux sur la qualité de la gouvernance démocratique dépassent le cadre de notre mandat, nous pensons que ce problème mérite d'être étudié de plus près.

Deuxièmement, nos interlocuteurs ont exprimé de façon réitérée leurs inquiétudes quant à la capacité de la démocratie à survivre dans un monde où l'infox règne et où les citoyens ne parviennent pas à se mettre d'accord sur les fondamentaux. S'il n'est pas exclu que la qualité de la délibération politique ait décliné dans certaines démocraties historiques, il convient de noter que les critiques contemporaines sur les manquements relatifs aux processus délibératifs sont antérieures à l'essor d'Internet[8]. Et tout comme les fausses informations et les discours de haine existent depuis des siècles, les citoyens des démocraties n'ont jamais eu une lecture unanime des événements et ne se sont jamais entendus sur la définition même des faits, quelle que soit

l'époque étudiée. Ils sont souvent en désaccord sur les fondamentaux et ne votent certainement pas sur la base de vérités communes[9]. La démocratie est précisément nécessaire parce que les citoyens sont en désaccord sur les fondamentaux. Même à l'ère numérique, la démocratie procure plusieurs avantages que le totalitarisme ne saurait apporter dans des conditions dignes de ce nom : protection des droits et des libertés, accès aux informations, plateformes d'interaction entre les citoyens et possibilité de débattre sur des sujets cruciaux.

D'un point de vue normatif, nous convenons que la qualité de la démocratie sort renforcée lorsqu'un consensus citoyen est atteint sur la nature et la véracité des faits. À ce titre, nous devrions nous attacher à améliorer les processus de délibération démocratique.

II. POLARISATION AFFECTIVE, RÉSEAUX SOCIAUX ET INTÉGRITÉ ÉLECTORALE

La polarisation met de plus en plus en danger la gouvernabilité, la cohésion sociale et les fondements de la démocratie à proprement parler. Le présent rapport s'intéresse principalement à l'une de ses multiples dimensions, à savoir la polarisation affective, laquelle conduit les sympathisants politiques, par esprit partisan, à entretenir des opinions et des convictions négatives à l'encontre de leurs adversaires. Lorsque la polarisation affective atteint un stade sévère, « les gens perçoivent et décrivent de plus en plus souvent la vie politique et la société selon la dichotomie nous/eux »[10], ce qui peut avoir des conséquences préjudiciables sur l'intégrité électorale. Comme l'affirme un rapport annuel sur la démocratie : « Les élites politiques et leurs partisans qui ne considèrent plus leurs adversaires politiques comme légitimes et dignes d'un égal respect – voire qu'ils rejettent leur propre famille ou cercle d'amis – risquent de moins respecter les règles démocratiques régissant la course au pouvoir »[11].

Aux États-Unis, la polarisation gagne régulièrement du terrain depuis les années 1970[12]. Avant la généralisation d'Internet, l'invention des smartphones et l'ascension des réseaux sociaux, la polarisation politique était attisée par les médias traditionnels partisans[13]. L'ouverture des chaînes d'actualité sur le câble dans les années 1980, la fin du principe d'impartialité acté en 1987 et l'émergence des stations de radio diffusant des messages de haine ont donné naissance à un écosystème médiatique extrémiste, particulièrement méfiant à l'égard des médias traditionnels et ouvert aux théories conspirationnistes et à la propagande[14]. Cet écosystème est devenu le lieu des pires excès de la désinformation et de l'incitation à la haine sur Internet, ainsi qu'une plateforme pour pléthore de personnalités politiques, experts et autres journalistes irresponsables[15].

L'exemple des États-Unis suggère que les pays où préexistent certaines conditions (polarisation, méfiance envers les médias traditionnels et

écosystèmes médiatiques partisans) sont beaucoup plus vulnérables aux manipulations sur les réseaux sociaux que ceux où la polarisation et la méfiance sont faibles[16]. Si la polarisation est déjà forte, il est facile de transformer les réseaux sociaux en instruments d'exacerbation et d'intensification des divisions et des conflits politiques. Lorsque les médias traditionnels inspirent peu confiance, les citoyens se détournent des organes d'informations objectifs. Les médias résolument partisans flattent les pires instincts de leur lectorat. Ce constat incite à ne pas généraliser imprudemment les effets des réseaux sociaux dans des pays dont les institutions, les divisions sociales et les écosystèmes médiatiques diffèrent considérablement.

D'une certaine façon, le niveau de polarisation, d'allégeance partisane des médias et de méfiance constaté aux États-Unis fait de ce pays un exemple extrême parmi les démocraties historiques[17]. Une étude récente a proposé de quantifier la polarisation affective en évaluant dans quelle mesure « le débat public est respectueux et factuel [et] les adversaires sont ouverts aux arguments adverses en faisant usage de leur raison ». L'enquête a classé les États-Unis au 98e rang sur 178, un score plus proche de celui de l'Inde (102e), de la Pologne (109e), du Brésil (117e) et de la Hongrie (127e) que des démocraties historiques telles que la Norvège (1er), la Suisse (2e) ou le Danemark (3e)[18].

Les démocraties du reste du monde livrent une image mitigée. De nombreuses démocraties d'Asie, d'Amérique latine et d'Afrique

atteignent les scores les plus élevés en termes de polarisation affective, mais quelques-unes des progressions les plus importantes ont été relevées en Europe occidentale. Des études empiriques indiquent que la polarisation et la méfiance observées dans divers pays à l'échelle internationale ne sont pas des phénomènes nouveaux mais plutôt le produit de tendances à long terme antérieures à l'arrivée des réseaux sociaux[19].

Alors que la polarisation politique a augmenté dans certaines démocraties, la confiance des citoyens envers leurs semblables, les médias et les parlements ou le corps législatif est généralement sur le déclin[20]. Dans la plupart des pays, on observe un recul régulier de la confiance que les gens éprouvent les uns envers les autres. En Europe, mais aussi en Amérique centrale, du Sud et du Nord, on constate en outre un déclin progressif du pourcentage de citoyens exprimant « une grande confiance » dans les médias. L'Afrique présente le déclin global le plus important et la plus forte volatilité. L'Asie-Océanie est la seule région où la confiance dans la presse a enregistré une nette augmentation au cours des trois décennies écoulées.

La confiance des citoyens dans le parlement s'est elle aussi délitée, mais avec davantage de variabilité. En Amérique du Nord, en Europe, en Amérique centrale et latine ainsi qu'en Afrique, le pourcentage de citoyens exprimant « une grande confiance » dans leur corps législatif a baissé en 30 ans. La seule région à faire exception est l'Asie-Océanie, où il a connu une légère augmentation globale entre le début des années 1980 et la période de l'enquête (2010-2014). La perte de confiance au fil du temps est moins due à des critères générationnels qu'au jugement que portent les citoyens sur les actions du gouvernement et leur fiabilité. Ce constat suggère que lorsque les démocraties tiennent leurs promesses, les citoyens réagissent positivement[21]. L'accroissement de la polarisation politique et le déclin de la confiance menacent l'intégrité électorale. La polarisation politique et la méfiance conduisent à douter de la sécurité mutuelle. Lorsque le doute s'installe, la désinformation organisée et les discours de haine en ligne peuvent empoisonner les campagnes électorales. La peur peut s'emparer des électeurs, convaincus qu'une défaite de leur parti à

court terme se perpétuera *ad vitam aeternam*. Le but des élections se limite alors à la victoire à tout prix, au mépris des règles, des lois, de l'éthique ou des normes démocratiques.

De nombreuses proto-démocraties du Sud se caractérisent par une polarisation élevée, une faible confiance et la présence de médias partisans, qui les rendent très vulnérables à la diffusion de la désinformation et des discours de haine en ligne. Dans ces pays, les élections constituent déjà des vecteurs de violence et de déstabilisation ; les réseaux sociaux y sont des instruments d'intensification de la polarisation et d'affaiblissement des normes de sécurité mutuelle nécessaires à un déroulement intègre des élections. Cette tendance non seulement se poursuivra, mais risque de monter en puissance.

La conclusion selon laquelle les pays à forte polarisation sont plus vulnérables à l'instrumentalisation des réseaux sociaux n'exonère en aucune façon les plateformes de leur responsabilité quant aux effets pernicieux de leurs produits. Elles se sont empressées de les proposer dans des pays tels que le Myanmar, Sri Lanka et le Kenya, particulièrement exposés à la désinformation, à la propagande et aux discours de haine. Elles n'ont pas cherché à anticiper les modalités d'utilisation de leurs outils dans des pays extrêmement polarisés avec des antécédents de violence. Une fois conscientes des conséquences en pertes humaines potentielles, elles ont commencé à y remédier, sans prendre pour autant la mesure de l'urgence.

Les causes de la polarisation à long terme sont complexes et très diverses. Un nombre croissant de publications attribuent la cause de la polarisation à la progression régulière des inégalités économiques[22] et au soutien croissant dont bénéficient les courants politiques extrémistes[23]. D'autres travaux suggèrent que les systèmes électoraux jouent un rôle et que les démocraties à système majoritaire uninominal sont les plus enclines à une extrême polarisation[24]. D'autres auteurs

mettent en avant l'inquiétude grandissante exprimée par les populations rurales et les travailleurs agricoles dont le statut les mettrait au ban de la croissance et du dynamisme des villes, phénomène auquel il faut ajouter les migrations, perçues par ces derniers comme une menace[25]. Plusieurs recommandations découlant de l'analyse causale sont envisageables : mettre en œuvre des politiques sociales et économiques qui protègent la classe moyenne et le droit du travail[26], instaurer des réformes politiques qui limitent les jeux à somme nulle (que cette réalité soit avérée ou simplement perçue)[27] et créer des plateformes sociales collectives favorisant les interactions et les délibérations, tout en incitant les citoyens à s'engager dans des causes politiques dépassant le cadre de leurs revendications particulières[28]. La formulation de recommandations sur les approches optimales en matière de prévention de la polarisation extrême n'est pas du ressort de la présente Commission. En revanche, nous essayons de dessiner à grands traits les contours d'une possible approche à même d'immuniser les sociétés contre les distorsions véhiculées par les réseaux sociaux.

RÉSEAUX SOCIAUX ET POLARISATION

L'importance d'Internet et des réseaux sociaux en tant que plateformes de consommation de nouvelles et d'informations suscite des inquiétudes croissantes quant aux risques d'exacerbation et d'aggravation de la polarisation favorisés par la technologie. À l'orée même d'Internet, certains chercheurs ont avancé que les réseaux sociaux engendreraient des bulles de filtrage et des chambres d'écho dans lesquelles s'isoleraient les citoyens, lesquels liraient les mêmes nouvelles,

ne communiqueraient qu'en vase clos et penseraient en conséquence selon les mêmes schémas, avec des effets délétères sur les modalités de la gouvernance démocratique[29]. Le filtrage algorithmique, individuel et social des contenus peut, quant à lui, influer sur la nature des informations auxquelles chaque personne est exposée. Les observateurs critiques suggèrent désormais que les électeurs qui passent leur temps à naviguer sur la toile risquent de ne pas avoir accès à un éventail de nouvelles et d'informations représentatif, équilibré ou exact et que les informations de qualité ne sont vraisemblablement pas diffusées de façon équitable au sein d'un électorat donné. De la même manière, certains journalistes affirment que les algorithmes radicalisent des pans importants de la population en leur proposant des contenus incitant à adopter des positions extrêmes. Une étude des médias menée récemment suggère que les algorithmes des réseaux sociaux comportent des biais qui poussent les utilisateurs vers des contenus extrémistes. Mentionnons à ce propos le moteur de recherche Google qui attribue aux sites négationnistes un rang supérieur à celui des sources d'information légitimes sur l'histoire de la Shoah[30]. Les fonctions de visionnage automatique de YouTube recommandant des contenus de plus en plus radicaux illustrent également ce phénomène[31].

Cependant, les études consacrées à cette question n'ont pas livré de résultats concluants pour deux raisons. Premièrement, il est difficile d'opérer la distinction entre les utilisateurs qui tendent à s'associer de leur plein gré avec des personnes et des sources de nouvelles qui renforcent leurs opinions politiques et leur vision du monde et ceux qui suivent des contenus qu'ils n'auraient pas choisis eux-mêmes mais que les algorithmes leur proposent par le biais de flux d'informations et de recommandations. Deuxièmement, les plateformes n'ont pas transmis aux chercheurs des données susceptibles de répondre à la question.

Des études suggèrent que les réseaux sociaux promeuvent en fait la diversité médiatique et l'accès à divers points de vue politiques et sources d'information, notamment par rapport aux sources

traditionnelles[32]. De la même manière, les plateformes offrent davantage de possibilités d'interactions transversales puisqu'elles connectent les individus à leur famille et à leurs amis proches, mais aussi à des parents éloignés, des collègues de travail ou de simples connaissances – des relations considérées comme des « liens faibles », plus susceptibles de publier ou de partager des contenus idéologiquement divers[33]. Grâce à cette dynamique, il n'est pas exclu que les plateformes de réseaux sociaux élargissent l'éventail d'opinions politiques auquel les utilisateurs sont exposés.

Dans le même temps, certaines personnes semblent répondre à la théorie de la chambre d'écho, tandis que d'autres y dérogent.

Une étude consacrée à l'Allemagne, à l'Espagne et aux États-Unis révèle que les utilisateurs de Twitter au sein de réseaux hétérogènes développent souvent des réseaux plus modérés politiquement au fil du temps, ce qui suggère que les personnes prédisposées à diversifier leurs sources d'information continuent à le faire dans leurs interactions en ligne[34]. D'un autre côté, des travaux récents suggèrent que les partisans exposés au point de vue de leurs adversaires sur les réseaux sociaux se polarisent davantage[35].

De toute évidence, certaines personnes se radicalisent sur Internet, justifiant les ressources conséquentes que les plateformes ont consacrées à la lutte contre l'enrôlement terroriste en ligne. Cependant en matière d'extrémisme politique, la question est de savoir si la radicalisation est le fait des algorithmes des plateformes. Il existe peu d'études rigoureuses sur les algorithmes de recommandation et les chercheurs ne parviennent pas aux mêmes conclusions : une étude a pointé du doigt un léger biais en faveur de la promotion de vidéos de plus en plus radicales dans l'algorithme de YouTube[36], alors qu'une autre suggère que le volume de vidéos extrémistes n'a progressé qu'en réponse à la demande et non du fait d'un biais algorithmique attirant les internautes vers les contenus plus radicaux[37].

ACTIONS À ENVISAGER

Afin d'élaborer des politiques efficaces qui limitent les risques, les décideurs ont besoin de s'appuyer sur un corpus significatif. Le volume limité de données mises à la disposition des chercheurs qualifiés par les plateformes constitue le principal obstacle à la compréhension de l'impact des réseaux sociaux sur la diversité des opinions ou la radicalisation des points de vue. La grande majorité des études existantes à ce jour portent sur les États-Unis et l'Europe. Les données communiquées par les plateformes sur l'Afrique, l'Asie et l'Amérique latine sont restreintes. En outre, nous disposons de peu de données sur des plateformes beaucoup plus présentes dans les pays du Sud telles que WhatsApp. Concernant des questions essentielles comme la radicalisation par l'intermédiaire de YouTube, l'impossibilité pour les chercheurs externes d'accéder à l'algorithme de recommandation ne permet pas d'évaluer si les résultats ont changé après les modifications apportées au cours de l'année passée.

Afin d'étudier les pathologies attribuées à la transformation de l'écosystème médiatique numérique, les chercheurs en sciences sociales doivent accéder à des données contrôlées par les plateformes pour connaître le profil des utilisateurs, ainsi que la nature et la fréquence de leur implication. Les chercheurs ont besoin de comprendre comment et quand la population (à différents échelons) interagit avec les nouveaux médias dans différents pays. Ils doivent également étudier les conséquences de ces interactions. Les plateformes qui se sont engagées à mettre leurs données à la disposition des chercheurs universitaires indépendants ont rarement tenu promesse[38].

Les pouvoirs publics doivent obliger les grandes plateformes Internet à communiquer à des tiers indépendants des données pertinentes concernant l'impact des réseaux sociaux sur la démocratie. Ces plateformes doivent notamment communiquer des données sécurisées (et respectant les règles de confidentialité) à des institutions universitaires certifiées afin qu'elles étudient les questions suivantes : existence éventuelle de biais favorables aux opinions extrémistes dans les algorithmes, impact des réseaux sociaux sur la polarisation politique et la consommation d'informations, décryptage de la corrélation entre discours de haine en ligne et violence hors ligne, etc.

Compte tenu du nombre élevé d'élections organisées chaque année dans le monde et de la sensibilité variable des pays aux phénomènes de polarisation néfaste, à la désinformation et aux discours de haine, la communauté internationale en faveur de l'intégrité électorale collaborant avec les plateformes aurait tout intérêt à déterminer les pays nécessitant une attention prioritaire et des ressources accrues pour protéger leur intégrité électorale.

Il conviendrait que la communauté en faveur de l'intégrité électorale investisse dans la création d'un indice de vulnérabilité électorale déterminant les élections à surveiller étroitement afin d'éviter une potentielle ingérence électorale, des comportements en ligne usurpateurs coordonnés, mais aussi la mésinformation et la désinformation.

III. DISCOURS DE HAINE ET INTÉGRITÉ ÉLECTORALE

Internet facilite la coordination et l'action collective de différents groupes, notamment d'extrémistes géographiquement dispersés. Gab, 4chan, 8chan et des subreddits ouvertement racistes sont devenus des forums populaires de discussion, de construction d'une identité commune et de mobilisation prisés de certains groupes marginaux. L'anonymat pratiqué sur ces réseaux contribue à faciliter la tenue de propos insultants et haineux sans que leurs auteurs n'aient à en assumer la responsabilité. La prolifération de ces propos échappant à la responsabilité juridique soulève des inquiétudes quant à la relation entre réseaux sociaux et nouvelles vagues d'extrémisme politique ainsi qu'entre réseaux sociaux et violence politique.

Ces dernières années, les liens entre discours de haine en ligne et harcèlement hors ligne sont devenus plus apparents. Dans plusieurs démocraties occidentales, des suprémacistes blancs ont divulgué sur les réseaux sociaux la perpétration de tueries de masse ciblant des minorités religieuses ou raciales[39]. En Inde, des rumeurs répandues sur WhatsApp ont incité à des lynchages et violences communautaires, se soldant par le décès de dizaines de personnes[40]. Au Sri Lanka, en mars 2018, des messages hostiles à l'islam ont alimenté des violences contre la population musulmane minoritaire, provoquant la mise à feu de plusieurs centaines de maisons et d'entreprises[41]. Au Myanmar, des agents gouvernementaux ont inondé Facebook de propos anti-musulmans et appelé à la purification ethnique en ciblant la minorité Rohingya, contribuant au déplacement de 700 000 réfugiés du fait de l'augmentation des menaces, des attaques physiques et des agressions sexuelles[42]. Le risque d'amplification des discours de haine sur les réseaux sociaux est notamment important dans les pays du Sud, où la juxtaposition de tensions ethniques ou religieuses anciennes et l'adoption rapide des nouvelles technologies de l'information sont à même d'intensifier les conflits politiques.

Les femmes sont notamment la cible de la haine en ligne. Selon un récent sondage commandé par Amnesty International, près qu'un quart (23 %) des femmes de huit démocraties déclarent avoir été victimes d'insultes ou de harcèlement en ligne au moins une fois dans leur vie[43]. De la même manière, le Parlement européen a découvert qu'un cinquième des femmes de l'Union européenne (UE) avaient subi du harcèlement sexuel en ligne[44]. L'intimidation en ligne fondée sur le genre peut s'avérer un puissant outil d'autocensure propre à entraver la liberté d'expression et à perturber la participation des groupes ciblés à la vie démocratique[45]. Selon Amnesty International, la plupart des femmes victimes d'abus en ligne ont changé leur mode d'utilisation des réseaux sociaux : modification de leurs paramètres de confidentialité et changement des contenus publiés[46] **[Encadré 1]**. L'effet démobilisateur des abus commis peut être particulièrement fort pour les femmes journalistes et les femmes politiques.

ENCADRÉ 1

Les réseaux sociaux, une arme contre les femmes

Les réseaux sociaux sont de plus en plus utilisés pour menacer de viol et de violence les femmes journalistes, militantes et politiques. La désinformation sert également à décrédibiliser et à remettre en cause les capacités des femmes occupant le devant de la scène politique démocratique. Ainsi, lorsque Maria Ressa, une journaliste philippine de premier plan, a commencé à couvrir le recours à la propagande par le Président Rodrigo Duterte dans la campagne électorale de 2016 aux Philippines, celui-ci, pour l'intimider, a orchestré une campagne en ligne de menaces, de harcèlement ciblé et d'allégations de corruption[47]. Après la publication sur Rappler, un site web d'information très populaire, de la transcription d'un entretien téléphonique entre le Président Trump et le Président Duterte, un réseau coordonné de bots et de faux comptes a inondé les réseaux sociaux avec le hashtag #ArrestMariaRessa, faisant de la journaliste la cible de messages de haine et de menaces ininterrompus, dont un appel à la « violer jusqu'à ce que mort s'ensuive »[48].

L'expérience de ce trolling d'État vécue par Mme Ressa est à l'image de plusieurs campagnes menées contre des femmes éminentes dans le monde. Après son intervention aux Nations Unies dénonçant l'impact du conflit au Donbass sur les femmes ukrainiennes, la députée ukrainienne Svitlana Zalishchuk a été la cible d'une campagne de désinformation soutenue par les autorités russes qui a abouti à la diffusion d'un faux tweet usurpant son identité et affirmant qu'elle « courrait nue dans les rues de Kiev si l'armée ukrainienne perdait une bataille décisive »[49]. Des images truquées la représentant dans le plus simple appareil ont circulé sur les réseaux sociaux afin de continuer à la discréditer et à la déshonorer.

Ces attaques ciblées entachent la réputation des femmes et recourent à l'intimidation pour les empêcher de s'exprimer et de participer à la vie politique. Les attaques contre les femmes durent souvent beaucoup plus longtemps que d'autres formes de trolls et utilisent des insultes dégradantes et sexualisées qui les rendent encore plus pernicieuses et tenaces. Les tactiques de cyberintimidation fondées sur le genre peuvent sérieusement entraver la liberté d'expression et perturber la participation des femmes à la vie politique en ligne et hors ligne[50].

Les discours de haine menacent l'intégrité électorale dans le sens où ils affaiblissent la sécurité mutuelle nécessaire à la contestation pacifique. Ils constituent autant d'armes pour les candidats et les partis qui attisent la violence afin d'empêcher leurs adversaires de voter. Leur fréquence est particulièrement inquiétante dans les proto-démocraties du Sud qui connaissent des antécédents de violence électorale et pâtissent d'un état de droit défaillant, inapte à demander des comptes aux délinquants.

APPROCHES DE RÉGLEMENTATION DES DISCOURS DE HAINE

La quasi-impossibilité de définir le discours de haine et de le distinguer d'autres cas de propos injurieux en complique sérieusement la modération en ligne. Même lorsque les plateformes en élaborent une définition de travail, la complexité et les variantes de la langue usuelle rendent la tâche de détection automatique du discours de haine imprécise et protéiforme. Bien que les leaders du secteur high-tech et les décideurs conviennent en général qu'il faudrait en faire davantage pour lutter contre les discours de haine, ils ne sont pas au diapason s'agissant des mesures à prendre, compte tenu de ces difficultés de conceptualisation et de mise en œuvre. Il est particulièrement difficile d'opérer la distinction entre le discours de haine et le discours politique légitime lorsque les dirigeants politiques jouent sur les mots, voire assument une parole raciste, laquelle doit être combattue par les plateformes, comme le rappellent les observateurs critiques.

Les débats sur l'équilibre entre liberté d'expression et protection des individus contre la discrimination ne datent pas d'hier. En revanche, la modération du discours de haine à l'ère du numérique est compliquée

par le cadre extra-juridictionnel dont jouissent les plateformes. Les multiples modèles régionaux qui ont vu le jour en réponse à cette situation procèdent tous à un arbitrage inhérent entre protection de la liberté d'expression et régulation des discours susceptibles de justifier la haine et la violence à l'encontre de certains groupes ou d'y inciter.

Le modèle de l'autorégulation domine aux États-Unis, où le Premier amendement protège juridiquement les discours de haine[51] et où les plateformes de réseaux sociaux sont exemptées de toute responsabilité juridique, hormis concernant la propriété intellectuelle et les crimes et délits fédéraux[52]. Cependant, les sociétés technologiques ont pris plusieurs mesures pour limiter la propagation des contenus haineux, notamment l'interdiction de certains comptes, la suppression et la rétrogradation de certains contenus ou encore la dilution des idées extrémistes en contre-balançant les informations par d'autres sources grâce, à la fois, de l'intelligence artificielle et de la modération humaine. L'autorégulation a des limites : les modérateurs de la Silicon Valley ne possèdent pas nécessairement les connaissances culturelles, politiques ou religieuses approfondies requises pour examiner les contenus publiés de l'autre côté du globe[53] et les modalités de mise en œuvre des décisions techniques et politiques se caractérisent par une faible transparence ou l'absence de responsabilisation juridique[54].

L'Union européenne a, quant à elle, élaboré un modèle réglementaire plus strict. Dans le cadre du droit européen préexistant, les plateformes avaient déjà l'obligation de retirer tout contenu illégal, discours de haine compris, sur notification. En 2016, la Commission européenne créait le Code de conduite visant à combattre les discours de haine au titre duquel Facebook, Microsoft, Twitter et YouTube ont accepté d'incorporer des interdictions en la matière dans leurs Règles de la communauté. Ce texte octroie aux Règles de la communauté des plateformes technologiques une fonction officielle de retrait des discours de haine telle que définie par le droit européen et fixe des délais spécifiques d'intervention après notification. En 2018, Instagram, Google+ et Snapchat ont également signé ce document[55]. Cette initiative est faiblement interventionniste

dans la mesure où elle ne confère pas à un régulateur la tâche de supprimer les contenus. Les organisations européennes de défense des libertés publiques ont reproché à ce cadre de ne pas fixer de responsabilités et de laisser carte blanche à des sociétés privées[56]. Bien que le Code de conduite de la Commission ait suscité des espoirs quant à sa capacité à bâtir des réseaux d'information fondés sur un sentiment de confiance entre le secteur technologique, la société civile et les gouvernements, les réactions mitigées ont vite pris le pas.

Avec la loi NetzDG de 2017, l'Allemagne s'est orientée vers une réglementation gouvernementale plus directe. Afin de protéger les utilisateurs allemands de réseaux sociaux contre les discours de haine et le harcèlement, ce texte confère aux sociétés de réseaux sociaux la responsabilité de traiter les plaintes des utilisateurs dans un délai raisonnable[57]. Elles encourent des amendes pouvant atteindre 50 millions d'euros en cas de non-retrait d'un contenu « clairement » illégal dans les 24 heures suivant notification[58]. Cependant, ce court délai ne permet pas aux plateformes d'examiner le contenu incriminé dans son contexte politico-culturel et incite à un retrait global à l'emporte-pièce susceptible de remettre en cause la liberté d'expression. En 2017, le Rapporteur spécial des Nations Unies pour la protection du droit à la liberté d'opinion a accusé cette loi d'inciter à la « censure de précaution » qui « interférerait avec le droit à chercher, recevoir et diffuser des informations de toute nature sur Internet »[59]. En outre, des gouvernements autoritaires appliquant une législation dont le mandat prendrait pour modèle la loi NetzDG pourraient ainsi légitimer un contrôle accru des informations[60] et fragiliser les normes internationales relatives aux droits de l'homme[61]. De fait, des lois identiques ont déjà été votées en Russie et au Venezuela, entre autres États autoritaires[62]. Dans des cas extrêmes, des gouvernements autoritaires coupent le réseau Internet pour contrôler les informations **[Encadré 2]**.

ENCADRÉ 2

Coupures du réseau Internet en Asie et en Afrique

Des gouvernements autoritaires d'Asie et d'Afrique continuent à recourir aux coupures du réseau Internet pour bâillonner la contestation politique. En 2015, des experts en droit international des Nations Unies, de l'OSCE, de l'OAS et de l'ACHPR (Commission africaine sur les droits de l'homme et des peuples) ont condamné les coupures, les accusant de porter gravement atteinte à la liberté d'expression et de restreindre l'accès aux informations et aux services d'urgence en période de troubles. Certaines figures politiques perpétuent une culture d'opposition à la liberté sur Internet en supprimant l'accès aux réseaux sociaux et aux forums en ligne dans les situations de crise[63].

Environ la moitié des coupures de réseau dans le monde, y compris les perturbations intentionnelles des réseaux sociaux, du service de téléphonie mobile et/ou de l'accès à Internet, se sont produites en Inde. Bien que le gouvernement indien ait recouru à cette méthode sous prétexte d'étouffer la violence pendant des périodes potentiellement conflictuelles au cours des dernières décennies, les coupures ont été liées à des actions collectives violentes et non violentes menées par des internautes[64].

Après les attentats à la bombe de Pâques 2019 au Sri Lanka, le gouvernement a bloqué l'accès aux sites des réseaux sociaux en prétextant la poursuite d'objectifs similaires. Bien que certains médias l'aient félicité d'avoir empêché la propagation des discours de haine, des analystes ont ultérieurement émis des critiques face à cette décision brutale. Dans un pays où les médias sont relativement affaiblis et sous liberté surveillée, l'arrêt des communications Internet a exacerbé le chaos et la confusion pendant la crise. En outre, des acteurs malveillants déterminés à répandre de fausses nouvelles et une rhétorique violente ont malgré tout pu déverser leurs propos haineux dans l'ensemble de la région par le biais de réseaux privés virtuels[65].

Les coupures du réseau Internet en Afrique ont augmenté ces dernières années. Plus d'une douzaine de pays africains, comme l'Égypte[66], le Togo et l'Éthiopie, ont subi des perturbations dans leur accès à Internet pendant la tenue d'élections ou lors de troubles politiques. Une étude portant sur 10 pays d'Afrique subsaharienne a conclu que les coupures s'étaient avérées à la fois dangereuses et coûteuses : entre 2015 et 2017, elles se sont soldées par une perte estimée à 235 millions de dollars US dans ces pays[67].

En Ouganda et au Bénin, les coupures se sont accompagnées d'une répression féroce de la part des autorités. Peu avant les élections de 2016 en Ouganda, la Commission électorale nationale a interrompu l'accès à Facebook, Twitter et d'autres forums similaires. Pendant la coupure, l'État a placé deux candidats à l'élection présidentielle en résidence surveillée et n'a rétabli le plein accès à Internet qu'à l'issue du scrutin. Les critiques ont avancé que cela avait permis au gouvernement de se protéger contre toute accusation d'ingérence dans les procédures électorales[68]. Au Bénin, pays réputé pour sa stabilité et sa viabilité démocratique, les autorités électorales ont également déclaré que des candidats issus de cinq partis d'opposition au Président Talon n'étaient pas habilités à se présenter aux élections parlementaires de 2019. Le gouvernement réprima les manifestations, resta sourd au tollé général, ferma certains sites de réseaux sociaux et finit par bloquer tout accès à Internet le jour de l'élection[69].

Ces exemples et bien d'autres illustrent les différentes menaces qui pèsent sur l'accès aux informations et sur les libertés électorales en Asie et en Afrique. Bien que les réseaux sociaux et d'autres forums de communication en ligne soulèvent des défis pour régulateurs, accroître le recours autoritaire aux coupures ne fait que renforcer la valeur potentielle de ces technologies aux yeux des militants pro-démocratie.

À noter qu'aucun de ces modèles ne propose un cadre de politique clair pour s'attaquer à la généralisation des discours de haine dans de nombreux pays ainsi qu'à leur présence croissante dans les débats politiques traditionnels et propos formulés par pléthore de leaders politiques. Les gouvernements doivent trouver une approche permettant aux plateformes de réagir à cette tendance sans s'ingérer dans les campagnes électorales ni créer de règlements partisans sur le type de discours politique devant être soumis à la censure.

ACTIONS À ENVISAGER

Les différents régimes de régulation s'appuient sur des principes distincts pour orienter le retrait des discours de haine des réseaux sociaux (s'agissant des modalités, du calendrier et du motif invoqué pour mettre en place les mesures appropriées). Cependant, tous exigent des plateformes technologiques qu'elles passent réellement à l'action pour adapter leurs pratiques à la taille de leur marché. Les solutions basées sur l'IA se heurtent encore à de nombreuses limites, surtout dans les pays du Sud et les zones où l'anglais n'est pas la langue principale. Parallèlement, les plateformes doivent appliquer les mêmes normes de modération des contenus partout dans le monde et faire preuve d'encore plus de réactivité lorsque des communautés vulnérables aux conflits ethniques, aux émeutes et aux crimes de haine sont concernées. Dans ces contextes, elles doivent consacrer des investissements conséquents à l'élaboration de systèmes d'alerte rapide qui signaleraient les contenus faisant peser un risque potentiel sur les élections ; ces derniers doivent alors être examinés par des intervenants humains avant qu'ils atteignent un certain niveau de viralité. Afin que les internautes jouissent de l'égalité des chances de participation au débat politique en ligne, les sociétés technologiques doivent allouer davantage de ressources à la modération automatique des contenus, à la traduction des textes, à la sensibilisation culturelle des modérateurs et à d'autres missions similaires. Elles doivent aussi fournir davantage de données sur les discours de haine présents sur leurs plateformes, et leur

degré de gravité. Si les rapports consacrés à la transparence fournissent des statistiques générales sur le nombre de retraits, une meilleure connaissance des types de contenus détectés et retirés permettrait non seulement d'améliorer les systèmes d'alerte précoce mais aussi d'éclairer la prise de décision factuelle concernant la protection des communautés plus vulnérables face aux discours de haine, au harcèlement et aux abus.

Les plateformes de réseaux sociaux doivent élaborer des systèmes d'alerte précoce prenant en compte la désinformation en rapport avec des élections, les ingérences étrangères, les crimes et délits motivés par la haine, les menaces proférées à l'encontre des femmes, la violence et les dissuasions à se rendre aux bureaux de vote.

Les plateformes doivent employer davantage de locuteurs de langues locales, sensibles au contexte culturel des régions où ils opèrent.

Afin de prévenir la diffusion virale des messages malveillants, des systèmes d'alerte précoce doivent permettre une intervention humaine afin de détecter les comptes et publications représentant une menace potentielle pour la bonne tenue des élections. Les contenus qui atteignent un certain degré de viralité devraient être modérés et examinés par des intervenants humains.

Les gouvernements doivent obliger les plateformes de réseaux sociaux à tenir à jour leurs comptes rendus sur la transparence afin de fournir au public des données sur le nombre de signalements de discours de haine et d'abus en ligne. Les données en question devraient porter, entre autres, sur les cas d'abus ciblés (selon des critères ethniques, de genre, d'orientation sexuelle ou d'affiliation religieuse) et la fréquence à laquelle ils visent différentes communautés.

La diversité du panel d'experts concevant les technologies d'examen des contenus constitue un défi majeur dans le cadre du renforcement du travail de modération. Les algorithmes, l'IA et les technologies connexes ne sont pas des outils neutres : ils intègrent les valeurs et les préjugés de leurs créateurs et de leurs utilisateurs. Un nombre croissant de travaux

empiriques expliquent comment les préjugés dont les responsables de sociétés technologiques font preuve dans le cadre de leur conception et de leurs pratiques peuvent conduire à des décisions automatiques incohérentes et souvent discriminatoires[70]. À ce propos, la majorité des ingénieurs qui imaginent les technologies dernière génération sont de jeunes hommes blancs basés dans la Silicon Valley. Une partie de la solution à long terme consistera à veiller à la diversité des milieux d'origine et des expériences des ingénieurs et des leaders du secteur. Cela nécessitera d'investir à long terme dans le renforcement de la diversité dans les domaines de l'informatique, de l'ingénierie et des données **[Encadré 3]**. Ces investissements à long terme renforceront l'intégrité électorale au sens large en conférant le pouvoir décisionnel en matière de conception des plateformes à un groupe d'experts représentatifs des caractéristiques démographiques et culturelles des consommateurs de réseaux sociaux.

Les pouvoirs publics, les organisations internationales, les fondations philanthropiques et la société civile doivent aider les démocraties dans l'élaboration de programmes technologiques civiques par le biais de l'enseignement du codage, notamment aux femmes et aux minorités, et de l'intégration de spécialistes techniques au sein des équipes gouvernementales.

Les citoyens, la société civile et les gouvernements peuvent aussi en faire davantage pour promouvoir un environnement en ligne sain et contribuer ainsi à élargir l'espace d'un débat politique respectueux et de qualité. Lors des élections de 2013 au Kenya, des organisations de la société civile ont déployé des efforts impressionnants pour limiter la prolifération des discours de haine en ligne. Grâce à la création d'un environnement permettant aux citoyens de contrer, discréditer et ridiculiser les auteurs de propos violents, elles ont réussi à réduire la prépondérance des discours de haine et à mettre en place un environnement électoral axé sur le dialogue non violent **[Encadré 4]**.

La communauté en faveur de l'intégrité électorale devrait financer les organisations de la société civile qui combattent les discours de haine, le harcèlement ciblé et l'incitation à la violence, notamment dans les périodes pré-électorales.

ENCADRÉ 3

Initiatives en faveur de la diversité dans le codage

L'intégrité électorale nécessite que les groupes marginalisés jouissent d'un accès égal à la participation politique. Cependant, les abus en ligne donnent aux populations vulnérables un sentiment d'insécurité, réduisent leur participation au débat politique en ligne et, dans les cas extrêmes, peuvent les empêcher de poursuivre leur carrière dans la politique ou le journalisme. Les outils actuels de conception des algorithmes et de modération des contenus ne parviennent pas à résoudre les préoccupations que soulèvent les discours de haine et le harcèlement. Une solution à long terme consiste à jouer la carte de la diversité chez les ingénieurs et les leaders technologiques qui développent les algorithmes et décident des contenus.

Ces dernières années, plusieurs organisations à but non lucratif se sont efforcées de créer diverses voies d'accès aux carrières technologiques. Ces initiatives contribueront à étendre le pouvoir décisionnel aux communautés marginalisées les plus concernées par les biais des algorithmes et les défaillances des systèmes de modération des contenus. Certaines sont des organisations de premier plan prônant une présence accrue des femmes dans le secteur technologique telles que Girls Who Code, le Grace Hopper Program et Women Techmakers ; certains programmes visent à promouvoir la participation des minorités (Black Girls Code, #YesWeCode et l'Algorithmic Justice League, etc.).

Un exemple de réussite notoire est Girls Who Code, une organisation à but non lucratif qui s'efforce d'augmenter le nombre de femmes travaillant dans l'informatique et l'ingénierie en proposant divers programmes de codage ciblés aux jeunes filles. L'organisation intervient en dehors des heures de classe pendant l'année scolaire et dispense des compétences en informatique, dont la programmation, la robotique, la conception web et le développement d'applications[71]. Selon son Rapport annuel 2018, les anciennes élèves du programme ont obtenu leur diplôme en choisissant une spécialisation en informatique dans des proportions inégalées (soit 15 fois le taux national)[72]. Ces initiatives de formation sont en train d'obtenir l'appui de sociétés technologiques majeures : Google, Twitter et GE font partie des parrains de Girls Who Code[73].

ENCADRÉ 4

Surveillance citoyenne des discours de haine au Kenya, 2012-2013

Les élections présidentielles de 2007 au Kenya ont déclenché deux mois de violence généralisée. Plus de 1 200 personnes ont été tuées et plus de 600 000 déplacées[74]. Des hypothèses non confirmées suggèrent que la prolifération des discours de haine en ligne a contribué à la manifestation de comportements violents[75].

Dans les mois précédant les élections de 2013, plus de 477 personnes ont été tuées lors de violences inter-communales dans un contexte de propos incendiaires sur fond de litiges fonciers. La Commission nationale sur la cohésion et l'intégration créée par le gouvernement après 2007 pour poursuivre en justice les auteurs de discours de haine, a peiné à définir ou appliquer ses propres politiques[76]. Cependant, la violence s'est estompée pendant les élections grâce à l'action collective de la société civile qui a pris des initiatives pour contrer les discours de haine.

Des organisations de la société civile ont publié largement des appels à la paix et à l'unité sur les réseaux sociaux (communément appelés « propagandes de paix »), mais aussi par voie d'affiches et de campagnes publicitaires. Une initiative stratégique à but non lucratif s'est soldée par l'envoi de SMS à 65 000 Kenyans sous la forme de messages d'appel à la paix. La série télévisée populaire Vioja Mahakamani a diffusé quatre épisodes autour du dialogue non violent. Les chercheurs ont constaté par la suite que ces épisodes avaient accru la méfiance des téléspectateurs à l'égard des rhétoriques motivées par la haine[77].

Une poignée de groupes ont piloté des programmes de surveillance des discours de haine qui ont permis à des individus d'agir contre ce type de propos sur les forums en ligne. L'initiative baptisée Projet Umati s'est déroulée de septembre 2012 à mai 2013. Après inspection des sites les plus prisés sur le web kenyan, une équipe de veilleurs a rapporté près de 6 000 cas de discours de haine. Elle a découvert qu'un quart d'entre eux constituaient des appels « très dangereux » à la violence et que plus de 80 % de ces propos se trouvaient sur Facebook[78].

Cette étude a donné naissance au projet Nipe Ukweli, qui a diffusé dans les médias traditionnels et sur les forums communautaires des directives concernant la surveillance citoyenne des discours de haine sur les réseaux sociaux. Des prospectus décrivaient les traits caractéristiques des discours de haine et encourageaient les citoyens à signaler les auteurs des abus via un service d'assistance (par SMS) ou une base de données Internet. Proposé en anglais et en swahili, le projet a mis l'accent sur l'initiative citoyenne en donnant aux intéressés le pouvoir de contrer et discréditer les discours violents et de s'en prémunir[79].

IV. PROTECTION DE L'INTÉGRITÉ ÉLECTORALE CONTRE LA DÉSINFORMATION

Définie comme la diffusion intentionnelle d'informations fausses ou trompeuses, la désinformation est devenue une menace sérieuse pour l'intégrité électorale. Ces dernières années, partout dans le monde, des acteurs très divers animés par des motivations politiques et économiques se sont servis des réseaux sociaux pour répandre et amplifier la désinformation et la propagande auprès d'électeurs potentiels avant la tenue d'élections, exacerbant des divisions ethniques, religieuses et sociales anciennes et semant la méfiance envers les médias et les institutions démocratiques.

Du point de vue normatif, nous voulons que les électeurs prennent des décisions éclairées. Lorsque les informations qu'ils reçoivent sont fausses, ils risquent de choisir un candidat qui ne correspond pas à leurs préférences. Les électeurs doivent comprendre les conséquences de leurs décisions et être en mesure de demander des comptes à leurs représentants. La désinformation a pour effet de réduire à néant le principe de redevabilité inhérent aux élections. Mais au-delà des préoccupations normatives, elle est directement en mesure d'affaiblir l'intégrité électorale en sapant la sécurité mutuelle. Elle peut également éroder la confiance dans le concept même d'élections libres et justes en semant le doute sur l'intégrité du scrutin et le professionnalisme de ses organisateurs. L'impartialité des organes de gestion des élections est elle aussi remise en cause, de même que le caractère légitime et fiable du scrutin, contesté à grand renfort de rumeurs.

La désinformation n'est un phénomène ni nouveau, ni propre aux technologies contemporaines de communication des informations[80]. Les arguments qui tendent à la désigner comme un problème purement lié aux « réseaux sociaux » détournent l'attention du rôle des médias traditionnels et des personnalités politiques. Ces derniers ne sont en

effet pas étrangers à la mise en place d'un écosystème d'information où prospèrent la désinformation et les discours de haine. Dans les pays dotés de médias traditionnels ouvertement partisans, la presse, la télévision et la radio amplifient et légitiment la désinformation et les pires rumeurs en ligne. Même lorsqu'ils font preuve d'un sens de la responsabilité et d'une objectivité certaine, les médias traditionnels peuvent être sensibles à la désinformation en ligne ou amplifier des récits visant à saper la confiance et l'intégrité électorale.

Néanmoins, les réseaux sociaux sont souvent le lieu où les utilisateurs découvrent initialement les propos faux ou trompeurs[81], en partie parce que ces plateformes ont fondamentalement changé les modes de production et de consommation des nouvelles et des informations. Il est de notoriété publique qu'à l'ère numérique toute personne disposant d'un clavier peut publier des textes. Grâce au microblogging et au journalisme citoyen, n'importe qui peut communiquer des nouvelles et des contenus à de vastes publics en temps réel. Les médias traditionnels et les sociétés de radiodiffusion, garde-fous de la communication politique, ont perdu le monopole de la diffusion des informations[82]. Bien que les réseaux sociaux permettent à leurs utilisateurs de devenir des producteurs d'informations, le déclin des régulateurs intermédiaires traditionnels signifie que les normes régissant les médias classiques ne s'appliquent pas toujours à la panoplie des contenus générés par les utilisateurs. Ainsi, la désinformation – et d'autres formes de contenus de mauvaise qualité, hyper partisans ou conspirationnistes – peut facilement trouver un terrain d'accueil sur les réseaux sociaux.

Les algorithmes des réseaux sociaux, ainsi que les politiques et les pratiques qui en régissent l'usage, contribuent également à la propagation en ligne de la désinformation, de diverses manières. L'environnement informationnel numérique actuel est façonné à la fois par des algorithmes (qui trient, classent, hiérarchisent et fournissent des contenus) et des utilisateurs qui influent sur les types de recommandations émises par les algorithmes à partir des données générées par leurs interactions en ligne[83]. Les algorithmes ne sont pas des technologies neutres[84]. Bien au contraire, ce sont des infrastructures de publicité et de persuasion, conçues pour maximiser l'attention des utilisateurs et, partant, les revenus publicitaires[85]. Parce que les personnes sont attirées par les contenus émotionnels, saisissants et captivants, les algorithmes d'optimisation de l'attention et les préférences humaines tendent à favoriser la fiction alléchante plutôt que les faits ennuyeux. Et la désinformation, visant précisément à susciter des réactions épidermiques et émotionnelles, peut provoquer un engagement plus vif que d'autres formes de nouvelles et d'informations[86].

Les préoccupations nouvelles soulevées par la relation entre les réseaux sociaux et la désinformation sont apparues sur le devant de la scène après le référendum sur le Brexit de juin 2016 au Royaume-Uni et l'élection présidentielle de novembre 2016 aux États-Unis. Des infox aux gros titres outranciers, telles que les allégations de participation d'Hillary Clinton à un réseau pédophile dans le sous-sol d'une pizzeria de Washington, ont occupé une place prépondérante dans les fils de réseaux sociaux de certains utilisateurs. Un grand nombre de ces fausses nouvelles ont obtenu de meilleurs résultats de consultation que les nouvelles émanant d'organes de presse professionnels[87] et détourné les gens d'autres débats publics importants en lien avec les élections. Alors que le « #Pizzagate » ou le soutien qu'aurait apporté le Pape à Donald Trump pendant les présidentielles américaines constituent des informations ostensiblement falsifiées, la plupart du temps la désinformation mêle vérité et mensonge de telle manière qu'il est difficile de définir clairement ce qui relève ou non de l'« infox ». Dans certains cas, la désinformation contient des éléments de véracité : des informations factuellement correctes peuvent servir à « dénigrer des points de vue opposés » ou à présenter les faits sous un

faux jour[88]. De plus, la satire, la parodie et l'exagération peuvent être interprétées comme de l'humour par certains et comme des nouvelles fiables par d'autres[89]. Le champ de la désinformation couvre-t-il les erreurs présentes dans les reportages, la satire politique, les déclarations erronées des acteurs politiques – ou uniquement les affabulations ? Les tentatives esquissées pour trouver une voie médiane et signaler les éventuelles fausses nouvelles sous la dénomination « contestées » ont eu des conséquences inattendues : ainsi les récits non signalés ont été perçus comme des nouvelles bénéficiant d'un degré d'exactitude et de vérification supérieur[90].

MESURE DE LA FRÉQUENCE DE LA DÉSINFORMATION

La définition même de la désinformation influe de manière significative sur sa fréquence estimée. Mais, contrairement à certaines idées reçues, les démocraties ne sont pas noyées sous la désinformation. Les recherches empiriques sur la réelle fréquence de la désinformation demeurent limitées et les études existantes tendent à conceptualiser différemment le phénomène ou à braquer les projecteurs principalement sur les États-Unis, ce qui rend difficile toute généralisation. Cependant, un nombre croissant de données probantes nous rappelle que l'échelle de la désinformation diffère selon les pays et les plateformes ainsi qu'entre les communautés d'utilisateurs. Privilégiant une définition restrictive des « infox », Allcott et Gentzkow ont estimé que, dans la période précédant l'élection présidentielle américaine de 2016, l'adulte américain moyen avait vu et mémorisé une infox sur les réseaux sociaux[91]. Une autre étude menée par Guess, Nyhan et Reifler a estimé qu'environ 27 % des Américains (soit 65 millions d'individus) avaient été exposés à au moins une infox pendant une durée similaire[92]. Recourant à une définition plus large, Howard *et al.* ont

révélé que, dans les deux semaines précédant l'élection, les utilisateurs de Twitter aux États-Unis avaient autant partagé les articles issus du « maljournalisme » ou « junk news » (contenus conspirationnistes, hyper partisans et non conformes aux normes du journalisme professionnel) que les nouvelles rédigées par des professionnels[93].

Cependant, la fréquence des infox ou du maljournalisme sur les réseaux sociaux varie selon les pays. Au Royaume-Uni, en France et en Allemagne, les utilisateurs de Twitter ont partagé beaucoup plus de nouvelles professionnelles (49, 46 et 40 % respectivement) que d'articles de maljournalisme (10, 4 et 9 % respectivement)[94]. En Suède, une URL sur trois partagée sur Twitter relevait du maljournalisme[95]. Et au Brésil, seul 1,2 % de l'ensemble des contenus Twitter partagés en lien avec les élections de 2018 s'apparentait à du maljournalisme[96]. Dans ce dernier cas, cependant, une autre étude de la communication politique sur WhatsApp a peint un tableau différent : sur ce réseau, qu'utilisent 90 % des internautes brésiliens, la désinformation a pris la forme de contenus visuels tels que mèmes, images et liens vers des vidéos YouTube[97]. Seules quatre des 50 images les plus partagées par les groupes WhatsApp publics contenaient des informations factuelles[98]. Une analyse qualitative a montré que la désinformation sur ce réseau prospérait sur fond de divisions politiques – en les exacerbant – et amplifiait le sentiment anti-féministe et anti-LGBTQ[99]. Des schémas de communication politique similaires ont été observés en Inde, où WhatsApp compte plus de 200 millions d'utilisateurs. Un tiers des images partagées par le parti Bharatiya Janata (BJP) et un quart de celles partagées par le parti du Congrès (INC) ont été classées comme conspirationnistes et clivantes[100].

Au-delà des différences entre les pays et les plateformes, il existe également des différences entre les publics qui partagent et consomment la désinformation. Bien que les jeunes utilisateurs aient parfois du mal à juger de la crédibilité des informations en ligne, le partage et la consommation de la désinformation tendent

à être générationnels et partisans. Aux États-Unis, les utilisateurs qui s'identifient comme conservateurs étaient plus susceptibles de partager de fausses nouvelles que ceux qui s'identifient comme progressistes ou modérés[101]. Cependant, l'âge a également joué un rôle important : les personnes de plus de 65 ans ont partagé le plus de fausses nouvelles, toutes appartenances politiques ou idéologiques confondues[102]. Il en va de même dans d'autres pays, comme le Nigéria, où les fausses nouvelles ont été plus largement partagées sur WhatsApp par les utilisateurs d'âge mûr[103].

LA DÉSINFORMATION COMME ARME POLITIQUE

Bien que les études actuelles ne livrent pas de conclusions claires quant à l'ampleur de la propagation de la désinformation sur les réseaux sociaux, des acteurs malveillants s'en servent de plus en plus comme arme à des fins politiques ou économiques. Profitant de la viralité et de l'anonymat offerts par les plateformes de réseaux sociaux, des réseaux coordonnés de faux comptes ont eu recours à la désinformation pour polluer l'agora numérique et imposer leurs idées marginales dans les fils d'actualité d'utilisateurs modérés. Le processus fonctionne souvent de manière organique en générant de faux profils militants par le biais de réseaux automatiques et coordonnés ou de faux comptes qui aiment, partagent, re-tweetent et transfèrent des messages afin d'alimenter la viralité. Dans de nombreuses démocraties, nous avons observé le recours à la « propagande informatique » pour amplifier les mèmes politiques, les vidéos et la désinformation afin de répandre la peur, la colère et l'indignation avec à la clé dans certains cas des troubles politiques et violents. À mesure que l'innovation technologique se poursuit, notamment concernant l'intelligence artificielle et l'analyse

des très gros volumes de données, les outils et les techniques de désinformation continuent à évoluer parallèlement. Nous avons déjà vu des exemples d'infox superficielle (« shallow fakes »), sous la forme de fichiers audio et vidéo manipulés grossièrement, se répandre en ligne ; mentionnons à cet égard la vidéo virale de la présidente de la Chambre des représentants des États-Unis, Nancy Pelosi – une vidéo falsifiée la montrant sous les traits d'une personne en état d'ébriété. Les technologies d'infox plus réalistes (« deep fakes »), qui utilisent l'intelligence artificielle pour simuler une expression faciale, un mouvement du corps et la modulation de la voix, risquent de bouleverser encore un peu plus le paysage de l'information numérique, notamment parce que les sociétés de réseaux sociaux ont du mal à empêcher la diffusion de contenus malfaisants sur leurs plateformes.

ACTIONS À ENVISAGER

Les préoccupations croissantes que suscitent la fréquence, l'impact et l'instrumentalisation de la désinformation enjoignent les décideurs à relever ce défi de taille. Depuis 2016, plus de 40 gouvernements ont proposé ou appliqué de nouvelles lois s'attaquant aux infox sur les réseaux sociaux[104]. Cependant, la lourde responsabilité qui leur incombe et la réponse à donner à un phénomène complexe et multidimensionnel soulèvent bien des questions tant les recherches menées jusqu'à présent ne permettent que d'effleurer les enjeux liés à la désinformation. Peu de travaux empiriques permettent de cerner le profil des protagonistes qui partagent les contenus de désinformation, les raisons invoquées ou encore le caractère intentionnel dudit partage[105]. Les études expliquant les effets de l'exposition à la désinformation et s'efforçant de déterminer si celle-ci fait le jeu de la polarisation, des comportements

partisans, de l'extrémisme ou de la violence sont encore plus rares. Dans un écosystème médiatique hybride, il est également difficile de déchiffrer les effets spécifiques des réseaux sociaux sur la démocratie[106].

La réflexion sur le rôle du gouvernement et des sociétés de réseaux sociaux dans la régulation en ligne de la désinformation et, *in fine*, des discours diffusés, doit prendre en compte le contexte mondial dans lequel opèrent les plateformes. Dans les pays caractérisés par des institutions défaillantes, la répression des droits de l'homme et le non-respect endémique des normes démocratiques, les plateformes de réseaux sociaux peuvent jouer un puissant rôle normatif et défendre les valeurs démocratiques. Les réseaux sociaux présentent un intérêt en tant qu'espace de parole, d'organisation, de contestation et de partage d'informations, notamment dans les régimes fermés ou répressifs. Mais octroyer à des entreprises le pouvoir de se comporter en « arbitres de la vérité » n'est pas sans risque. Les avantages en matière de réduction de l'exposition à la désinformation doivent donc être considérables pour conférer un tel pouvoir d'organisation de la parole à des sociétés axées sur la maximisation des profits[107].

Il est important pour l'intégrité électorale que les citoyens aient accès à des informations de grande qualité dont les faits ont été vérifiés. Si des acteurs malveillants ont tenté de noyer l'écosystème numérique sous des vagues de désinformation, il existe aussi plusieurs exemples positifs d'organisations de la société civile ayant lutté contre ce phénomène. Dans des pays comme le Mexique et l'Indonésie, la collaboration entre organisations de la société civile, médias traditionnels et plateformes technologiques visant à débusquer les infox et à en stopper la propagation a eu des résultats impressionnants [voir les encadrés 5 et 6]. Ce type d'actions requiert beaucoup de temps et d'efforts, mais les faits suggèrent que les partenariats nationaux en faveur de la défense de l'intégrité électorale peuvent se montrer efficaces s'ils se rendent accessibles aux citoyens, suscitent la confiance dans leur jugement et réussissent à discréditer les exemples flagrants de désinformation. L'efficacité de ces initiatives est optimale lorsque les médias traditionnels valorisent l'objectivité et que les organes de gestion des élections avertissent, comme il se doit, le public de la menace que constituent les infox.

La communauté en faveur de l'intégrité électorale doit favoriser le renforcement des capacités des partenariats nationaux de défense de l'intégrité des élections luttant contre la désinformation, et appuyer l'amélioration de l'évaluation et du partage des bonnes pratiques.

Il convient également d'envisager de mettre en œuvre des politiques limitant l'aptitude des acteurs malveillants à transformer les plateformes de réseaux sociaux en armes et à générer la diffusion de contenus falsifiés. Profitant de la nature anonyme (notamment via l'utilisation de pseudos) des réseaux sociaux, des acteurs malveillants ont créé de faux comptes susceptibles d'accélérer la propagation de la désinformation et d'en augmenter la portée. La Commission considère l'anonymat comme un élément essentiel pour la démocratie et l'intégrité électorale car il constitue un précieux bouclier dans les pays où la protection des droits de l'homme, essentielle à la participation démocratique, n'existe pas. Cependant, associé à l'automatisation, l'anonymat peut faire courir des risques importants aux utilisateurs de l'agora numérique. Plutôt que de limiter l'anonymat favorisé par la nature même d'Internet et des plateformes de réseaux sociaux, les sociétés devraient améliorer la transparence des comptes automatiques. Le signalement des comptes automatiques renforcera les efforts de transparence et aidera le public à évaluer la popularité des sources d'information ainsi que l'éventualité du gonflement artificiel de l'audience de certains contenus, tout en préservant l'anonymat, essentiel à la participation démocratique.

Les gouvernements devraient obliger les plateformes à déclarer les comptes qui recourent à l'automatisation. Les plateformes seraient alors passibles de pénalités financières obligatoires fixées par les pouvoirs publics en cas de comptes automatiques non déclarés comme tels (bots, etc.).

L'arme de la désinformation touche l'ensemble de l'écosystème médiatique. Bien qu'une campagne puisse démarrer sur une seule plateforme, les mêmes images, mèmes, vidéos ou URL pourront être partagés sur d'autres structures. Les plateformes doivent améliorer la coordination de leur

réponse face aux campagnes de désinformation. Les entreprises devront collaborer plus étroitement afin d'identifier les contenus douteux et les réseaux de comptes qui les partagent. La responsabilité de la lutte contre les comportements usurpateurs coordonnés ne doit pas s'arrêter à la porte de chaque plateforme. L'amélioration du partage d'informations et des stratégies trans-plateformes de détection et de limitation de la portée de la désinformation et des discours de haine est nécessaire pour renforcer l'intégrité électorale.

Les plateformes de réseaux sociaux devraient former une coalition visant à combattre les menaces numériques à l'encontre de la démocratie et de l'intégrité électorale, à l'instar des mesures prises pour lutter contre le terrorisme et l'exploitation des enfants. Les membres de la coalition se réuniraient à intervalles réguliers et élaboreraient des stratégies trans-plateformes pour détecter et limiter la portée de la désinformation et des discours de haine.

À long terme, les sociétés démocratiques devront se vacciner contre le virus de la désinformation. Les citoyens de l'ère numérique devront développer une expertise dans les domaines de la diffusion des informations, de la propagande et de l'identification des sources sur Internet[108]. Ils devront savoir reconnaître les fausses informations et repérer les théories conspirationnistes. L'aptitude à repérer l'identité de l'auteur d'une page web donnée et les positions qu'il défend constitue une composante cruciale de l'éducation au numérique. S'il est important de former les citoyens à la recherche de l'origine d'une information, il l'est tout autant de leur apprendre à reconnaître leurs propres sources potentielles de préjugés. Nous invitons les électeurs à se poser la question suivante : « D'où vient l'information et quels intérêts sert-elle ? ». Une autre question s'impose : « Pourquoi suis-je prédisposé(e) à croire ou non cette information ? ».

Les pouvoirs publics devraient promouvoir l'éducation aux usages numériques et aux médias dans les écoles ainsi que dans le cadre de programmes d'intérêt public destinés à l'ensemble de la population.

ENCADRÉ 5

Lutte contre la désinformation au Mexique

Pour les élections de 2018, l'Institut électoral national (INE) fédéral du Mexique s'est préparé à contrer les infox susceptibles d'influencer l'opinion des électeurs, d'éroder la confiance publique dans les processus électoraux ou d'accroître la polarisation et la fragmentation[109]. Pendant le cycle électoral, il a lancé avec succès une stratégie tripartite visant à nouer une « alliance » avec les réseaux sociaux et d'autres médias, afin de soutenir une initiative de la société civile, *Verificado 2018*, et d'instaurer un système informatique de contrôle des faits, *Certeza 2018* ; l'objectif étant de corriger les fausses informations diffusées en ligne[110].

Dans le cadre d'un effort coordonné unique en son genre, l'INE a signé des accords de coopération formels avec Facebook, Twitter et Google. Cette approche a permis la toute première diffusion en streaming et en direct des débats présidentiels mexicains et des annonces électorales de l'INE, regardés par des millions d'électeurs dans le pays[111]. L'INE a également collaboré avec Facebook à la mise en œuvre de « boutons » interactifs permettant aux utilisateurs d'accéder au site web officiel de l'autorité électorale, de répandre des messages d'incitation au vote et de faire participer les utilisateurs au choix des sujets de débat[112]. De la même manière, Google a mis au point un bouton de réacheminement des utilisateurs vers les contenus du site de l'INE et hébergé une application Google Maps fournissant aux électeurs des informations sur l'emplacement des bureaux de vote[113]. Twitter et l'INE ont organisé conjointement des discussions sur les débats présidentiels autour de la question des hashtags traçables, créé un forum de commentaires journalistiques en temps réel et utilisé une fonction de réponse automatique pour communiquer les résultats électoraux en temps réel[114].

L'INE a également soutenu l'initiative de vérification des faits *Verificado 2018*, pilotée par Animal Politico, AJ+ Español, Newsweek Español et Pop-Up Newsroom, qui a rassemblé plus de 60 autres organisations de la société civile. Verificado a créé un groupe WhatsApp et une multitude d'autres forums sur les réseaux sociaux par le biais desquels les utilisateurs pouvaient s'enquérir de la véracité des revendications politiques et recevoir des réponses fiables en temps voulu. Les opérateurs du projet ont répondu à 400 demandes, produit 50 vidéos d'information et reçu des millions de visiteurs sur leur site officiel[115].

L'INE a également mis en place un mécanisme technologique baptisé Certeza 2018. À l'aide de systèmes de contrôle humains et informatiques, d'agents de terrain et d'une équipe d'évaluation, Certeza a adopté une approche en cinq étapes pour s'attaquer à la mésinformation : 1) surveillance des fausses informations à l'aide de mots clés, 2) évaluation des cas détectés, 3) vérification de la marche à suivre adaptée, 4) collecte de preuves, et 5) diffusion de notifications aux médias à la suite de l'évaluation des cas[116]. Pour diffuser les résultats de ses vérifications, Certeza a bénéficié à la fois d'accords de coopération avec des plateformes médiatiques et de la force de frappe de Verificado. Après avoir contrôlé des millions de publications sur les réseaux sociaux, le système a identifié 217 cas de désinformation le jour des élections et répondu simultanément aux utilisateurs demandant des informations spécifiques sur le scrutin[117].

Outre le lancement et le soutien de ces méthodes de lutte contre la désinformation, l'INE s'est protégé contre les cyberattaques grâce à 2 000 audits de ses systèmes informatiques et à la surveillance de la sécurité en temps réel 24 heures sur 24 et 7 jours sur 7[118]. Globalement, l'approche de l'INE lors des élections de 2018 a constitué un modèle révolutionnaire et efficace que pourront emprunter d'autres nations à l'occasion d'élections futures.

ENCADRÉ 6

Lutte contre la désinformation en Indonésie, 2018-2019

L'Indonésie a connu une fréquence accrue des infox pendant les élections de 2018-2019[119]. Les organes électoraux nationaux ont réagi en déployant plusieurs initiatives de collaboration avec des organisations de la société civile, les entités gouvernementales compétentes et les plateformes de réseaux sociaux. Axés sur la lutte active contre la désinformation et les discours de haine ainsi que sur la préservation de la confiance du public en contexte électoral, ces partenariats ont pris la forme d'activités de sensibilisation, veillé à l'application des dispositions légales et réglementaires et conduit des initiatives conjointes de vérification des faits.

Les deux organes de gestion des élections (Commission électorale générale [KPU] et Agence de supervision des élections [Bawaslu]), ainsi que des organisations de la société civile – dont l'Indonesian Anti-Slander Community (MAFINDO) et le Centre for the Study of Religion and Democracy (PUSAD) Paramadina – ont élaboré des stratégies de lutte contre la désinformation dans le contexte indonésien. Leur action s'est inspirée des bonnes pratiques partagées par la Fondation internationale pour les systèmes électoraux (IFES), à partir de son expérience récente au Kenya[120]. L'initiative a consisté, entre autres, à obtenir l'engagement de diverses parties prenantes, à sensibiliser la population, à collecter des données, à élaborer une contre-communication et à statuer sur les cas en toute équité[121]. En coordination avec le ministère de la Communication et des technologies de l'information, le KPU et Bawaslu ont établi une « cellule de crise » qui a surveillé en permanence l'activité sur les réseaux sociaux. La police nationale a été chargée d'appliquer les lois indonésiennes existantes sur la désinformation et la discrimination, tandis que le Bureau du Président dialoguait avec des organisations partenaires[122]. Bawaslu a également pris l'initiative d'une déclaration visant à « rejeter et contrer l'achat de votes, les insultes, les incitations et les conflits clivants lors des élections à Pilkada de 2018 et des élections générales de 2019 » qui a recueilli la signature de 102 groupes de la société civile ainsi que de plateformes comme Google, Facebook et Twitter[123].

Des initiatives ont été conduites par des organisations à but non lucratif telles que l'opération de vérification des faits « Hoax Crisis Center » de MAFINDO visant à discréditer les canulars sur les réseaux sociaux pendant les élections aux organes exécutifs locaux de 2018. De la même manière, en 2019 MAFINDO et 24 organes de presse ont mis en ligne – moyennant des financements de Google News – le site CekFakta.com dans le but de démasquer les canulars et les fausses déclarations des candidats, et de rétablir la vérité[124]. Ces partenaires ont également élaboré des outils de vérification des faits à l'usage du grand public, dont une application pour téléphone qui permettait aux bureaux des autorités provinciales de corriger les fausses nouvelles en temps réel, à mesure que les utilisateurs les signalaient. Parmi les autres projets, on peut citer les formations à la lutte contre la désinformation à l'intention des organisations de la société civile du Center for the Study of Religion and Democracy et les annonces de service public générées par MAFINDO et Bawaslu. Mentionnons également les ateliers sur les infox et les discours de haine identitaires organisés par l'IFES à l'intention des organes de gestion des élections[125].

À l'échelle nationale, ces efforts coordonnés ont permis de vérifier 821 cas de désinformation politique, dont plus de la moitié en rapport avec des élections imminentes[126]. Au niveau infranational, un « Hoax Crisis Center » conjoint et d'autres projets locaux ont contribué à maintenir la paix dans des régions enclines aux conflits telles que le Kalimantan occidental[127]. Les efforts publics, privés et de la société civile menés en Indonésie constituent un modèle d'action collective apte à défendre les processus démocratiques, remis en cause par la diffusion de fausses informations numériques virales et de rhétoriques violentes.

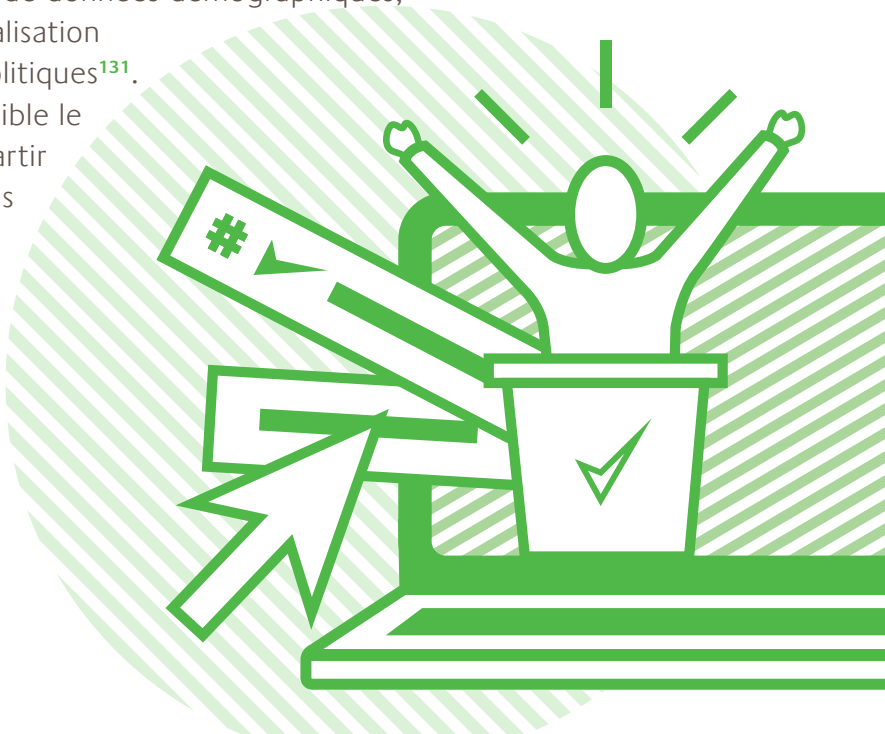
V. LA PUBLICITÉ À DES FINS POLITIQUES À L'ÈRE DU NUMÉRIQUE

Ces trois dernières années, nul volet de la réglementation d'Internet n'a reçu plus d'attention que la réforme de la publicité politique en ligne. Compte tenu de la corrélation existant entre publicité en ligne et polarisation, désinformation et ingérence étrangère dans les élections, cette prise de conscience du public est la bienvenue. De plus, du fait qu'elles acceptent la publicité politique et lui offrent un terrain propice, les grandes plateformes Internet exploitent, amplifient et ciblent à l'extrême les messages, lesquels compromettent la santé du débat démocratique et l'intégrité électorale. À de nombreux titres, la publicité en ligne crée un effet de loupe permettant de voir tous les risques et avantages d'Internet pour la démocratie.

Au même titre qu'Internet et les technologies de communication numériques en général, la publicité politique en ligne présente des apports significatifs pour la vie démocratique. Souvent beaucoup moins onéreuse que les annonces publicitaires à la télévision et à la radio, la publicité numérique permet aux candidats disposant de peu de ressources de faire passer leur message, notamment à l'échelon local[128]. En outre, en dépit de toutes les critiques qu'il suscite, le micro-ciblage permet aux responsables de campagnes et aux groupes de pression de transmettre efficacement des messages aux personnes qu'ils souhaitent toucher ; et ce, à l'image des responsables marketing qui depuis des années adoptent le publipostage, le démarchage téléphonique et, plus récemment, le courrier électronique. Enfin, Internet s'est avéré particulièrement utile pour collecter des fonds auprès de petits donateurs. Des candidats et des groupes s'en sont servis pour lever des montants significatifs grâce au nombre élevé des donateurs, « démocratisant » ainsi le financement politique[129].

Mais la publicité politique en ligne s'est également avérée un terrain fertile pour toutes les pathologies de la démocratie attribuées aux

technologies de communication numériques. Si le micro-ciblage peut aider à mobiliser et collecter des fonds, il permet aussi aux organisateurs des campagnes d'envoyer des messages sélectifs de démobilisation et de propagande polarisante à des électeurs influençables dont les affinités psychologiques et politiques peuvent être identifiées avec une précision croissante grâce aux données collectées par les plateformes Internet et d'autres sociétés. Les tests de contenus et l'apprentissage automatique permettent aussi aux publicitaires de peaufiner les messages qu'ils souhaitent envoyer pour renforcer l'adhésion aux contenus, ce qui aboutit souvent à la création d'une centaine de variantes d'une même publicité[130]. De ce fait, des messages différents (voire contradictoires) peuvent être envoyés à différentes personnes à l'insu des autres. Sous cet angle, le côté sombre du micro-ciblage se traduit par la création artificielle (et non pas spontanée) de chambres d'écho en ligne. Les plateformes Internet permettent aux publicitaires d'envoyer des messages sélectifs à des petits groupes d'électeurs sur la base de données démographiques, de leurs centres d'intérêt, de leur localisation géographique et d'autres variables politiques[131]. En fait, elles rendront également possible le ciblage de « publics sur mesure » à partir de listes d'adresses e-mail individuelles fournies par les campagnes et de « publics sosies » que la plateforme extraira de sa base de données volumineuse de façon à atteindre un groupe visé dans le cadre d'une campagne.



L'absence de réglementation de la publicité politique en ligne a ouvert la voie à l'adoption de pratiques opaques de la part d'acteurs nationaux et étrangers, consistant à diffuser des messages polarisants et trompeurs lors des campagnes électorales. Les interventions russes pendant la campagne présidentielle américaine de 2016 a révélé les vulnérabilités du système de publicité à visée politique, même face à des annonces parrainées par des puissances étrangères. On a ainsi assisté à la diffusion de messages polarisants dans le but d'influer sur les résultats électoraux et d'exploiter les divisions sociales du pays[132]. Moyennant plus de 100 000 dollars US de publicités sur Facebook, dont certaines achetées en roubles, l'Internet Research Agency (IRA) russe a envoyé des messages ciblés qui mentionnaient parfois les candidats, mais consistaient le plus souvent en propagande polarisante autour de questions sociales clivantes telles que l'immigration, le droit au port d'armes à feu et la brutalité policière à connotation raciste[133]. Parfois, différentes annonces répandaient une propagande duale dans le but de fomenter la division et la polarisation, et non de convaincre les différents publics du bien-fondé des arguments des parties adverses. Tendant au sensationnalisme et n'hésitant pas à masquer l'identité du véritable annonceur, ces publicités ont permis à l'Internet Research Agency russe de façonner des audiences pouvant être ciblées par des messages organiques et transférés au réseau élargi de l'utilisateur.

La controverse suscitée par les publicités russes lors de l'élection de 2016 n'a pas débouché sur une action législative ou réglementaire aux États-Unis mais a contraint les grandes plateformes Internet à mettre en œuvre de nouvelles mesures concernant la publicité à des fins politiques. En l'occurrence, au cours des deux années suivant l'élection, Facebook, Google et Twitter ont adopté des règles de transparence pour les publicités politiques : ils ont mis à disposition des archives – accessibles aux utilisateurs et aux groupes de vigilance – contenant l'historique des publicités ainsi que des renseignements sur les annonceurs et des informations restreintes sur le ciblage et l'exposition. En outre, pour empêcher l'achat anonyme de publicités par des acteurs étrangers,

les plateformes ont adopté des systèmes de vérification exigeant de tous les annonceurs politiques la mention de leur adresse (afin d'en vérifier la validité via un système d'envoi et de retour de carte postale). Il s'agit de s'assurer qu'un acteur national identifiable est l'acheteur réel de l'annonce. Si les plateformes de réseaux sociaux ont mis en œuvre des contremesures pour empêcher des entités étrangères d'acheter des annonces politiques aux États-Unis, cela n'a pas empêché des publicités parrainées par des instances étrangères de cibler d'autres nations[134].

Les législateurs du monde entier ont émis des propositions pour renforcer le contrôle de la publicité politique mais ils se heurtent souvent à des difficultés de taille. La principale concerne la définition de la « publicité à visée politique » : comment la loi peut-elle spécifier les types de questions suffisamment « politiques » pour relever des règles relatives à la publicité politique ? La tâche est encore plus ardue lorsque les sociétés mêlent messages politiques et messages commerciaux : par exemple, comment qualifier une publicité pour des rasoirs faisant référence à la lutte contre le harcèlement sexuel, une publicité pour des chaussures de sport faisant référence aux joueurs de football américain s'élevant contre les brutalités policières racistes ou encore une publicité pour de la bière envoyant un message positif sur l'immigration en mettant en avant l'histoire de la brasserie ? En outre, si la publication payante de sujets politiques doit être traitée comme une publicité politique, les journalistes et les organisations médiatiques seront pris la main dans le sac chaque fois qu'ils paieront (comme ils le font fréquemment) pour promouvoir leurs articles sur les réseaux sociaux afin d'élargir leur lectorat. Vu qu'une part importante des publicités politiques faisant l'objet de polémiques est de nature partisane (l'ingérence étrangère et la diffusion de messages polarisants ou marqués par la désinformation étant incriminées), les réformes de la publicité qui feront l'impasse sur cette dimension ne résoudront pas le problème.

Chaque plateforme a traité le problème de la publicité partisane différemment. La société Twitter a annoncé récemment qu'elle ne diffuserait plus d'annonces mentionnant des candidats, des référendums

ou des législations imminentes mais autoriserait la « publicité défendant des causes ». Google n'inclut par les publicités partisanes dans ses archives d'annonces politiques. En revanche, le géant américain a fait savoir récemment qu'il n'autoriserait plus les annonceurs à baser leur ciblage sur l'appartenance politique et qu'il empêcherait les annonceurs politiques de faire des promesses frauduleuses dans les publicités, comme il le fait déjà pour la fraude à la consommation. La société Facebook met à disposition les archives de publicités politiques les plus fournies, comprenant non seulement les annonces des candidats mais aussi d'autres composantes qu'elle a identifiées en s'appuyant sur l'initiative universitaire « Comparative Agendas Project ». Cependant, sa politique anti-censure concernant les publicités politiques – qui exempte les acteurs politiques de toute vérification factuelle par des tiers, afin de préserver la liberté d'expression[135] – a fait l'objet de vives critiques, même en interne de la part d'employés qui ont adressé au New York Times un courrier arguant que « liberté d'expression et expression payante doivent être dissociées »[136].

Par ailleurs, les entreprises et les régulateurs sont en train de réfléchir à d'autres types de réformes afin de répondre aux préoccupations relatives à la manipulation par l'intermédiaire de la publicité politique. Certaines plateformes ont envisagé de restreindre la possibilité de cibler des audiences personnalisées ou de limiter la taille de l'échantillon ciblé par les publicités politiques. D'autres exigeraient une vérification factuelle des publicités contestées afin de s'assurer de la véracité des affirmations. D'autres encore adapteraient la réglementation existante sur la télévision pour interdire, par exemple, la publicité à visée politique dans la période pré-électorale – lorsque les responsables de campagnes éprouvent le plus de difficultés à réagir aux publicités mensongères et se relever à temps. Ayant fini par admettre que ces décisions sont trop importantes – notamment s'agissant des enjeux démocratiques qu'elles engagent – pour être laissées au bon vouloir de grandes multinationales motivées par la maximisation des profits, les plateformes ont appelé, elles-mêmes, de leurs vœux une orientation législative en la matière.

ACTIONS À ENVISAGER

Une approche responsable en matière de publicité politique numérique requiert que les partis politiques, les plateformes de réseaux sociaux et les autorités publiques compétentes agissent tangiblement. Premièrement, les acteurs politiques, les partis politiques et les candidats doivent se porter garants d'une utilisation de la publicité numérique à même de respecter le principe d'intégrité électorale. Le mode d'utilisation des nouvelles technologies de publicité numérique dans le cadre des campagnes peut influencer l'ensemble du processus électoral : augmenter le niveau de confiance des citoyens et leur donner accès à davantage d'informations, ou au contraire saper l'intégrité électorale par des pratiques de campagne trompeuses mettant l'accent sur les rumeurs, la conspiration, la désinformation et la manipulation des médias. Il existe déjà des exemples d'acteurs politiques adhérant à des codes de conduite et des bonnes pratiques dans un contexte de campagne politique sain **[Encadré 7]**. L'intégrité électorale à l'ère numérique requiert des normes éthiques plus strictes concernant les modalités d'utilisation des réseaux sociaux et de la publicité numérique par les personnalités politiques, les partis et les candidats.

Nous adhérons à l'appel de la Commission transatlantique sur l'intégrité des élections demandant aux candidats, aux partis et aux groupes politiques de s'engager par écrit à rejeter les pratiques de campagnes numériques trompeuses, à savoir : utilisation de données ou de documents volés, recours à des supports visuels altérés déformant les propos d'une personnalité à un degré de réalisme plus ou moins élevé (« shallow fakes » et « deep fakes »), publication de fausses images de nus (« deep nudes »), production, utilisation ou diffusion de documents falsifiés ou faux, ou encore collusion avec des gouvernements étrangers et leurs agents dans le but de manipuler une élection.

ENCADRÉ 7

Accord d'Abuja sur la conduite des élections au Nigéria, 2015

Avant les élections générales de 2015, de nombreux Nigérians craignaient une répétition des événements de 2011, marqués par une violence pré-électorale de grande ampleur qui s'était soldée par plus de 800 morts et des milliers de personnes déplacées[137]. Alarmé par l'éventualité d'une catastrophe électorale, Kofi Annan s'était rendu au Nigéria et avait vivement conseillé aux candidats à l'élection présidentielle de signer un traité de paix les engageant à mener des campagnes propres, fondées sur de véritables enjeux. En janvier 2015 à Abuja,en présence de M. Annan en qualité de témoin, les candidats se sont engagés à ne pas mener de campagnes négatives susceptibles d'inciter à la violence religieuse, tribale ou ethnique[138]. L'accord a été mis en place par de nombreuses organisations nationales, comprenant des chefs religieux chrétiens et musulmans, avec l'assistance de plusieurs ONG[139]. Il appelait à la création d'un Comité national de la paix chargé de suivre le respect de ces dispositions[140].

L'Accord d'Abuja a été une indiscutable réussite. En mars 2015, deux jours avant l'élection présidentielle, les deux principaux candidats ont renouvelé leur engagement, en guise de symbole d'unité nationale, de stabilité et de sécurité avant le jour du scrutin[141]. Il a rapidement servi de modèle à d'autres élections, notamment au Mozambique pendant la période précédant l'élection d'octobre 2019[142]. Des variantes de l'Accord ont également été signées par la plupart des représentants de l'État au Nigéria[143]. Pendant le cycle des élections générales de 2019, les chefs de partis nigérians ont signé un autre accord dans le même esprit[144]. L'héritage de l'Accord d'Abuja montre l'efficacité potentielle des engagements des responsables de campagnes en faveur de comportements respectueux et non violents.

Toutes les grandes sociétés de réseaux sociaux ont pris des mesures pour relever certains des nouveaux défis numériques que soulève la publicité politique. Nous pensons cependant qu'il est possible d'en faire davantage pour appuyer l'intégrité électorale. À titre d'exemple, toutes les plateformes pourraient prendre des mesures supplémentaires pour améliorer la transparence de la publicité politique (publication de davantage de données sur le micro-ciblage et divulgation de l'identité des annonceurs, notamment) et renforcer le contrôle des utilisateurs sur les types de publicités qui les ciblent. En outre, les plateformes pourraient contribuer à renforcer les normes positives des campagnes politiques en exigeant des acteurs politiques, partis et candidats acheteurs de publicités qu'ils s'engagent par écrit à éviter les pratiques de campagne trompeuses et à respecter leurs promesses. Toutes ces mesures seraient susceptibles de renforcer l'intégrité électorale.

Les plateformes devraient assurer la transparence accrue des publicités politiques.

- Les plateformes devraient laisser le choix aux utilisateurs d'accepter ou de refuser la publicité à des fins politiques.

- Les plateformes ne devraient accepter de vendre des espaces publicitaires qu'aux candidats, aux partis et aux groupes s'étant formellement engagés à éviter les pratiques de campagne trompeuses. Cet engagement deviendrait alors la norme contractuelle régissant l'approbation ou le refus d'une publicité donnée.

- Afin d'éviter que les financeurs ne se cachent derrière des noms d'organisations frauduleux, les plateformes devraient exiger la divulgation publique de l'identité des personnes finançant la publicité politique, quelle qu'elle soit.

Enfin, les autorités publiques compétentes doivent assumer leurs responsabilités s'agissant de la protection de l'intégrité électorale. Plus important encore, il convient d'adapter à l'ère numérique les lois et les réglementations relatives aux campagnes et à la publicité politiques. La définition de la nature même d'une publicité politique devrait notamment relever du droit et non être confiée à des sociétés dont l'objectif principal consiste à maximiser les profits. Les autorités publiques compétentes devraient également préciser la taille minimale de l'échantillon du public visé par le micro-ciblage des publicités politiques et envisager de légiférer sur une période de suspension des publicités politiques numériques, en s'inspirant des dispositions légales actuelles régissant la radiodiffusion dans certains pays. Si les plateformes ont fait des progrès significatifs en matière de transparence des publicités à visée politique, il reste beaucoup à faire pour promouvoir un environnement favorable au renforcement de l'intégrité électorale. Les gouvernements doivent prendre des mesures pour obliger les sociétés de réseaux sociaux à rendre publiques les données relatives à la publicité politique, notamment en exigeant des plateformes qu'elles publient des informations sur l'identité de l'annonceur ainsi que les critères de ciblage, les montants dépensés et l'identité des créateurs effectifs de l'annonce.

Les pays doivent adapter leurs réglementations sur la publicité politique à l'environnement en ligne. Les autorités publiques compétentes doivent :

- définir en droit la nature des publicités à visée politique ;
- obliger les plateformes de réseaux sociaux à rendre publiques toutes les informations relatives à l'achat de publicités, notamment l'identité réelle de l'annonceur, les montants dépensés, les critères de ciblage et l'identité des créateurs effectifs de l'annonce ;
- préciser en droit la taille minimale du segment de la population ciblée par les publicités ; et
- légiférer sur l'arrêt de la diffusion des publicités numériques à visée politique au moins 48 heures avant la tenue d'élections.

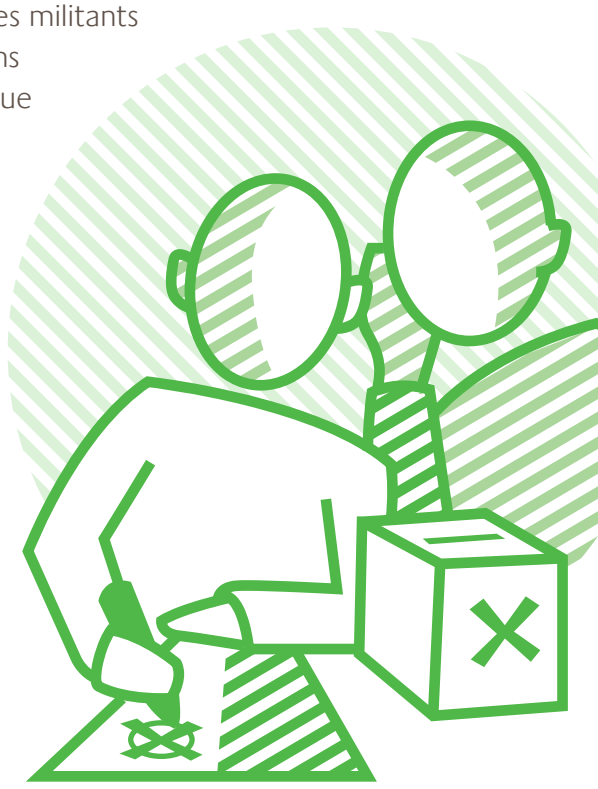
VI. PROTECTION DES PROCESSUS ÉLECTORAUX CONTRE L'INGÉRENCE ÉTRANGÈRE

En dépit des nombreux effets positifs d'Internet et des réseaux sociaux sur la vie démocratique et électorale – notamment la promotion de la libre expression, les opportunités de mobilisation politique et la démocratisation des informations –, les activités d'ingérence étrangère constituent l'aspect le plus manifeste de leur mauvais usage potentiel. Au cours de la décennie écoulée, des acteurs étatiques et non étatiques ont mis Internet au service de leurs programmes politiques, économiques et militaires, combinant stratégiquement opérations militaires traditionnelles, cyberattaques et campagnes de propagande en ligne. Du fait de la nature ouverte, anonyme et supranationale des technologies numériques, les réseaux sociaux ont offert de nouvelles occasions d'ingérence transnationale aux acteurs malveillants. L'intégrité électorale est étroitement liée à la souveraineté électorale ; à ce compte, les acteurs extérieurs ne devraient pas pouvoir influer sur les résultats d'une élection.

À ce jour, l'entremise de la Russie dans l'élection présidentielle américaine de 2016 constitue l'exemple d'ingérence étrangère le plus flagrant. Associant techniques de piratage classiques et campagnes numériques cordonnées sur divers médias traditionnels et nouveaux, les agents russes ont tenté d'influer sur l'opinion publique américaine et le résultat du scrutin. La fuite stratégique de données volées a nui à l'investiture présidentielle de Hillary Clinton[145]. Des organes médiatiques contrôlés par des entités russes tels que Russia Today (RT) et Sputnik ont diffusé des mensonges conspirationnistes et alimenté le sentiment anti-Clinton à grand renfort d'allégations de corruption, à la télévision et sur certaines chaînes YouTube. Des comptes usurpateurs ou automatisés, gérés par l'IRA, ont amplifié ces messages sur Facebook, Twitter et Instagram. Des publicités politiques, conçues pour polariser l'opinion à l'occasion de débats politiques particulièrement sensibles, ont ciblé des communautés d'électeurs dans le but de semer la division et la méfiance au sein de la

population américaine. En outre, des publications, des pages et des groupes devenus viraux sans le déboursement du moindre dollar ont atteint plus de 126 millions d'Américains pendant la période précédant le scrutin de 2016[146].

Bien que l'immixtion de la Russie dans l'élection américaine de 2016 ait été l'une des plus manifestes, notamment compte tenu de son échelle et de sa complexité, les États-Unis n'ont pas été le seul pays ciblé par l'ingérence russe. Des preuves éparses attestant de campagnes de désinformation parrainées par la Russie ont été découvertes dans de nombreuses parties du monde, notamment en Ukraine, au Royaume-Uni et en Afrique[147]. Plus inquiétant encore, d'autres pays désireux de se servir des réseaux sociaux pour exercer un pouvoir géopolitique ont adopté le modèle russe d'ingérence électorale, axé sur la déstabilisation d'un adversaire par un État nation. Il suffit de regarder la récente campagne de désinformation de la Chine à l'égard des manifestants de Hong Kong, qui dépeint les militants politiques comme violents et impopulaires[148], ou les opérations d'influence iranienne encourageant la diffusion d'une rhétorique anti- saoudienne et anti-israélienne, tout en exerçant des pressions pour un retournement de la politique américaine en faveur de l'Iran[149].



La lutte contre l'ingérence étrangère n'est pas sans poser de nouvelles difficultés, notamment celle qui consiste à opérer la distinction entre les activités de campagne normales de représentants officiels d'acteurs politiques nationaux et les opérations d'information anti-démocratiques menées par des gouvernements étrangers, des entités économiques douteuses ou des groupes nationaux. Les figures et partis politiques populistes ont recouru aux mêmes outils et aux mêmes stratégies que

les agents étrangers pour imposer des discours ultra-nationalistes et anti-immigration dans le cadre des débats politiques classiques. Des groupes de pression se sont servis des médias pour envoyer des messages partisans à des citoyens de pays étrangers. L'envoi ciblé de publicités politiques à des citoyens irlandais par des groupes pro-vie américains avant le référendum de 2018 sur l'avortement en constitue un exemple[150]. Du fait du chevauchement de ces efforts, il devient de plus en plus difficile de tracer la frontière traditionnelle entre activité politique étrangère et nationale, organisations gouvernementales et non gouvernementales, opérations d'information illicites et activités de campagne licites.

ÉMERGENCE D'ACTEURS TRANSNATIONAUX SPÉCIALISÉS DANS LA MANIPULATION ÉLECTORALE

L'ingérence est également monétisée par des acteurs privés et des sociétés de communication stratégique, qui vendent à un public spécifique divers produits destinés à l'ingérence électorale. Le scandale de Cambridge Analytica, une firme qui doit sa notoriété à l'utilisation de données Facebook pour envoyer de la propagande à des électeurs ciblés pendant l'élection américaine de 2016, constitue l'un des exemples les plus flagrants de la professionnalisation de la manipulation électorale[151]. Cambridge Analytica et sa maison mère, Strategic Communications Laboratories (Groupe SLC), se sont servis de données privées issues des réseaux sociaux et de leur infrastructure pour rédiger, cibler et adapter des messages de persuasion et de démobilisation dans le but d'influer sur les résultats électoraux de divers pays, dont le Nigéria, Sri Lanka, le Kenya, les Philippines, Trinidad-et-Tobago et

le Royaume-Uni[152]. Bien que l'efficacité des techniques de datamining et de « profilage psychographique » de Cambridge Analytica ait été largement surestimée[153], ce cas illustre le phénomène plus général de la professionnalisation de la manipulation électorale.

Actuellement, une multitude d'entreprises, de cabinets de conseil, d'agences de communication politique et de sociétés de marketing numérique utilisent des outils marketing pour influencer les électeurs[154]. Présentes sur tout le globe, ces entités collaborent avec des personnalités politiques et des gouvernements pour diffuser désinformation et propagande et envoyer à des électeurs ciblés des messages les incitant à ne pas voter[155]. Dans certains cas, elles opèrent à l'échelle internationale afin de masquer la véritable identité de la personne physique ou morale à l'origine de la campagne d'influence[156] et de profiter du faible coût de la main-d'œuvre numérique dans des pays tels que l'Inde[157] ou les Philippines[158], où a émergé le secteur lucratif des « fermes à trolls ».

PROTECTION DES INFRASTRUCTURES ÉLECTORALES

Tous les citoyens jouissent du droit au comptage de leur bulletin de vote, selon des modalités équitables et rigoureuses. Il est impératif pour l'intégrité électorale que les citoyens aient confiance dans le comptage des votes. L'intégrité électorale tient pour une grande part à la foi qu'ont les électeurs dans i) la légalité de leur inscription sur les listes électorales, ii) la fiabilité du comptage des votes et iii) l'exactitude des résultats officiels. Outre les effets subjectifs et subtils potentiels de la propagande et de la désinformation sur les

élections, il est important d'avoir conscience des inquiétudes liées à la cybersécurité des équipements que soulèvent les technologies électorales électroniques (TEE).

La protection des équipements et des logiciels informatiques utilisés pour l'inscription des électeurs et le scrutin est essentielle pour l'intégrité électorale. Au-delà des TEE elles-mêmes, un vaste écosystème technologique décentralisé appuie les élections : systèmes d'inscription en ligne sur les listes électorales, systèmes de comptage des votes, systèmes d'audit, etc. Toutes ces technologies sont vulnérables aux attaques numériques et aux erreurs internes qui, toutes deux, sont susceptibles d'éroder la confiance des électeurs et de mettre à mal l'intégrité électorale.

Le piratage des équipements et des logiciels électoraux peut avoir pour but de modifier les résultats, de manipuler les listes électorales ou simplement de saper la confiance des citoyens dans leurs élections. Il peut également être motivé par la simple volonté d'un gouvernement étranger ou d'un acteur national d'obtenir un résultat en sa faveur. Le piratage ne constitue qu'un des outils de manipulation des TEE. Lors de l'élection de 2014 au Mozambique, le gouvernement a ainsi supprimé l'inscription biométrique des électeurs dans les zones aux mains de l'opposition « en dépêchant du matériel inadapté et des équipes insuffisamment formées »[159]. Au-delà de l'ingérence visant un candidat donné, les gouvernements étrangers peuvent trouver globalement intérêt à semer la discorde, créer le chaos, saper la légitimité et éveiller la méfiance dans le but d'affaiblir le pays ciblé. Lorsque la sécurité des TEE sème le doute, les acteurs politiques mécontents sautent sur l'occasion pour imputer leur défaite à la manipulation des équipements et des logiciels de scrutin et affaiblir encore plus la confiance des citoyens dans le processus et ses résultats.

De plus, la sécurité des TEE n'est pas qu'un problème technique. Les responsables électoraux eux-mêmes sont susceptibles de la

compromettre, de façon délibérée ou non[160]. La dimension humaine « étant sensiblement présente à toutes les étapes opérationnelles des élections, les vulnérabilités humaines risqueront indubitablement d'être exploitées »[161]. La résilience de l'infrastructure électorale dépendra de la protection des systèmes techniques et de la formation aux bonnes pratiques de cybersécurité des personnes intervenant à tous les niveaux de l'écosystème des TEE. Il est utile de souligner le rôle essentiel que peuvent jouer les organes de gestion des élections professionnels, compétents et indépendants dans la protection de l'intégrité électorale à l'ère du numérique.

ACTIONS À ENVISAGER

Le droit international propose plusieurs recours légaux à l'ingérence d'acteurs étatiques dans des élections étrangères. L'article 2 de la Charte des Nations Unies garantit l'intégrité territoriale et politique des États, à laquelle contreviennent les campagnes d'influence étrangères menées par des acteurs étatiques. Les gouvernements peuvent l'appuyer en postulant que les équipements et logiciels électoraux constituent des infrastructures cruciales, et en prônant une norme internationale relative aux cyberattaques contre lesdites infrastructures.

Les gouvernements démocratiques doivent considérer les TEE comme des infrastructures cruciales et soutenir la norme approuvée par le G20, à savoir : Les États ne doivent pas mener ou soutenir en connaissance de cause une quelconque activité relevant des technologies de l'information et de la communication (...) qui endommagerait intentionnellement les infrastructures cruciales.

Plus délicate sera néanmoins la distinction à opérer entre d'une part, l'aide étrangère légitime (et défendable) encourageant la démocratie et l'intégrité électorale et d'autre part, l'ingérence électorale étrangère illégitime. Trop souvent, les défenseurs de l'ingérence étrangère observée récemment dans des élections démocratiques affirment que les agents russes n'ont fait qu'imiter les démocraties occidentales qui soutiennent la création de partis politiques en Afrique ou promeuvent des organisations de la société civile demandant des comptes aux gouvernements autoritaires. La meilleure façon pour les démocraties de contrer ces arguments fondés sur une fausse équivalence est d'énoncer clairement ce qui constitue et ne constitue pas un appui transnational légitime à la démocratie.

Les gouvernements démocratiques doivent joindre leurs forces pour mettre en place une convention internationale sur le rôle des gouvernements étrangers et de leurs agents dans les élections d'autres pays. Ils devraient notamment élaborer des normes internationales qui distinguent l'assistance transfrontière légitime des interventions illicites ou illégales.

Au-delà de l'ingérence étrangère par des acteurs étatiques, il n'existe pas non plus de règles ou de réglementations régissant le secteur émergent de la manipulation électorale. En dépit de tous les scandales et de toutes les pratiques contraires à l'éthique, des sociétés comme Cambridge Analytica ont pu changer de raison sociale et poursuivre leurs activités. Il est nécessaire d'instaurer une réglementation gouvernementale, des codes de conduite et des bonnes pratiques à l'intention des cabinets de conseil politique et de communication stratégique. Deux associations professionnelles basées sur une participation bénévole, l'International Association of Political Consultants et l'American Association of Political Consultants, ont élaboré des codes de conduite et pourraient servir de forum de concertation entre le secteur du conseil électoral, les gouvernements et la communauté en

faveur de l'intégrité électorale au sens large dans le but de créer et d'appliquer des normes transnationales contraignantes de déontologie, applicables aux activités de conseil électoral.

Il conviendrait que la communauté en faveur de l'intégrité électorale élabore des normes applicables aux cabinets transnationaux de conseil spécialisés dans les campagnes politiques, y compris aux sociétés de relations publiques et de communication stratégique, ainsi qu'aux experts en marketing numérique. Les réglementations devraient établir des procédures de certification régissant l'activité de ces consultants, et interdire aux sociétés qui violent les normes et les règles de consulting en campagnes électorales de poursuivre leurs missions.

Compte tenu du rôle central des technologies électorales électroniques dans la quasi-totalité des aspects du processus électoral, la fiabilité de la cybersécurité constitue un élément essentiel de l'intégrité des élections. Cependant la sécurité des TEE soulève plusieurs problèmes. Le manque de transparence et de coopération des principaux fournisseurs de TEE, très lents à s'adapter aux menaces numériques qui pèsent sur l'intégrité électorale, représente un obstacle majeur à la protection des processus électoraux démocratiques contre le piratage. Les responsables électoraux ne possèdent pas toujours les connaissances techniques requises pour se porter garants des systèmes qu'ils supervisent. Les organes de gestion des élections se soucient parfois davantage de la méfiance des électeurs liée aux risques de piratage de leurs systèmes que de la menace réelle d'ingérence extérieure[162]. Dans certains pays, l'achat de TEE est corrompu par des fournisseurs prêts à distribuer des pots-de-vin aux responsables des acquisitions en leur vendant des équipements onéreux, non sécurisés et inadaptés au niveau de développement local[163].

La communauté en faveur de l'intégrité électorale devrait aider ces OGE à acquérir une expertise en matière de bonnes pratiques de cybersécurité.

Certains OGE pourront nécessiter une assistance technique à court terme afin de réagir aux menaces que font peser les ingérences étrangères – ainsi que le piratage et les discours de haine incitant à la violence en contexte électoral – sur l'intégrité des élections. Dans ce type de cas, l'assistance technique internationale requise pour les aider à assurer le bon déroulement des élections devra être dispensée aussitôt après réception de la demande. Afin de permettre cette réactivité, nous conseillons la mise en place d'équipes permanentes de cybersécurité électorale pouvant être déployées immédiatement sur demande. Ces équipes pourraient être basées dans des organisations internationales existantes telles que la Division de l'assistance électorale des Nations Unies, des organisations régionales ou une nouvelle institution internationale. La rotation des postes techniques constituerait une bonne pratique de gouvernance numérique au sein de ces instances.

Bien qu'essentielle en termes d'intégrité électorale et de confiance du public dans le résultat des élections, aucune réglementation internationale ne régit le secteur des TEE. Plusieurs gouvernements et sociétés technologiques privées entretenant des liens étroits avec les pouvoirs publics de leur pays sont déjà fournisseurs de matériel électoral et de services d'appui aux élections. Rien ne garantit que ces fournisseurs ne se transformeront pas en instruments de politique étrangère plutôt qu'en pourvoyeurs indépendants de services électoraux. Les gouvernements autoritaires commercialisent de plus en plus de technologies à double emploi susceptibles d'assurer l'inscription et l'identification des électeurs, mais aussi potentiellement de permettre la surveillance des citoyens et des opposants par les pouvoirs publics.

Le secteur mondial des technologies électorales doit collaborer aux efforts internationaux d'élaboration de normes afin de protéger les informations numériques, le comptage des votes, la transmission des

résultats, mais aussi les équipements et logiciels contre l'intrusion, le piratage, la manipulation et l'ingérence par des acteurs intérieurs ou étrangers. Cette collaboration profiterait non seulement aux démocraties du monde entier, mais aussi aux sociétés technologiques spécialisées dans les élections et reconnues pour leur rôle de garant du respect de l'intégrité électorale.

Les fournisseurs d'équipements et de services électoraux devraient s'engager à respecter un code de conduite afin de garantir que leurs produits sont sécurisés, que leurs pratiques commerciales protègent les droits, la vie privée et les données des citoyens des pays clients, et que leurs pratiques d'achat sont honnêtes et transparentes. La communauté internationale en faveur de l'intégrité électorale devrait s'engager quant à elle à conditionner l'assistance électorale dispensée aux pays à la signature et au respect de ce code par les fournisseurs. L'élaboration de ce code de conduite devrait se dérouler dans le cadre d'une initiative multipartite impliquant la communauté en faveur de l'intégrité électorale, le Réseau mondial d'observateurs nationaux des élections et des partenaires internationaux.

VII. SYNTHÈSE DES RECOMMANDATIONS

La défense de l'intégrité électorale contre le mauvais usage des réseaux sociaux dépendra des choix et du comportement des entreprises et des grandes plateformes technologiques tout autant que de l'attitude des gouvernements, des personnalités politiques, des médias traditionnels, des organes de gestion des élections, et des citoyens. Pour protéger l'intégrité électorale à l'ère numérique, nous devrons renforcer les capacités de ses défenseurs et élaborer des normes communes sur l'utilisation acceptable des technologies numériques lors de la tenue d'élections. Les plateformes technologiques et les pouvoirs publics doivent prendre des mesures pour soutenir l'intégrité électorale.

RENFORCEMENT DES CAPACITÉS

Recommandation 1

Il faut impérativement consacrer davantage d'attention et de ressources à la promotion de l'intégrité électorale. Les pouvoirs publics, les organisations internationales, les fondations philanthropiques et la société civile doivent investir dans le recours à des spécialistes en technologie et le renforcement des capacités numériques, tout en favorisant les initiatives auprès des médias et en appuyant la constitution d'organes de gestion des élections qui protègent et promeuvent le principe d'intégrité. Toutes les parties prenantes intéressées doivent coopérer, collaborer et partager rapidement les informations relatives aux menaces pesant sur l'intégrité électorale. Ces efforts prendront les formes suivantes :

- Création d'un indice de la vulnérabilité électorale déterminant les élections qui nécessitent une étroite surveillance contre une éventuelle ingérence, les comportements en ligne usurpateurs coordonnés, la mésinformation ou encore la désinformation.

- Renforcement des capacités des partenariats nationaux de défense de l'intégrité des élections luttant contre la désinformation et soutien à l'amélioration de l'évaluation et du partage des bonnes pratiques.

- Financement des organisations de la société civile qui combattent les discours de haine, le harcèlement ciblé et l'incitation à la violence, notamment dans les périodes pré-électorales.

- Dispense d'une expertise à l'adresse des organes de gestion des élections en matière de bonnes pratiques liées à la cybersécurité.

- Soutien apporté aux démocraties dans l'élaboration de programmes technologiques civiques par le biais de l'enseignement du codage, notamment aux femmes et aux minorités, et de l'intégration de spécialistes techniques au sein des équipes gouvernementales.

Recommandation 2

Certains organes de gestion des élections pourront nécessiter une assistance technique à court terme afin de réagir aux menaces que font peser les ingérences étrangères – ainsi que le piratage et les discours de haine incitant à la violence en contexte électoral – sur l'intégrité des élections. Dans ce type de cas, l'assistance technique internationale requise pour les aider à assurer le bon déroulement des élections devra être dispensée aussitôt après réception de la demande. Afin de permettre cette réactivité, nous conseillons la mise en place d'équipes permanentes de cybersécurité électorale pouvant être déployées immédiatement sur demande. Ces équipes pourraient être basées dans des organisations internationales existantes telles que la Division de l'assistance électorale des Nations Unies, des organisations régionales ou une nouvelle institution internationale. La rotation des postes techniques constituerait une bonne pratique de gouvernance numérique au sein de ces instances.

RENFORCEMENT DES NORMES

Recommandation 3

Nous adhérons à l'appel de la Commission transatlantique sur l'intégrité des élections invitant les candidats, partis et groupes politiques à s'engager par écrit à rejeter les pratiques de campagnes politiques numériques trompeuses, à savoir : utilisation de données ou de documents volés, recours à des supports visuels altérés déformant les propos d'une personnalité à un degré de réalisme plus ou moins élevé (« shallow fakes » et « deep fakes »), publication de fausses images de nus (« deep nudes »), production, utilisation ou diffusion de documents falsifiés ou faux, ou encore collusion avec des gouvernements étrangers et leurs agents dans le but de manipuler une élection.

Recommandation 4

Les gouvernements démocratiques doivent joindre leurs forces afin d'élaborer une convention internationale sur le rôle des gouvernements étrangers et de leurs agents dans les élections d'autres pays. Il serait notamment judicieux qu'ils établissent des normes internationales opérant la distinction entre assistance transfrontière légitime et interventions illicites ou illégales.

Recommandation 5

Les gouvernements démocratiques doivent considérer les TEE comme des infrastructures cruciales et soutenir la norme approuvée par le G20, à savoir : Les États ne doivent pas mener ou soutenir en connaissance de cause une quelconque activité relevant des technologies de l'information et de la communication (...) qui endommagerait intentionnellement les infrastructures cruciales.

Recommandation 6

Les fournisseurs d'équipements et de services électoraux devraient s'engager à respecter un code de conduite afin de garantir que leurs produits sont sécurisés, que leurs pratiques commerciales protègent les droits, la vie privée

et les données des citoyens des pays clients, et que leurs pratiques d'achat sont honnêtes et transparentes. La communauté internationale en faveur de l'intégrité électorale devrait s'engager quant à elle à conditionner l'assistance électorale dispensée aux pays à la signature et au respect de ce code par les fournisseurs. L'élaboration de ce code de conduite devrait se dérouler dans le cadre d'une initiative multipartite impliquant a minima la communauté en faveur de l'intégrité électorale, le Réseau mondial d'observateurs nationaux des élections et des partenaires internationaux.

Recommandation 7

Il conviendrait que la communauté en faveur de l'intégrité électorale élabore des normes applicables aux cabinets transnationaux de conseil spécialisés dans les campagnes politiques, y compris aux sociétés de relations publiques et de communication stratégique, ainsi qu'aux experts en marketing numérique. Les réglementations devraient établir des procédures de certification régissant l'activité de ces consultants, et interdire aux sociétés qui violent les normes et les règles de consulting en campagnes électorales de poursuivre leurs missions.

ACTIONS À MENER PAR LES POUVOIRS PUBLICS

Recommandation 8

Les pays doivent adapter leurs réglementations sur la publicité politique à l'environnement en ligne. Les autorités publiques compétentes doivent :

- définir en droit la nature des publicités à visée politique ;
- obliger les plateformes de réseaux sociaux à rendre publiques toutes les informations relatives à l'achat de publicités, notamment l'identité réelle de l'annonceur, les montants dépensés, les critères de ciblage et l'identité des créateurs effectifs de l'annonce ;

- préciser en droit la taille minimale du segment de la population ciblée par les publicités ;

- légiférer sur l'arrêt de la diffusion des publicités numériques à visée politique au moins 48 heures avant la tenue d'élections.

Recommandation 9

Les pouvoirs publics doivent obliger les grandes plateformes Internet à communiquer à des tiers indépendants des données pertinentes concernant l'impact des réseaux sociaux sur la démocratie. Les plateformes doivent notamment :

- communiquer des données sécurisées (et respectant les règles de confidentialité) à des institutions universitaires certifiées afin qu'elles étudient les questions suivantes : existence éventuelle de biais favorables aux opinions extrémistes dans les algorithmes, impact des réseaux sociaux sur la polarisation politique et la consommation d'informations, décryptage de la corrélation entre discours de haine en ligne et violence hors ligne, etc. ;

- tenir à jour leurs comptes rendus sur la transparence afin de fournir au public des données sur le nombre de signalements de discours de haine et d'abus en ligne. Les données en question devraient porter, entre autres, sur les cas d'abus ciblés (selon des critères ethniques, de genre, d'orientation sexuelle ou d'affiliation religieuse) et la fréquence à laquelle ils visent différentes communautés ;

- déclarer les comptes ayant recours à des pratiques d'automatisation. Les plateformes doivent être passibles de pénalités financières en cas de comptes automatiques non déclarés comme tels (bots, etc.).

Recommandation 10

Les pouvoirs publics devraient promouvoir l'éducation aux usages numériques et aux médias dans les écoles ainsi que dans le cadre de programmes d'intérêt public destinés à l'ensemble de la population.

ACTIONS À MENER PAR PLATEFORME

Recommandation 11

Les plateformes devraient assurer la transparence accrue des publicités politiques.

- Les plateformes devraient laisser le choix aux utilisateurs d'accepter ou de refuser la publicité à des fins politiques.

- Les plateformes ne devraient accepter de vendre des espaces publicitaires qu'aux candidats, aux partis et aux groupes s'étant formellement engagés à éviter les pratiques de campagne trompeuses. Cet engagement deviendrait alors la norme contractuelle régissant l'approbation ou le refus d'une publicité donnée.

- Afin d'éviter que les financeurs ne se cachent derrière des noms d'organisations frauduleux, les plateformes devraient exiger la divulgation publique de l'identité des personnes finançant la publicité politique, quelle qu'elle soit.

Recommandation 12

Les plateformes de réseaux sociaux doivent élaborer des systèmes d'alerte précoce prenant en compte la désinformation en rapport avec des élections, les ingérences étrangères, les crimes et délits motivés par la haine, les menaces proférées à l'encontre des femmes, la violence et les dissuasions à se rendre aux bureaux de vote.

- Les plateformes doivent employer davantage de locuteurs de langues locales, sensibles au contexte culturel des régions où ils opèrent.

Afin de prévenir la diffusion virale des messages malveillants, des systèmes d'alerte précoce doivent permettre une intervention humaine afin de détecter les comptes et publications représentant une menace potentielle pour la bonne tenue des élections. Les contenus qui atteignent un certain degré de viralité devraient être modérés et examinés par des intervenants humains.

Recommandation 13

Les plateformes de réseaux sociaux devraient former une coalition visant à combattre les menaces numériques à l'encontre de la démocratie et de l'intégrité électorale, à l'instar des mesures prises pour lutter contre le terrorisme et l'exploitation des enfants. Les membres de la coalition se réuniraient à intervalles réguliers et élaboreraient des stratégies trans-plateformes pour détecter et limiter la portée de la désinformation et des discours de haine.

REMERCIEMENTS

Nous remercions les personnes et les institutions qui ont contribué aux travaux de la Commission pendant les délibérations.

Laura Jakli, doctorante à l'université de Californie, Berkeley, a piloté le comité restreint de chercheurs hébergé par le Center of Democracy, Development, and Rule of Law de l'université de Stanford qui a assisté Stephen Stedman dans ses travaux. Ce comité est composé de Sylvie Ashford, Carolyn Chun, Yingjie Fan et Whitney McIntosh. Laura Jakli et Samatha Bradshaw, doctorante (DPhil) à l'Oxford Internet Institute, ont apporté une contribution notable à la rédaction et à la révision du rapport. Young Lee et Eloise Duvillier ont assuré l'appui budgétaire et administratif à Stanford.

Declan O'Brien, Sebastian Brack, Li Ling Low et Stephanie Lewis de la Fondation Kofi Annan ont assuré un soutien organisationnel tout au long des travaux de la Commission. Bijan Farnoudi et Genna Ingold étaient responsables quant à eux de la communication et de la stratégie de sensibilisation.

Plusieurs universitaires et praticiens ont fait part de leurs avis à la Commission ; mentionnons à cet égard : Tanja Bosch, Pablo Boczkowski, Michelle Brown, Chipo Dendere, Katherine Ellena, Jonas Kaiser, Daphne Keller, Admire Mare, Mora Matassi, Pat Merloe, Eugenia Mitchelstein, Vasu Mohan, Joyojeet Pal et Erica Shein.

Le groupe principal de l'initiative sur l'intégrité électorale de la Fondation Kofi Annan a joué un rôle central dans le regroupement des idées et recommandations formulées.

La Fondation Kofi Annan souhaite également remercier le groupe de partenaires de financement mobilisés pour soutenir les travaux de la Commission, un panel à la fois diversifié et équilibré : la Chancellerie fédérale autrichienne, l'Open Society Foundation, la Fondation des Nations Unies, William H. Draper III, Facebook et Twitter.

La présence de différents acteurs du secteur privé, des gouvernements, des fondations et des particuliers a été constructive, tout en préservant le caractère indépendant de la Commission.

À PROPOS DE LA FONDATION KOFI ANNAN

La Fondation Kofi Annan est une organisation indépendante à but non lucratif qui œuvre à la promotion d'une meilleure gouvernance mondiale et au renforcement de la capacité des populations et des pays à bâtir un monde plus juste et pacifié.

Elle mobilise la volonté politique pour venir à bout des menaces qui pèsent sur la paix, le développement et les droits de l'homme. Dans la plupart des cas, nous possédons l'expertise et les données factuelles nécessaires pour résoudre les problèmes urgents, tels que la pauvreté, les conflits armés et la mauvaise gouvernance. Mais le leadership ou la volonté politique pour concevoir et fournir les solutions font souvent défaut. La Fondation rassemble des acteurs à même d'exercer une influence et de mettre leur leadership au service de la lutte contre les principaux fléaux qui touchent la planète.

BIBLIOGRAPHIE

1 Nathaniel Persily. *The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms*, report for the Kofi Annan Commission on Elections and Democracy in the Digital Age, 2019. **2** Pablo J. Boczkowski, Eugenia Mitchelstein et Mora Matassi, *Social Media and Democracy in Latin America*, rapport à l'intention de la Commission Kofi Annan sur les élections et la démocratie à l'ère du numérique, 2019. **3** Boczkowski, Mitchelstein et Matassi, *Social Media and Democracy in Latin America*. Voir également Tanja Bosch, Chipo Dendere et Admire Mare, *The Effect of Social Media on Democracy and Elections in Africa*, rapport à l'intention de la Commission Kofi Annan sur les élections et la démocratie à l'ère du numérique, 2019. **4** Bosch, Dendere et Mare, *The Effect of Social Media on Democracy and Elections in Africa*. **5** Commission mondiale sur les élections, la démocratie et la sécurité, Deepening Democracy: *A Strategy for Improving the Integrity of Elections Worldwide* (Genève : Fondation Kofi Annan, 2012). **6** « Electoral Integrity Assessments », *Fondation internationale pour les systèmes électoraux*, www.ifes.org/issues/electoral-integrity-assessments. **7** Commission mondiale sur les élections, la démocratie et la sécurité, *Deepening Democracy,* 24-26. Mutual security as a precondition for democracy comes from Robert Dahl, *Polyarchy: Participation and Opposition* (New Haven : Yale University Press, 1971). **8** James S. Fishkin, *Democracy and Deliberation: New Directions for Democratic Reform* (New Haven : Yale University Press, 1991). **9** Christopher H. Achen et Larry M. Bartels, *Democracy for Realists: Why Elections Do Not Produce Responsive Government* (Princeton : Princeton University Press, 2016). **10** Murat Somer et Jennifer McCoy, « Déjà vu? Polarization and Endangered Democracies in the 21st Century », *American Behavioral Scientist* 62, nº 1 (2018) : 3-15. **11** Lührmann *et al.*, « State of the World 2018: Democracy Facing Global Challenges », *Democratization* 26, nº 6 (2019) : 895-915. **12** Nolan McCarty, Keith T. Poole et Howard Rosenthal, *Polarized America: the Dance of Ideology and Unequal Riches* (Cambridge : MIT Press, 2006) ; Jacob Jensen *et al.*, « Political Polarization and the Dynamics of Political Language: Evidence from 130 Years of Partisan Speech », *Brookings Papers on Economic Activity* 43, nº 2 (2012) : 1–81 ; Matthew Gentzkow, « Polarization in 2016 », livre blanc, *Toulouse Network for Information Technology*, 2016. **13** Yochai Benkler, Rob Faris et Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (New York : Oxford University Press, 2018). **14** Benkler, Faris et Roberts, *Network Propaganda.* **15** Benkler, Fari et Roberts, *Network Propaganda.* **16** Edda Humprecht, « Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies », *Information, Communication, and Society* 22, nº 13 (2019) : 1973-88. **17** Humprecht, « Where 'Fake News' Flourishes », 1973-88. **18** Lührmann *et al.*, « Democracy Facing Global Challenges » 895-915. **19** Noam Gidron, James Adams et Will Horne, « Toward a Comparative Research Agenda on Affective Polarization in Mass Publics », *APSA Comparative Politics Newsletter* 29 (2019) : 30-36 ; Jennifer McCoy et Murat Somer, « Toward a Theory of Pernicious Polarization and How It Harms Democracies: Comparative Evidence and Possible Remedies », *The ANNALS of the American Academy of Political and Social Science* 681, nº 1 (2019) : 234- 271. **20** Nic Newman *et al.*, « Reuters Institute Digital News Report 2019 », *Reuters Institute for the Study of Journalism*, 2019 ; Ronald Inglehart *et al.*, « World Values Survey: All Rounds-Country-Pooled Datafile 1981-2014 » (Madrid : JD Systems Institute, 2014).

21 Pippa Norris, *Why Electoral Integrity Matters* (Cambridge : Cambridge University Press, 2014). **22** McCarty *et al.*, *Polarized America*, 78-81. **23** Herman Winkler, « The Effect of Income Inequality on Political Polarization: Evidence from European Regions, 2002-2014 », *Economics and Politics* 31, nº 2 (2019) : 137-162. **24** Benjamin Reilly, *Democracy in Divided Societies: Electoral Engineering for Conflict Management (Cambridge : Cambridge University Press, 2001)* ; Lee Drutman, « The Case for Proportional Voting », National Affairs 34 (2017) : 50-63. **25** Ryan D. Enos, *The Space between Us: Social Geography and Politics* (Cambridge : Cambridge University Press, 2017) ; Dante J. Scala et Kenneth M. Johnson, « Political Polarization along the Rural-Urban Continuum? The Geography of the Presidential Vote, 2000–2016 », *The ANNALS of the American Academy of Political and Social Science* 672, nº 1 (2017) : 162-184. **26** Jonas Pontusson et David Rueda, « Inequality as a Source of Political Polarization: A Comparative Analysis of Twelve OECD Countries » dans *Democracy, Inequality, and Representation*, éd. Pablo Beramendi et Christopher J. Anderson (New York : Russell Sage Foundation, 2008), 312-353. **27** Drutman, « The Case for Proportional Voting ». **28** McCoy et Somer, « Toward a Theory of Pernicious Polarization », 234-271. **29** Cass R. Sunstein, *Republic. Com* (Princeton : Princeton University Press, 2001). **30** Carole Cadwalladr, « Google Is Not 'Just' a Platform. It Frames, Shapes and Distorts How We See the World », *The Guardian,* 11 décembre 2016, sec. Opinion, https://www.theguardian.com/commentisfree/2016/dec/11/google-frames-shapes-and-distorts-how-we-see-world. **31** Kelly Weill, « How YouTube Built a Radicalization Machine for the Far-Right ». *The Daily Beast,* 17 décembre 2018, https://www.thedailybeast.com/how-youtube-pulled-these-men-down-a-vortex-of-far-right-hate. Voir également Kevin Roose, « The Making of a YouTube Radical », *The New York Times*, 8 juin 2019, https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html. **32** Richard Fletcher et Rasmus Kleis Nielsen, « Are People Incidentally Exposed to News on Social Media? A Comparative Analysis », *New Media & Society* 20, nº 7 (2018) : 2450-2468. **33** Matthew Barnidge, « Exposure to Political Disagreement in Social Media versus Face-to-Face and Anonymous Online Settings », *Political Communications*. 34, nº 2 (2017) : 302-321. **34** Pablo Barbera, « How Social Media Reduces Mass Political Polarization. Evidence from Germany, Spain, and the U.S ». *Document de travail*, 2014. **35** Christopher A. Bail *et al.*, « Exposure to Opposing Views on Social Media can Increase Political Polarization », *Proceedings of the National Academy of Sciences* 115, nº 37 (2018) : 9216-9221. **36** Manoel Horta Ribeiro *et al.*, « Auditing Radicalization Pathways on YouTube », 2019, http://arxiv.org/abs/1908.08313. **37** Kevin Munger et Joseph Phillips, « A Supply and Demand Framework for YouTube Politics », *Document de travail*, 2019. **38** « Public Statement from the Co-Chairs and European Advisory Committee of Social Science One », 11 décembre 2019, https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one. **39** Jenni Marsh et Tara Mulholland, « How the Christchurch Terrorist Attack Was Made for Social Media », *CNN*, 16 mars 2019, https://www.cnn.com/2019/03/15/tech/christchurch-internet-radicalization-intl/index.html ; Kevin Roose, « On Gab, an Extremist-Friendly Site, Pittsburgh Shooting Suspect Aired His Hatred in Full », *The New York Times*, 28 octobre 2018, https://www.nytimes.com/2018/10/28/us/gab-robert-bowers-pittsburgh-synagogue-shootings.html. **40** Timothy McLaughlin, « How WhatsApp Fuels Fake News

and Violence in India », *Wired*, 12 décembre 2018, https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/. **41** Amalini De Sayrah, « Facebook Helped Foment Anti-Muslim Violence in Sri Lanka. What Now? », *The Guardian*, 5 mai 2018, https://www.theguardian.com/commentisfree/2018/may/05/facebook-anti-muslim-violence-sri-lanka. **42** Paul Mozur, « A Genocide Incited on Facebook, With Posts From Myanmar's Military », *The New York Times,* 18 octobre 2018, section « Technology », https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html. **43** « Amnesty Reveals Alarming Impact of Online Abuse against Women », *Amnesty International*, 20 novembre 2017, https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/. **44** Adriane Van Der Wilk, « Cyber Violence and Hate Speech Online against Women », *Commission du Parlement européen chargée des droits de la femme et de l'égalité des genres*, septembre 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf. **45** David Kaye, « UN Experts Urge States and Companies to Address Online Gender-Based Abuse but Warn against Censorship », *OHCHR*, 8 mars 2017, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317&LangID=E. **46** « Toxic Twitter - The Silencing Effect ». *Amnesty International*, mars 2018, www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-5/. **47** Lauren Etter, « Rodrigo Duterte Turned Facebook Into a Weapon, With a Little Help from Facebook », *Bloomberg News*, 7 décembre 2017, https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook. **48** Carly Nyst et Nick Monaco, « State-Sponsored Trolling: How Governments are Deploying Disinformation as Part of Broader Digital Harassment Campaigns », *Institute for the Future*, 2018, http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf. **49** Nina Jankowicz, « How Disinformation Became a New Threat to Women », *World Policy*, 20 décembre 2017, https://worldpolicy.org/2017/12/20/how-disinformation-became-a-new-threat-to-women/. **50** Amnesty International, « Toxic Twitter—The Silencing Effect ». **51** Le dernier jugement de la Cour suprême opposé à la réglementation des discours de haine a été prononcé à l'unanimité en juin 2017 dans l'affaire opposant *Matal à Tam, 52 U.S.* (2017). https://www.supremecourt.gov/opinions/16pdf/15-1293_1o13.pdf. **52** Daphne Keller et Paddy Leerssen, « Facts and Where to Find Them: Empirical Research on Internet Platforms and Online Speech » dans *Social Media and Democracy: The State of the Field*, éd. Nathaniel Persily et Joshua Tucker (New York : Cambridge University Press, à paraître). **53** Steve Stecklow, « Why Facebook Is Losing the War on Hate Speech in Myanmar », *Reuters*, 15 août 2018, https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/. **54** Tarelton Gillespie, *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions That Shape Social Media* (New Haven : Yale University Press, 2018). **55** « Code de conduite de l 'Union européenne », *Commission européenne*, 4 février 2019, https://ec.europa.eu/info/policies/justice- and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en. **56** Keller et Leerssen, « Facts and Where to Find Them ». **57** « Germany to Enforce Hate Speech Law », *BBC News*, section « Technology », 1er janvier 2018, https://www.bbc.com/news/technology-42510868. **58** Daphne Keller, « Internet Platforms: Observations on Speech, Danger, and Money », Hoover Working Group on National Security, Technology, and Law, Aegis Series, article nº 1807 (2018) : 2. **59** David Kaye, « Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression » (juin 2017) : 4. https://www.ohchr.org/Documents/Issues/Opinion/Legislation/

OL-DEU-1-2017.pdf. **60** Samantha Bradshaw, Lisa-Maria Neudert et Philip Howard, « Government Responses to the Malicious Use of Social Media », *NATO Strategic Communications Centre of Excellence*, novembre 2018, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/01/Nato-Report.pdf. **61** David Kaye et Fionnuala Ni Aolain, « Mandates of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; and the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism », 2019, https://freedex.org/wp-content/blogs.dir/2015/files/2019/04/OL-AUS-04.04.19-5.2019-2.pdf. **62** Jacob Mchangama et Joelle Fiss, « Germany's Online Crackdowns Inspire the World's Dictators », *Foreign Policy*, 6 novembre 2019, foreignpolicy.com/2019/11/06/germany-online-crackdowns-inspired-the-worlds-dictators-russia-venezuela-india/. **63** Access Now, « Joint Letter on Internet Shutdown in Uganda », *CIPESA*, 24 février 2016, https://cipesa.org/2016/02/joint-letter-on-internet-shutdown-in-uganda/. **64** Jan Rydzak, « Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India », 7 février 2019, https://ssrn.com/abstract=3330413. **65** Louise Matsakis et Issie Lapowsky, « Don't Praise the Sri Lankan Government for Blocking Facebook », *Wired*, 23 avril 2019, https://www.wired.com/story/sri-lanka-bombings-social-media-shutdown/. **66** Daniel Arnaudo *et al.*, « Political and Economic Implications of Authoritarian Control of the Internet » *in* Jonathan Butts et Sujeet Shenoi, *Critical Infrastructure Protection VII*. (Berlin, Heidelberg : Springer Berlin Heidelberg, 2013), 3-19. **67** Abdi Latif Dahir, « Internet Shutdowns Are Costing African Governments More than We Thought », *Quartz Africa*, 28 septembre 2017, https://qz.com/africa/1089749/internet-shutdowns-are-increasingly-taking-a-toll-on-africas-economies/. **68** Access Now, « Joint Letter on Internet Shutdown in Uganda ». **69** Roderick Fanou *et al.*, « OONI - Open Observatory of Network Interference », 30 avril 2019, https://ooni.org/. **70** Ribeiro *et al.*, « Auditing Radicalization Pathways on YouTube ». **71** Christopher Ross, « Reshma Saujani's Ambitious Plan for Technology », *The Wall Street Journal*, 6 novembre 2014, https://www.wsj.com/articles/reshma-saujanis-ambitious-plan-for-technology-1415237831. **72** « Girls Who Code: Annual Report 2018 », girlswhocode.com/2018report/. **73** Ross, « Reshma Saujani's Ambitious Plan for Technology ». **74** Kimiko de Freytas-Tamura, « Kenyan Election Official Is Killed on Eve of Vote », *The New York Times*, 31 juillet 2017, section « World », https://www.nytimes.com/2017/07/31/world/africa/chris-musando-kenya-election-official-dead.html. **75** Nanjira Sambuli, « The Importance of Monitoring Online Hate Speech », *Deutsche Welle*, 3 octobre 2016, https://www.dw.com/en/the-importance-of-monitoring-online-hate-speech/a-19104789. **76** Ibid. **77** Susan Benesch, « Countering Dangerous Speech to Prevent Mass Violence during Kenya's 2013 Elections », *Berkman Center for Internet and Society*, 9 février 2014, https://www.ushmm.org/m/pdfs/20140212-benesch-kenya.pdf. **78** Kagonya Awori, « Umati Final Report », *iHub Research*, juin 2013, https://preventviolentextremism.info/sites/default/files/Umati%20Final%20Report.pdf. **79** Ibid. **80** Luciano Floridi, « Fake News and a 400-Year-Old Problem: We Need to Resolve the 'Post-Truth' Crisis », *The Guardian*, 29 novembre 2016, www.theguardian.com/technology/2016/nov/29/fake-news-echo-chamber-ethics-infosphere-internet-digital. **81** Hunt Allcott et Matthew Gentzkow, « Social Media and Fake News in the 2016 Election », *Journal of Economic Perspectives* 31, n° 2 (2017) : 211-36. **82** Stephen Coleman, « The Digital Difference: Media Technology and the Theory of Communication Effects », *Journal of Communication* 67, n° 6 (2017) : E7-E8. **83** Ralph Schroeder, « Does Google Shape What we Know? » *Prometheus* 32, n° 2 (2014) : 145-160. **84** Tarleton Gillespie, « The Relevance of Algorithms » *in* : Tarleton Gillespie, Pablo J. Boczkowski et Kirsten A. Foot, éd. *Media*

Technologies: Essays on Communication, Materiality, and Society (Cambridge : MIT Press, 2014), 167-194. **85** Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (New York : Knopf, 2016) ; James Williams, *Stand Out of Our Light: Freedom and Resistance in the Attention Economy* (Cambridge : Cambridge University Press, 2018). **86** Benkler, Faris et Roberts, *Network Propaganda*; Marchal *et al.*, « Junk News during the EU Parliamentary Elections », *Oxford Internet Institute*, Data Memo 2019.3. **87** Craig Silverman, « This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook », *BuzzFeed News*, 16 novembre 2016, www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook. **88** Joshua Tucker *et al.*, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature* (William and Flora Hewlett Foundation, 2018). **89** Claire Wardle et Hossein Derakhshan, « Information Disorder: Toward and Interdisciplinary Framework for Research and Policy Making », Rapport du conseil de l'Europe DGI (2017) 09. *Conseil de l'Europe*, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html. **90** Gordon Pennycook et David Rand, « Assessing the Effect of 'Disputed' Warnings and Source Salience on Perceptions of Fake News Accuracy », *Document de travail*, 2017, 10.2139/ssrn.3035384. **91** Allcott et Gentzkow, « Social Media and Fake News in the 2016 Election ». **92** Andrew Guess, Brendan Nyhan et Jason Reifler, « Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 US Presidential Campaign », *Conseil européen de la recherche 9* (2018). **93** Samantha Bradshaw *et al.*, « Sourcing and Automation of Political News and Information over Social Media in the United States, 2016-2018 », *Political Communication* (2019) : 1-21. **94** Lisa-Maria Neudert, Philip Howard et Bence Kollanyi, « Sourcing and Automation of Political News and Information During Three European Elections », *Social Media+ Society* 5, nº 3 (2019) : 2056305119863147. **95** Freja Hedman *et al.*, « News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter », *Oxford Internet Institute*, Data Memo 2018.3. **96** Caio Machado *et al.*, « News and Political Information Consumption in Brazil: Mapping the First Round of the 2018 Brazilian Presidential Election on Twitter », *Oxford Internet Institute*, Data Memo 2018.4. **97** Caio Machado, « WhatsApp's Influence in the Brazilian Election and How It Helped Jair Bolsonaro Win ». *Council on Foreign Relations*, 13 novembre 2018, www.cfr.org/blog/whatsapps-influence-brazilian-election-and-how-it-helped-jair-bolsonaro-win. **98** Chico Mares et Clara Becker, « Só 4 Das 50 Imagens Mais Compartilhadas Por 347 Grupos de WhatsApp São Verdadeiras », https://piaui.folha.uol.com.br/lupa/wp-content/uploads/2018/10/Relat%C3%B3rio-WhatsApp-1-turno-Lupa-2F-USP-2F-UFMG.pdf. **99** Rafael Evangelista et Fernanda Bruno, « WhatsApp and Political Instability in Brazil: Targeted Messages and Political Radicalization », Data-Driven Elections: Workshop Papers, *Surveillance Studies Centre*, 2019. https://www.sscqueens.org/sites/sscqueens.org/files/evangelista_bruno-2019-04.pdf. **100** Vidya Narayanan *et al.*, « Polarization, Partisanship and Junk News Consumption over Social Media in the US », *Oxford Internet Institute*, Data Memo 2018.1. **101** Andrew Guess, Jonathan Nagler et Joshua Tucker, « Less than you Think: Prevalence and Predictors of Fake News Dissemination on Facebook », *Science Advances* 5, nº 1 (2019) : eaau4586. **102** Guess, Nagler et Tucker, « Less than You Think ». **103** Jamie Hitchen *et al.*, « WhatsApp and Nigeria's 2019 Elections: Mobilizing the People, Protecting the Vote ». Abuja : Centre for Democracy and Development, https://www.cddwestafrica.org/whatsapp-nigeria-2019-elections/. **104** Bradshaw, Neudert et Howard, « Government Responses to the Malicious Use of Social Media ». **105** Nathaniel Persily et Joshua Tucker, « Introduction » *in : Social Media and Democracy: The State of the Field*,

éd. Nathaniel Persily et Joshua Tucker (New York : Cambridge University Press, à paraître). **106** Andrew Chadwick, The Hybrid Media System: Politics and Power (Oxford : Oxford University Press, 2013). **107** Persily et Tucker, *Social Media and Democracy.* **108** Sam Wineburg, *Why Learn History (When It's Already on Your Phone)* (Chicago : University of Chicago Press, 2018), 139-159. **109** « New Challenges for Democracy: Elections in Times of Disinformation », *Instituto Nacional Electoral*, juin 2019, 4-5. **110** Ibid., 7. **111** Ibid., 7. **112** Ibid., 8. **113** Ibid., 9. **114** Ibid., 12. **115** Ibid., 9-11. **116** Ibid., 12-13. **117** Ibid., 14-15. **118** Ibid., 16. **119** Vasu Mohan, Maya Jacobs, Tana Azuaje, Kyle Lemargie et Carla Chianese, « The Race Against SARA and Hoaxes in Indonesian Elections », Document de travail *International Foundation for Electoral Systems*, 20 août 2019, 3. **120** Vasu Mohan et Catherine Barnes, « Countering Hate Speech in Elections: Strategies for Electoral Management Bodies », livre blanc, *International Foundation for Electoral Systems*, janvier 2018, ivi. https://www.ifes.org/sites/default/files/2017_ifes_countering_hate_speech_white_paper_final.pdf. **121** Ibid., 20-34. **122** Mohan *et al*., « The Race Against SARA1 and Hoaxes2 in Indonesian Elections », 4. **123** Ibid., 6. **124** Fanny Potkin et Agustinus Beo de Costa, « Fact-checkers vs. hoax peddlers: a fake news battle ahead of Indonesia's election », *Reuters*, 10 août 2019, https://www.reuters.com/article/us-indonesia-election-fakenews-insight/fact-checkers-vs-hoax-peddlers-a-fake-news-battle-ahead-of-indonesias-election-idUSKCN1RM2ZE. **125** Mohan *et al*., « The Race Against SARA1 and Hoaxes2 in Indonesian Elections », 6-7. **126** Ibid., 8. **127** « Update on Local Election Results in West Kalimantan And Papua », rapport nº 50, *Institute for Policy Analysis of Conflict*, août 2018, 6. http://file.understandingconflict.org/file/2018/08/IPAC_Report_50_Update.pdf. **128** Erika Franklin Fowler *et al*., « Political Advertising Online and Offline », *Document de travail*, https://web.stanford.edu/~gjmartin/papers/Ads_Online_and_Offline_Working.pdf. **129** Jessica Baldwin-Philippi, « The Myths of Data-Driven Campaigning », *Political Communication* 34, nº 4 (2017) : 627-633. **130** Jeff Chester et Kathryn Montgomery, « Follow the Tech: Emerging Digital Practices in the 2020 Election », Data-Driven Elections: Workshop Papers, *Surveillance Studies Centre*, 2019. https://www.sscqueens.org/sites/sscqueens.org/files/chester_montgomery-2019-04.pdf. **131** Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (London: Penguin, 2016). **132** Robert S. Mueller, « Report on the Investigation into Russian Interference in the 2016 Presidential Election (Vol. I of II) » (Washington, DC : US Department of Justice, 2019). **133** Philip N. Howard, Bhrath Ganesh et Dimitra Liotsiu, « The IRA, Social Media and Political Polarization in the United States, 2012-2018 », *Computational Propaganda Research Project*, Université d'Oxford, 2019, https://assets.documentcloud.org/documents/5632779/IRA-Report-2018.pdf ; Rene DiResta *et al*., « The Tactics & Tropes of the Internet Research Agency ». *New Knowledge Whitepaper*, 2018. **134** Shannon McGregor, Bridget Barrett et Daniel Kreiss, « Barely Legal: Digital Politics and Foreign Propaganda », *Document de travail*, 2019. https://digitalpoliticalethics.weebly.com/uploads/5/0/9/9/50994643/mcgregorbarrettkreissapsa19_submit.pdf. **135** Nick Clegg, « Facebook, Elections and Political Speech ». Facebook Newsroom, 24 septembre 2019, about.fb.com/news/2019/09/elections-and-political-speech/. **136** « Read the Letter Facebook Employees Sent to Mark Zuckerberg About Political Ads », *The New York Times*, 28 octobre 2019, www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-letter.html. **137** « Nigeria National Elections: 2015 Nigeria Election Observation Report », *International Republication Institute*, 28 mars 2015, 5. http://www.iri.org/2015%20Nigeria%20Election%20Observation%20Report/1/assets/basic-html/index.html#III. **138** « Abuja Accord On the Prevention of Violence and Acceptance of Elections Results by Presidential

Candidates and Chairpersons of Political Parties contesting the 2015 General Elections », *Institut international pour la démocratie et l'assistance électorale*, 2015, https://www.idea.int/sites/default/files/codesofconduct/Abuja%20Accord%20January%202015.pdf. **139** International Republication Institute, « Nigeria National Elections », 5. **140** Institut international pour la démocratie et l'assistance électorale, « Abuja Accord », 2. **141** International Republication Institute, « Nigeria National Elections », 6. **142** The Associated Press, « Mozambique Peace Accord Is Signed, Paving Way for Elections », *The New York Times*, 6 août 2019, www.nytimes.com/2019/08/06/world/africa/mozambique-peace-accord-signed-paves-way-for- elections.html. **143** International Republication Institute, « Nigeria National Elections », 5. **144** Fidelis Mbah, « Nigeria Elections: Presidential Candidates Sign 'Peace Deal », *Al Jazeera*, 13 février 2019, www.aljazeera.com/news/2019/02/nigeria-elections-presidential-candidates-sign-peace-deal-190213154706618.html. **145** Michael McFaul et Bronte Kass, « Understanding Putin's Intentions and Actions in the 2016 US Presidential Election » *in* : Michael McFaul, *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, 2019, 1-16. **146** « HPSCI Minority Open Hearing Exhibits », U.S House of Representatives Permanent Select Committee on Intelligence (HPSCI), Minority Report, 1er novembre 2017. **147** Shelby Grossman, Daniel Bush et Renee DiResta, « Evidence of Russia-Linked Influence Operations in Africa », *Stanford Internet Observatory*, 29 octobre 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_pdf. **148** Steven Lee Myers et Paul Mozur, « China Is Waging a Disinformation War Against Hong Kong Protesters », *The New York Times*, 14 août 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html. **149** FireEye Intelligence, « Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East », *FireEye Threat Research*, 21 août 2018, https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html. **150** Adam Satariano, « Ireland's Abortion Referendum Becomes a Test for Facebook and Google ». *The New York Times*. 25 mai 2018, https://www.nytimes.com/2018/05/25/technology/ireland-abortion-vote-facebook-google.html. **151** Hannes Grassegger et Mikael Krogerus, « The Data That Turned the World Upside Down », *Vice News*, 28 janvier 2017, www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win. **152** Colin Bennett et Smith Oduro-Marfo, « Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities », document de l'Office of the Information Commissioner (Royaume-Uni) présenté lors de l'édition 2019 de l'International Conference of Data Protection and Privacy Commissioners (ICDPPC), https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf. **153** Baldwin-Philippi, « The Myths of Data-Driven Campaigning » ; Daniel Kreiss, « Micro-Targeting, the Quantified Persuasion », *Internet Policy Review* 6, no 4 (2017) : 1-14. **154** Tactical Tech Data and Politics Team, « Personal Data: Political Persuasion. Inside the Influence Industry », *Tactical Tech*, https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry. **155** Samantha Bradshaw et Philip Howard, « The Global Disinformation Disorder: 2019 Global Inventory of Social Media Manipulation », document de travail de l'Oxford Internet Institute 2019.3. Oxford, R.-U. : Project on Computational Propaganda. **156** Jane Lytvynenko et Logan McDonald, « Hundreds Of Propaganda Accounts Targeting Iran And Qatar Have Been Removed From Facebook », *BuzzFeed News*, 7 octobre 2019, www.buzzfeednews.com/article/janelytvynenko/uae-propaganda. **157** Michael Riley, Lauren Etter et Bibhudatta Pradhan,

« A Global Guide to State-Sponsored Trolling », Bloomberg News, 19 juillet 2018, https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/. **158** Jonathan Corpus Ong et Jason Vincent A. Cabanes, « Architects of Networked Disinformation », *Newton Tech4Dev Network*, 2018, http://newtontechfordev.com/wp-content/uploads/2018/02/Architects-of-Networked-Disinformation-Executive-Summary-Final.pdf. **159** Nic Cheeseman, Gabrielle Lynch et Justin Willis, « Digital Dilemmas: The Unintended Consequences of Election Technology », *Democratization* 25 nº 8 (2018) : 1397-1418. **160** Herbert Lin, Alex Stamos, Nathaniel Persily et Andrew Grotto, « Increasing the Security of the US Election Infrastructure » *in* : Michael McFaul, *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, 2019, 17-26. **161** Ibid. **162** Peter Wolf, « Cybersecurity and Elections: An International IDEA Round-Table », *Institut international pour la démocratie et l'assistance électorale*, 8 juillet 2017, www.idea.int/news-media/news/cybersecurity-and-elections-international-idea-round-table-summary. **163** Cheeseman, Lynch et Willis, « Digital Dilemmas », 1397-1418.

En 2018, Kofi Annan, Président de la Fondation portant son nom, mettait sur pied la Commission Kofi Annan sur les élections et la démocratie à l'ère du numérique. Composée de personnalités issues des secteurs public, privé et de la société civile se prévalant d'une expérience de haut niveau dans les affaires gouvernementales, les technologies, le monde universitaire ou encore les médias, la Commission a été chargée par M. Annan d'étudier les perspectives et les défis que présentent les innovations technologiques pour garantir l'intégrité électorale.

Le présent rapport rend compte des principales conclusions de l'étude et des consultations menées par la Commission, ainsi que de ses recommandations visant une utilisation des nouvelles technologies, des plateformes de réseaux sociaux et des outils de communication à même de concrétiser, sans contraintes, les aspirations des citoyens en matière de gouvernance démocratique.

Publié par

Kofi Annan FOUNDATION

Towards a fairer, more peaceful world