



Doc. 15028

08 janvier 2020

La démocratie piratée? Comment réagir?

Rapport¹

Commission des questions politiques et de la démocratie

Rapporteur: M. Frithjof SCHMIDT, Allemagne, Groupe des socialistes, démocrates et verts

Résumé

Le rapport analyse l'impact de la désinformation sur la démocratie, notamment via internet et les médias sociaux. Il souligne la nécessité d'améliorer le contenu et l'architecture d'internet, de renforcer la résilience des sociétés et des systèmes démocratiques européens, de lutter contre la désinformation, d'investir dans un journalisme de qualité et de préserver la liberté d'expression et le pluralisme politique et des médias, en particulier dans le contexte des élections.

Afin de relever les défis de la désinformation, les Etats membre du Conseil de l'Europe sont invités à mettre en œuvre un certain nombre de stratégies dans une perspective européenne et mondiale, notamment en ce qui concerne les campagnes électorales axées sur les données tirées des médias sociaux et l'utilisation des données à caractère personnel lors d'élections, la promotion de compétences en matière de culture numérique, les initiatives de vérification des faits et la transparence des publicités à caractère politique en ligne, ainsi que l'accès des chercheurs aux données, la coopération entre agences de sécurité, des cadres d'autorégulation pour les entreprises de médias et des réformes judiciaires appropriées. La commission des questions politiques et de la démocratie soutient les efforts de la Commission de Venise en vue d'élaborer une liste de principes pour l'utilisation des technologies numériques dans le contexte des élections.

1. Renvoi en commission: Décision du Bureau, renvoi 4353 du 22 janvier 2018.



Sommaire

Page

A. Projet de résolution	3
B. Exposé des motifs par M. Frithjof Schmidt, rapporteur	6
1. Introduction	6
2. L'ampleur du problème	7
3. Manipulation des processus de formation des opinions démocratiques et questions relatives à la vie privée pendant les élections	9
4. Travaux pertinents du Conseil de l'Europe	11
5. Action de l'Union européenne et Code sur la désinformation autorégulé par l'industrie: est-ce suffisant?	14
6. Réglementation et éducation: les cas de l'Allemagne, de la France et de la Suède	16
7. Conclusions	18

A. Projet de résolution²

1. L'Assemblée parlementaire est préoccupée par l'ampleur de la pollution de l'information dans un monde de plus en plus polarisé et numériquement connecté, par la multiplication des campagnes de désinformation visant à façonner l'opinion publique, par les tendances à la manipulation et aux ingérences étrangères dans le processus électoral, ainsi que par les comportements abusifs et l'intensification des propos haineux sur internet et les médias sociaux, qui sont autant de défis posés à la démocratie, et notamment aux processus électoraux, dans l'ensemble des États membres du Conseil de l'Europe.
2. En ce qui concerne les cyber-attaques, l'Assemblée renvoie aux problématiques soulevées dans la [Résolution 2217 \(2018\)](#) et la [Recommandation 2130 \(2018\)](#) «Problèmes juridiques posés par la guerre hybride et obligations en matière de droits de l'homme», en particulier en ce qui concerne les nombreux cas de campagnes de désinformation de masse visant à porter atteinte à la sécurité, à l'ordre public et aux processus démocratiques pacifiques, ainsi qu'à la nécessité de développer des outils pour protéger la démocratie des «armes de l'information».
3. Internet et les médias sociaux imprégnant de plus en plus le paysage politique, l'Assemblée met en avant la nécessité d'améliorer le contenu et l'architecture d'internet, de renforcer la résilience des sociétés et des systèmes démocratiques européens, de lutter contre la désinformation, d'investir dans un journalisme de qualité, de préserver la liberté d'expression ainsi que le pluralisme politique et des médias, en particulier dans le contexte des élections.
4. L'Assemblée est d'avis que les campagnes électorales axées sur les données tirées des médias sociaux, basées sur la segmentation et le profilage des utilisateurs, en particulier les publicités occultes diffusées sur les plateformes et visant des électeurs potentiels, sont un phénomène croissant qui devrait être mieux régulé afin d'assurer la transparence et la protection des données, et de gagner la confiance du public. En particulier, l'Assemblée:
 - 4.1. salue le travail accompli par le Conseil de l'Europe dans le domaine de la protection des données à caractère personnel et des droits électoraux, notamment la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108) et sa pertinence concernant les droits électoraux, ainsi que les autres instruments non contraignants abordant différents aspects de la protection de la vie privée et des données à caractère personnel dans le contexte de la société de l'information, dont les réseaux sociaux;
 - 4.2. se félicite de l'adoption du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223), qui modernise la convention et s'attaque aux nouveaux défis résultant de l'utilisation des nouvelles technologies d'information et de communication; elle soutient l'appel du Rapporteur spécial des Nations Unies sur le droit au respect de la vie privée, M. Joseph A. Cannataci, à tous les États membres des Nations Unies à adhérer à la Convention 108 lorsque leurs législation et pratique sont conformes aux dispositions de la Convention;
 - 4.3. soutient les travaux futurs du Comité de la Convention 108 sur l'utilisation de données à caractère personnel lors d'élections et leur utilisation abusive dans un contexte politique.
5. Afin de relever les défis de la désinformation dans le contexte d'élections démocratiques, les gouvernements des États membres du Conseil de l'Europe doivent:
 - 5.1. reconnaître la nature transnationale du problème et améliorer la coopération avec les intermédiaires d'internet et les opérateurs de réseaux sociaux dont les intérêts commerciaux tendent à entrer en conflit avec les droits de l'homme et les droits politiques, par exemple avec le principe de l'équité électorale, conformément à la [Recommandation CM/Rec \(2018\)2](#) du Comité des Ministres sur les rôles et les responsabilités des intermédiaires d'internet;
 - 5.2. permettre aux électeurs de recevoir des informations dignes de confiance et d'être mieux informés et plus engagés, en vue de préserver l'exercice de leur droit à des élections véritablement libres et équitables;
 - 5.3. briser le monopole des entreprises technologiques qui contrôlent, dans une large mesure, l'accès des citoyens à l'information et aux données.

2. Projet de résolution adopté par la commission le 9 décembre 2019.

6. Pour faire face à ces défis, l'Assemblée invite les États membres du Conseil de l'Europe à mettre en œuvre un certain nombre de stratégies dans une perspective européenne et mondiale et à créer un modèle fondé sur la coresponsabilité et de multiples approches réglementaires et de résolution des conflits, en prenant en particulier les mesures suivantes:

6.1. promouvoir l'éducation aux médias et les compétences en matière de culture numérique afin de renforcer la culture juridique et démocratique des citoyens, conformément à la [Résolution 2314 \(2019\)](#) «L'éducation aux médias dans le nouvel environnement médiatique», sensibiliser davantage le public à la façon dont les données sont produites et traitées, donner aux électeurs les moyens d'évaluer de façon critique la communication électorale et accroître le degré de résilience de la société à l'égard de la désinformation;

6.2. encourager et soutenir les initiatives collaboratives sur la vérification des faits et d'autres améliorations dans les systèmes de modération et de conservation de contenus qui visent à lutter contre la diffusion d'informations trompeuses et mensongères, y compris dans les médias sociaux, conformément à la [Résolution 2281 \(2019\)](#) «Médias sociaux: créateurs de liens sociaux ou menaces pour les droits humains?»;

6.3. garantir un financement approprié des médias indépendants de service public afin qu'ils puissent allouer des ressources suffisantes à l'innovation en termes de contenus, de formes et de technologie en vue de promouvoir leur rôle en tant qu'acteurs principaux de la lutte contre la désinformation et la propagande, et en tant qu'intervenants cruciaux de la protection des écosystèmes de la communication et des médias en Europe, conformément à [Résolution 2255 \(2019\)](#) «Les médias de service public dans le contexte de la désinformation et de la propagande»;

6.4. renforcer la transparence des publicités à caractère politique en ligne, de la diffusion de l'information, des algorithmes et des modèles économiques des opérateurs de plateforme, notamment:

6.4.1. en garantissant, là où les partis politiques et les candidats ont le droit d'acheter de l'espace publicitaire à des fins électorales, l'égalité de traitement en ce qui concerne les conditions et les tarifs appliqués;

6.4.2. en élaborant des cadres de régulation spécifiques concernant les contenus internet en période électorale, en incluant des dispositions sur la transparence en matière de contenus sponsorisés sur les médias sociaux, afin que le public puisse avoir connaissance de la source qui finance la publicité électorale ou toute autre information ou opinion, conformément à la [Résolution 2254 \(2019\)](#) «La liberté des médias en tant que condition pour des élections démocratiques», et en empêchant les ingérences illicites étrangères;

6.5. prendre en compte les implications du microciblage des publicités politiques en vue de promouvoir un paysage politique plus responsable, qui se prête moins aux manipulations;

6.6. soutenir l'accès des chercheurs aux données, y compris aux ensembles de données relatifs à des comptes et contenus supprimés, afin d'examiner l'influence de la désinformation stratégique sur la prise de décision démocratique et les processus électoraux, et de proposer éventuellement la mise en place d'un réseau européen de chercheurs dans ce domaine;

6.7. envisager l'élaboration d'une réglementation nationale et internationale pour partager les bonnes pratiques et renforcer la coopération entre les agences de sécurité, par exemple en créant un mécanisme spécifique de surveillance, de gestion des crises et d'analyse postcrise, et en mutualisant les ressources existantes dans les divers pays, conformément à la [Recommandation 2144 \(2019\)](#) «Gouvernance de l'internet et droits de l'homme»;

6.8. inviter les professionnels et les organisations du secteur des médias à développer des cadres d'autorégulation contenant des normes professionnelles et éthiques concernant leur couverture des campagnes électorales, incluant notamment une plus grande exactitude et fiabilité des informations, le respect de la dignité humaine et du principe de non-discrimination, conformément à la [Résolution 2254 \(2019\)](#) «La liberté des médias en tant que condition pour des élections démocratiques»;

6.9. engager des réformes judiciaires et créer des sections spécialisées pour les juges et les procureurs, axées sur la désinformation et le discours de haine.

7. Par ailleurs, l'Assemblée salue l'action menée par l'Union européenne pour lutter contre la désinformation, faire face aux menaces d'ingérence extérieure dans les élections européennes et garantir une plus grande transparence de la publicité politique payante et des règles plus claires concernant le financement des partis politiques européens, dans le cadre du prochain plan d'action pour la démocratie

européenne pour 2019-2024. Elle appelle l'Union européenne à assurer une synergie avec l'action du Conseil de l'Europe dans ces domaines et à promouvoir une coopération accrue avec les 47 États membres du Conseil de l'Europe.

8. Enfin, l'Assemblée soutient les efforts déployés par la Commission européenne pour la démocratie par le droit (Commission de Venise) en vue d'élaborer une liste de principes pour l'utilisation des technologies numériques dans le contexte des élections et décide de suivre de près cette question.

B. Exposé des motifs par M. Frithjof Schmidt, rapporteur

1. Introduction

1. J'ai été désigné rapporteur le 12 mars 2018, à la suite d'un débat d'actualité tenu à l'initiative de notre collègue M. Emanuelis Zingeris (Lituanie, PPE/DC), lors de la réunion de la Commission permanente à Copenhague en novembre 2017 intitulé «La démocratie piratée? Comment réagir?»³. La question soulevée lors de ce débat a ensuite été renvoyée à la commission des questions politiques et de la démocratie pour rapport. Le changement opéré au niveau des structures publiques par les technologies modernes et les réseaux sociaux dans le fonctionnement des systèmes démocratiques européens et les effets de ce que l'on appelle communément les «désordres de l'information» – à savoir mésinformation, désinformation, information malveillante – sur les processus électoraux présentent un intérêt manifeste pour notre commission.

2. Je souhaiterais, pour commencer, poser les questions suivantes: la transformation numérique des structures publiques menace-t-elle nos débats publics et le modèle actuel des démocraties représentatives? Comment pouvons-nous accroître le degré de résilience de la société à l'égard de la désinformation? Le fonctionnement des réseaux sociaux, en accentuant ce que les chercheurs appellent le «cocooning», c'est-à-dire la tendance de groupes de personnes connectées à pratiquer l'entre-soi et de ne suivre que des «informations», qu'elles soient avérées ou fausses, qui confortent leur point de vue, ainsi que la logique commerciale des opérateurs de plateformes et le manque de transparence dans la diffusion de l'information ne risquent-ils pas de rendre ces communautés d'internautes imperméables à la confrontation d'opinions qui ne sont pas les leurs? En d'autres termes, si la démocratie renvoie à l'acceptation du débat entre des personnes qui ont des opinions différentes, cette tendance ne rend-elle pas obsolète cet élément de la démocratie?

3. La démocratie et le nouvel environnement technologique entretiennent des relations complexes. D'un côté, internet et les médias sociaux sont devenus un forum central d'échanges politiques. Dans certaines démocraties, l'utilisation des outils technologiques a facilité la participation démocratique et le militantisme politique. D'un autre côté, internet et les réseaux sociaux peuvent compromettre le libre arbitre des électeurs ou le principe de l'égalité des chances entre tous les candidats ainsi que le droit des électeurs au respect de la vie privée.

4. De fait, l'accroissement de la production de contenus⁴ et la centralisation des canaux de diffusion en ligne, comme Twitter, Google et Facebook, ont eu plusieurs effets indésirables: la prolifération des tactiques de désinformation, publiques et privées, mais surtout l'arrivée dans l'arène démocratique d'acteurs privés non réglementés, littéralement propriétaires des infrastructures d'information et des points d'accès à l'information. Les outils virtuels peuvent être utilisés pour mettre en péril l'intégrité des élections de plusieurs façons, notamment en faisant baisser la participation, en truquant les résultats, en volant les données des électeurs, en se livrant au cyber espionnage ou au «doxing» de candidats (pratique consistant à mettre en ligne des informations personnelles d'un tiers pour lui porter préjudice) à des fins de manipulation, et pour orienter les opinions des électeurs.

5. Dans le domaine de la défense, les cybers attaques occupent une place grandissante dans ce que l'on appelle désormais les «guerres hybrides»: un nouveau type de guerre mêlant des méthodes conventionnelles et non conventionnelles. Elles redéfinissent d'ailleurs les concepts classiques de la stratégie militaire que sont l'attaque et la défense. Dans ce contexte, le risque est grand que la société civile soit directement visée et que ses droits soient menacés. L'importance de cette question ne fait aucun doute, mais elle n'entre pas dans le cadre du présent rapport et je renvoie à la [Résolution 2217 \(2018\)](#) et la [Recommandation 2130 \(2018\)](#) «Problèmes juridiques posés par la guerre hybride et obligations en matière de droits de l'homme», adoptées par l'Assemblée le 26 avril 2018, ainsi qu'à la réponse du Comité des Ministres du 13 décembre 2018.

3. <https://pace.coe.int/documents/10643/4007015/AS-PER-2017-PV-03-FR.pdf/f055cf71-c7c2-4f4b-99a9-d2230ba8cadf>.

4. Selon le rapport 2018 Digital Global, plus de 4 milliards de personnes à travers le monde utilisent internet chaque mois et plus de 3 milliards les réseaux sociaux. L'internaute moyen passe maintenant environ six heures par jour à utiliser des appareils et services connectés à internet.

6. J'entends mettre l'accent sur les questions liées à la désinformation, l'infrastructure et la transparence d'internet et leur impact sur le processus démocratique et les élections. J'examinerai la manière dont les pays européens abordent la question de la désinformation, en particulier dans le contexte des élections, ainsi que le travail accompli par le Conseil de l'Europe et l'Union européenne et les efforts en matière d'autorégulation consentis par les entreprises de médias sociaux.

7. Le 25 juin 2018, la commission a tenu un premier échange de vues consacré à la sécurité pendant les élections avec la participation de M^{me} Simona Granata-Menghini, secrétaire adjointe de la Commission européenne pour la démocratie par le droit du Conseil de l'Europe (Commission de Venise), et aux désordres de l'information avec la participation de M. Patrick Penninckx, chef du Service de la société de l'information, Direction générale Droits de l'homme et État de droit du Conseil de l'Europe.

8. Le 11 septembre 2018, la commission a procédé à une autre audition, à laquelle ont participé M^{me} Divina Frau-Meigs, professeure, sociologue et chercheuse spécialisée dans les médias, à l'université Sorbonne Nouvelle, Paris, et M. Ben Scott, membre du conseil d'administration du groupe de réflexion Stiftung Neue Verantwortung et conseiller politique en matière d'innovation au sein du département d'État de l'administration de l'ancien président américain Barack Obama.

9. Le 15 mai 2019, je me suis rendu à Stockholm pour m'entretenir de la question avec les autorités suédoises⁵ qui ont été confrontées à des tentatives d'ingérence dans leurs élections et ont une vision globale des réponses possibles susceptible d'être partagée avec d'autres États membres du Conseil de l'Europe.

10. Enfin, le 14 novembre 2019 à Berlin, la commission a organisé conjointement avec la commission des questions juridiques et des droits de l'homme une audition à laquelle ont participé M. Georg Thiel, président de l'Office fédéral allemand des statistiques et directeur du scrutin fédéral, M^{me} Astrid Schumacher, cheffe de la division «Conseil en sécurité des technologies de l'information et sécurité des documents classifiés» de l'Office fédéral allemand de la sécurité des technologies de l'information, M. Johan Farkas, de l'université de Malmö et M^{me} Ulrike Klinger de l'Institut d'études sur la communication et les médias, à l'université libre de Berlin. Au cours de la réunion, notre collègue, M. Emanuelis Zingeris, qui prépare un avis sur ce rapport, m'a également fourni de précieuses informations.

11. Je pense qu'il est désormais temps pour tous les États membres du Conseil de l'Europe d'assumer de plus grandes responsabilités et de s'employer à lutter contre la désinformation, préserver l'intégrité des élections, protéger la démocratie et renforcer le principe de la responsabilité des médias sociaux proprement dits.

2. L'ampleur du problème

12. Selon Freedom House, les tactiques de manipulation et de désinformation ont joué un rôle important dans les élections d'au moins 18 pays en 2017, compromettant la capacité des citoyens à choisir leurs dirigeants sur la base d'informations factuelles et de véritables débats, et donnant lieu à l'émergence de ce qui a été qualifié «d'autoritarisme numérique». Dans le même temps, certains gouvernements partout dans le monde renforcent le contrôle des données des citoyens et invoquent le phénomène des «fake news» (fausses informations) pour faire taire les voix dissidentes, minant ainsi la confiance envers internet et affaiblissant les fondements de la démocratie⁶.

13. En janvier 2018, M. Anders Thornberg, chef du service de sécurité suédois, s'exprimant dans le cadre des élections générales tenues dans le pays, a pointé du doigt plusieurs exemples d'articles relayant de fausses informations aux fins de créer des dissensions et de saper la confiance, dont un qui affirmait que des musulmans avaient vandalisé une église. Cette dernière «information» a été propagée par des «bots» (robots)⁷, implantés hors de la Suède. M. Thornberg a mis en avant les conséquences en termes de sécurité nationale lorsqu'un acteur étranger a recours à de telles campagnes de désinformation⁸. En janvier 2019, Facebook a mis fin à deux opérations de désinformation de grande ampleur liées à des acteurs étatiques russes et opérant dans toute l'Europe centrale et orientale⁹. Le mois suivant, en février, les autorités

5. J'ai rencontré des représentants de la commission sur la Constitution et de la commission de la Défense du Parlement suédois, du ministère des Affaires étrangères et de la Culture, des chercheurs spécialisés dans l'éducation aux médias, à l'information et au dialogue démocratique, des ONG et des acteurs de la société civile, des représentants de l'Agence suédoise de la protection civile ainsi que de l'autorité électorale.

6. Freedom House, Freedom on the Net 2018, [the rise of digital authoritarianism](#) (dernier en date).

7. Comptes de médias sociaux contrôlés par des programmes informatiques qui tentent de se faire passer pour des utilisateurs humains légitimes.

8. BBC News, [Swedish security chief warning on fake news](#), 4 janvier 2018.

allemandes ont interpellé un étudiant âgé de 20 ans qui a reconnu avoir accédé illégalement à des informations relatives à plus de mille personnalités, dont des responsables politiques de haut rang¹⁰. Plus récemment, en novembre 2019, Facebook a annoncé avoir supprimé 5,4 milliards de faux comptes durant l'année¹¹.

14. Construit comme un lieu ouvert et démocratique, internet est aussi ce «village mondial» qui permet de diffuser les informations facilement et à faible coût. Il est par conséquent difficile de distinguer les informations fiables ou de déterminer les personnes responsables de comportements illégaux en ligne. La propagande, la désinformation et les discours de haine en ligne se sont intensifiés à l'ère numérique. Dans ce contexte, un défi majeur consiste à garantir la liberté de vote et des élections équitables, tout en préservant la liberté d'expression. Dès lors que les citoyens ne sont pas en mesure de distinguer les vraies informations des fausses et méconnaissent les conditions dans lesquelles ils peuvent exercer leurs droits et libertés, la pureté de leurs intentions pourrait être altérée, et la légitimité démocratique des élections elles-mêmes compromise¹².

15. Selon les experts, la mésinformation, qui a parfois bénéficié de l'appui de gouvernements, a déjà influencé plusieurs événements majeurs en Europe. À titre d'exemple, d'aucuns affirment que la désinformation a pu impacter le vote néerlandais sur l'accord d'association entre l'Union européenne et l'Ukraine, le résultat du référendum sur le Brexit, les débats sur l'indépendance de la Catalogne et les questions d'immigration en Italie.

16. D'après le rapport final de la Commission du numérique, de la culture, des médias et du sport de la Chambre des communes du Royaume-Uni publié le 14 février 2019, à l'issue d'une enquête de 18 mois sur la désinformation, la démocratie est menacée par le ciblage malveillant et incessant de citoyens par la désinformation et par des «publicités occultes» personnalisées provenant de sources non identifiables et diffusées par les principales plateformes de médias sociaux¹³.

17. Par ailleurs, selon une étude de la Commission de Venise, le recours à l'intelligence artificielle (IA) dans le cadre des campagnes électorales soulève des questions en matière d'éthique et de démocratie dans la mesure où il existe des preuves et des possibilités supplémentaires d'y recourir pour manipuler les citoyens et influencer les résultats électoraux¹⁴. M^{me} Deborah Bergamini (Italie, PPE/DC) prépare actuellement un rapport pour notre commission qui met l'accent sur la nécessité d'une gouvernance démocratique de l'intelligence artificielle.

18. Derrière la désinformation qui sévit sur internet se cachent, selon moi, certaines questions clés qui relèvent du mandat de la commission. Je souhaiterais d'autre part faire référence aux précédentes résolutions et recommandations basées sur les rapports pertinents préparés par la commission de la culture, de la science, de l'éducation et des médias¹⁵, dont la récente [Résolution 2314 \(2019\)](#) «L'éducation aux médias dans le nouvel environnement médiatique», qui a été adoptée le 29 novembre 2019. En ce qui concerne la

9. <https://www.politico.eu/article/facebook-takes-down-two-russian-disinformation-networks-in-eastern-europe/>.

10. <https://www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation/>.

11. <https://edition.cnn.com/2019/11/13/tech/facebook-fake-accounts/index.html>.

12. Commission de Venise «Study on the role of social media and the internet in democratic development» (Étude sur le rôle des réseaux sociaux et d'internet dans le développement de la démocratie), [CDL-LA \(2018\)001](#); 21/11/2018, 9 (anglais uniquement).

13. <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/1791/179102.htm>.

14. Commission de Venise, «Joint Report on Digital Technologies and Elections» (Rapport joint sur les technologies digitales et les élections), [CDL-AD\(2019\)016](#); 24/06/2019, 10.

15. [Résolution 2256 \(2019\)](#) «Gouvernance de l'internet et droits de l'homme»; [Résolution 2254 \(2019\)](#) «La liberté des médias en tant que condition pour des élections démocratiques»; [Recommandation 2033 \(2014\)](#) et [Résolution 1970 \(2014\)](#) «Internet et la politique: les effets des nouvelles technologies de l'information et de la communication sur la démocratie»; [Résolution 2213 \(2018\)](#) «Le statut des journalistes en Europe»; [Résolution 2212 \(2018\)](#) «La protection de l'intégrité rédactionnelle»; [Résolution 2255 \(2019\)](#) «Les médias de service public dans le contexte de la désinformation et de la propagande»; [Résolution 2143 \(2017\)](#) «Médias en ligne et journalisme: défis et responsabilités», [Recommandation 2075 \(2015\)](#) et [Résolution 2066 \(2015\)](#) «La responsabilité et la déontologie des médias dans un environnement médiatique changeant», [Recommandation 2111 \(2017\)](#) et [Résolution 2179 \(2017\)](#) «L'influence politique sur les médias et les journalistes indépendants», [Recommandation 2106 \(2017\)](#) et [Résolution 2171 \(2017\)](#) «Le contrôle parlementaire de la corruption: la coopération des parlements avec les médias d'investigation»; [Recommandation 2097 \(2017\)](#) et [Résolution 2141 \(2017\)](#) «Attaques contre les journalistes et la liberté des médias en Europe», [Recommandation 2062 \(2015\)](#) et [Résolution 2035 \(2015\)](#) «La protection de la sécurité des journalistes et de la liberté des médias en Europe»; [Résolution 1877 \(2012\)](#) et [Recommandation 1998 \(2012\)](#) «La protection de la liberté d'expression et d'information sur l'internet et les médias en ligne».

manipulation des processus de formation des opinions démocratiques, en particulier lors de scrutins électoraux, la commission devrait se concentrer sur les moyens d'accroître la transparence, sur les ressources devant être allouées à la formation et à la recherche, et celles dédiées à la vérification de l'information. Il importe également de préciser ce qui doit relever de la responsabilité des États quant à la protection des citoyens, par la voie de réformes judiciaires et de procureurs spécialisés, et de la garantie de cette protection au niveau international par le renforcement des conventions existantes et l'élaboration de nouvelles conventions internationales.

19. Pour ce qui est de la protection des données et de la sécurité informatique, je m'intéresserai à la protection d'une société que je souhaite voir rester ouverte, assortie de garanties pour veiller au respect de la vie privée et de la liberté de tous les citoyens et pour faire en sorte que les violations soient sanctionnées par le droit international.

20. La littérature sur le piratage de la démocratie est particulièrement abondante, en particulier au sein des parlements. À titre d'exemple, la Commission du numérique de la Chambre des communes du Royaume-Uni, et des commissions de l'Assemblée nationale et du Sénat français ont produit des rapports sur la lutte contre la manipulation de l'information. Citons également les procès-verbaux cruciaux d'auditions importantes comme celles de M. Mark Zuckerberg, président-directeur général de Facebook, devant le Sénat et la Chambre des Représentants américains, les autorités allemandes et le Parlement européen, ou de M. Christopher Wylie, lanceur d'alerte de l'affaire *Cambridge Analytica*, devant la commission du numérique de la Chambre des communes¹⁶.

3. Manipulation des processus de formation des opinions démocratiques et questions relatives à la vie privée pendant les élections

21. Il est beaucoup question aujourd'hui de «fake news», qui désignent la diffusion virale délibérée de fausses informations sur internet et les réseaux sociaux. Le terme fait référence à du contenu fabriqué, du contenu manipulé, du contenu imposteur, du contenu trompeur, une connexion ou un contexte erronés, voire une satire ou une parodie.

22. En novembre 2017, la Première ministre britannique a déclaré que la diffusion de fausses informations était un moyen de «transformer l'information en arme»¹⁷. D'un point de vue social, la désinformation contribue à former des communautés de personnes qui ont accès aux mêmes opinions, partagent la même idéologie et les mêmes théories conspirationnistes.

23. La désinformation peut prendre plusieurs formes: déclarations ou expressions d'opinions infondées. L'initiative de cette manipulation de l'opinion publique peut être d'origine privée mais certains gouvernements tentent de contrôler les médias sociaux pour façonner l'opinion publique, contrer l'opposition et désamorcer les critiques.

24. Les nouvelles technologies de l'information facilitent l'accès de tous les citoyens aux processus démocratiques. Que ce soit le droit d'accès à l'information ou la constitution de registres centralisés des électeurs, internet facilite à chacun l'exercice de ses droits politiques. De surcroît, internet et les nouvelles technologies de l'information permettent davantage de transparence et de responsabilité, ainsi que des formes plus larges et efficaces de participation politique, et élargissent le champ de la sphère publique, renforçant ainsi la démocratie délibérative. Cependant, l'utilisation des médias sociaux en tant que source d'information peut aboutir au phénomène appelé «l'info me trouve»: c'est-à-dire des personnes qui ne recherchent pas activement des informations mais qui croient que leur réseau les informera d'une manière ou d'une autre. Cette perception peut entraîner une baisse des connaissances politiques.

25. Les médias sociaux définis comme des «plateformes en ligne permettant des échanges de contenus générés par leurs utilisateurs»¹⁸ ont également des effets positifs sur la démocratie. Ils constituent aujourd'hui un important forum de débat politique et sont devenus, en tant que tels, des sources d'information politique cruciales et un élément indispensable des campagnes politiques modernes¹⁹. Dans le même temps, les entreprises de médias sociaux sont à but lucratif et les problèmes qu'elles peuvent poser à la démocratie sont au mieux des dommages collatéraux.

16. <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-evidence-wylie-correspondence-17-19/>.

17. <https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news>.

18. Définition de International IDEA 2014.

26. Lors des élections présidentielles américaines de 2008 et 2012, les équipes de campagne de M. Barack Obama ont disposé de dizaines de séries de données sur quasiment tous les électeurs. Il semblerait aussi que la désinformation stratégique ait pu avoir une influence sur la campagne de Donald Trump à l'élection présidentielle américaine de 2016. Le rapport Mueller publié en mars 2019 montre de façon très détaillée que le discours public relatif à ces élections a été influencé par des acteurs associés à des sources russes²⁰. En France, lors du scrutin présidentiel de 2017, des tentatives d'influence d'acteurs russes sur le processus électoral ont également été constatées²¹.

27. Cinq étapes de l'ingérence électorale ont été identifiées: (1) utiliser la désinformation pour amplifier les soupçons et les divisions; (2) voler des données sensibles et «fuitables»; (3) «fuir» les données volées via des «hacktivists» présumés; (4) blanchir les données volées via les médias traditionnels; et (5) établir une collusion secrète [entre un candidat et un État étranger] à des fins de synchronisation des actions électorales²².

28. À titre d'exemple, je rappellerai l'affaire *Cambridge Analytica*, qui portait sur l'utilisation de données personnelles d'utilisateurs de Facebook récoltées sans leur accord au cours de l'élection présidentielle américaine de 2016. Il s'agit là d'un cas manifeste d'influence sur le processus de formation de l'opinion des électeurs. Cette opération de microciblage reposait sur un accès illégal à des données et un apprentissage automatique pour influencer sur les émotions des personnes. Ainsi, les différents électeurs ont reçu des messages différents en fonction des prédictions concernant leur propension à se laisser influencer par certains arguments²³.

29. Les techniques d'IA plus couramment utilisées pour façonner les opinions des électeurs sont les suivantes:

- les plateformes sociales recueillent et traitent les informations au moyen d'algorithmes, sélectionnant ainsi celles à afficher en fonction des préférences des utilisateurs ciblés. Compte tenu de l'évolution rapide des algorithmes, il est difficile de comprendre la façon dont les données sont traitées et les implications complexes qui en découlent. Cela peut se faire en faveur ou en défaveur d'un parti ou d'un candidat donné;
- les informations utilisées pour produire des publicités politiques comprennent également des données recueillies par les partis politiques. Cependant, les messages publicitaires ciblés ne permettent pas toujours d'identifier leur nature et sources politiques. Des prestataires anonymes, éventuellement basés en dehors du pays concerné par la tenue du scrutin en question, peuvent être à l'origine de l'introduction de telles publicités. Il devient donc difficile de contrôler le financement de la campagne²⁴;
- la propagation massive d'informations fausses ou préjudiciables s'effectue aussi par le biais de faux profils, dont beaucoup sont automatisés. Des centres Web proposant des services de promotion de campagnes peuvent facilement créer des profils anonymes, des robots ou de faux comptes. En imitant le comportement en ligne des internautes, ces centres amplifient encore la diffusion des informations et génèrent des tendances d'opinion de manière artificielle;
- une technique de manipulation puissante peut consister à cloner un profil social existant avec de faux profils imitant celui-ci, de manière à imputer des informations erronées à tel ou tel parti ou candidat. La création d'un nouveau «personnage» qui interagit avec d'autres profils, à des fins de renforcement de la réputation et de la confiance, est une autre technique courante. En se rapprochant d'une certaine catégorie d'électeurs, le robot peut jouer le rôle d'influenceur auprès des internautes.

19. Pour une analyse détaillée, je renvoie au rapport de la commission de la culture, de la science, de l'éducation et des médias sur les médias sociaux: créateurs de liens sociaux ou menaces pour les droits humains? (rapporteur: M. José Cepeda, Espagne, SOC), Doc. 14844.

20. <https://apps.npr.org/documents/document.html?id=5955997-Muellerreport>.

21. Center for strategic and international studies (Centre d'études stratégiques et internationales), [Successfully countering Russian electoral interference](#), juin 2018.

22. Mika Aaltola, [Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling](#), Briefing Paper 226 (Helsinki: Institut finlandais des affaires internationales, novembre 2017).

23. The Conversation, [How artificial intelligence conquered democracy](#), 8 août 2017.

24. Un rapport sur «Transparence et réglementation des dons de sources étrangères en faveur de partis politiques et de campagnes électorales» (rapporteur: M. Konstantin Kuhle, Allemagne, ADLE) est actuellement en préparation.

30. Des experts ont également critiqué l'utilisation de publicités politiques microciblées, qui sont personnalisées et adressées aux citoyens en fonction des données de leur profil concernant leurs préférences et comportement personnels, leurs «J'aime» sur les réseaux sociaux, leur âge et leur sexe. Selon de nombreux détracteurs, l'interdiction ou la limitation des publicités politiques microciblées permettrait de rendre notre paysage politique plus responsable et moins sujet aux manipulations.

31. Par ailleurs, le suivi des activités d'internautes sans leur consentement et en vue d'exploiter leurs comportements en ligne est contraire au principe même d'élections libres et équitables mais aussi au droit au respect de la vie privée. Je suis d'avis que nous avons besoin de nouveaux instruments juridiques internationaux pour faire face à la nouvelle structure de communication et de médias publics.

32. D'après l'Eurobaromètre spécial de l'Union européenne de 2018 sur la démocratie et les élections, 73 % des personnes ayant répondu se sont déclarées préoccupées ou très préoccupées par la désinformation ou la mésinformation²⁵. Les adversaires politiques ont un intérêt à se pirater mutuellement et les entreprises de cybersécurité à faire la démonstration de leurs services et contre-services en période électorale. Des entreprises comme Twitter et Facebook reconnaissent également que les faux comptes représentent une menace pour l'intégrité des élections²⁶.

33. Une étude de l'Oxford Internet Institute a révélé que moins de 4 % des sources d'information partagées sur Twitter avant les élections au Parlement européen de 2019 relevaient de la désinformation, tandis que 34 % étaient des médias professionnels traditionnels. D'après FactCheckEU, il y a eu moins de désinformation que prévu au cours de la période précédant les élections européennes et ce phénomène n'a pas dominé le débat comme cela avait été le cas à l'occasion des dernières élections au Brésil, au Royaume-Uni, en France ou aux États-Unis²⁷.

34. Cependant, d'après un rapport de 2019 de la Commission européenne sur la mise en œuvre du plan d'action contre la désinformation²⁸, des groupes ou des acteurs russes ont mené une vaste campagne de désinformation visant à réduire le taux de participation des électeurs et à influencer leurs préférences et se sont servis de sujets brûlants pour susciter la colère du public. Ces activités ont couvert un large éventail de sujets, allant de la contestation de la légitimité démocratique de l'Union européenne à l'exploitation de débats publics clivants sur des thèmes tels que la migration et la souveraineté.

35. En 2019, Facebook a fait savoir que les annonceurs seront désormais tenus de fournir des coordonnées de contacts à des fins de vérification avant de pouvoir mener des campagnes politiques sur des plateformes sociales. Les restrictions imposent à ceux souhaitant diffuser des messages à caractère «politique» (défini différemment selon les pays), de prouver qu'ils résident dans le pays visé et d'archiver pendant sept ans toutes leurs annonces publicitaires dans une base de données publique, accompagnées d'informations concernant les personnes ciblées, le montant dépensé et le nombre d'individus exposés à une publicité. Les règles obligent les annonceurs à renseigner le champ «financé par», une exigence qui a suscité dans le passé des critiques vis-à-vis de Facebook, l'entreprise permettant alors aux utilisateurs d'y mentionner ce qu'ils voulaient sans procéder à aucune vérification d'identité. Les utilisateurs auront toujours la possibilité d'indiquer la source de financement de leur choix mais devront fournir au minimum un numéro de téléphone ou une adresse électronique permettant aux parties intéressées de contacter l'annonceur. Ceux qui souhaitent diffuser un message publicitaire à titre personnel seront libres de ne pas saisir cette information, mais leur nom, vérifié par le site, sera alors publié à la place²⁹. Twitter a également déclaré bannir à l'avenir toute publicité politique tandis que YouTube a fait part de son intention de supprimer les contenus illégaux de manière plus stricte. Tout en saluant ces mesures positives, il importe, selon moi, de se pencher davantage sur une réglementation internationale qui s'appliquerait à toutes les entreprises de médias sociaux.

4. Travaux pertinents du Conseil de l'Europe

36. Le Conseil de l'Europe a accompli un travail remarquable dans le domaine de la protection des données à caractère personnel. Il a non seulement adopté le premier instrument international juridiquement contraignant, c'est-à-dire la [Convention pour la protection des personnes à l'égard du traitement automatisé](#)

25. <https://ec.europa.eu/comfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2198>.

26. Politico, [Europe's most hackable election – The EU faces hackers, trolls and foreign agents as it gears up for a vote in May](#), 16 janvier 2019.

27. Oxford Internet Institute, [Junk News during the EU Parliamentary Elections](#), mai 2019.

28. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52019JC0012>.

29. Facebook, [La protection des élections dans l'UE](#), 28 mars 2019.

des données à caractère personnel (STE n° 108) mais a aussi élaboré des instruments juridiques non contraignants abordant différents aspects de la protection de la vie privée et des données à caractère personnel dans le contexte de la société de l'information, notamment des réseaux sociaux. Notre Assemblée devrait soutenir les travaux futurs du Comité de la Convention 108 sur l'utilisation de données à caractère personnel lors d'élections et leur utilisation abusive dans un contexte politique.

37. Conformément à la Convention européenne des droits de l'homme, telle qu'interprétée par la Cour européenne des droits de l'homme, les États membres du Conseil de l'Europe ont l'obligation de garantir à toute personne relevant de leur juridiction les droits et libertés, tant en ligne qu'hors ligne. La question cruciale est de déterminer si les obligations de l'État d'assurer aux candidats et aux partis politiques une exposition médiatique égale doivent s'appliquer aux intermédiaires internet et si oui, de quelle manière.

38. À cet égard, la [Recommandation CM/Rec \(2018\)1](#) sur le pluralisme des médias et la transparence de leur propriété et la [Recommandation CM/Rec \(2018\)2](#) du Comité des Ministres sur les rôles et les responsabilités des intermédiaires d'internet, affirment que le contrôle des plateformes en ligne sur le flux, la disponibilité, la facilité de recherche et l'accessibilité des informations pourrait s'avérer aujourd'hui délétère pour le pluralisme des médias. Le Comité des Ministres a ainsi appelé les États membres à agir en tant que garants en dernier ressort du pluralisme des médias, en assurant ce pluralisme dans la totalité de l'écosystème multimédia.

39. Les intermédiaires internet, y compris les médias sociaux, jouent un rôle essentiel dans la prestation de services à valeur publique et dans la promotion du discours public et du débat démocratique. Les normes du Conseil de l'Europe définissent les responsabilités des intermédiaires s'agissant de garantir les droits humains et les libertés fondamentales sur leurs plateformes, dont le droit à des élections libres. À cet égard, les intermédiaires internet devraient faire l'objet d'un contrôle effectif et vérifier régulièrement et avec une diligence raisonnable qu'ils s'acquittent bien de leurs responsabilités³⁰.

40. En 2002, la Commission de Venise a adopté le [Code de bonne conduite en matière électorale](#) qui garantit l'équité électorale et l'égalité des chances. Ces principes portent entre autres sur le temps d'antenne à la radio et à la télévision, les subventions publiques et autres formes de soutien et impliquent la neutralité des autorités publiques, concernant notamment les campagnes électorales, la couverture médiatique, en particulier par les médias publics, et le financement public des partis et campagnes. Cependant, le Code énonce également que «la loi devrait prévoir que les médias audiovisuels privés assurent un accès minimal aux différents participants aux élections, en matière de campagne électorale et de publicité» et que «le principe de l'égalité des chances peut, dans certains cas, conduire à limiter les dépenses des partis, notamment dans le domaine de la publicité»³¹.

41. Par ailleurs, la Commission de Venise accomplit un travail considérable et a notamment adopté, le 24 juin 2019, un rapport sur les technologies numériques et les élections élaboré conjointement avec la Direction de la société de l'information et de la lutte contre la criminalité, qui s'avère fort utile dans le cadre de mon analyse³². Elle a également décidé d'établir une liste de principes pour une utilisation des technologies numériques respectueuse des droits humains, dans le contexte des élections. Notre Assemblée devrait encourager, soutenir et suivre cette initiative, au moyen éventuellement d'un rapport distinct.

42. En 2011, notre Assemblée a adopté la [Résolution 1843 \(2011\)](#) et la [Recommandation 1984 \(2011\)](#) «La protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne». La résolution souligne que la protection de la vie privée est un élément nécessaire de la vie humaine et du fonctionnement humain d'une société démocratique; toute violation de la vie privée d'une personne met en jeu sa dignité, sa liberté et sa sécurité.

43. En 2012, le Comité des Ministres a adopté deux Recommandations pertinentes sur la protection des droits de l'homme dans le contexte des moteurs de recherche et dans le cadre des services de réseaux sociaux respectivement. Dans le premier texte³³, le Comité des Ministres reconnaît le défi posé par le fait que l'historique des recherches d'un individu contient une empreinte qui peut révéler ses convictions, ses centres d'intérêt, ses relations ou ses intentions, et pourrait aussi dévoiler entre autres ses opinions politiques,

30. Commission de Venise, "Joint Report on Digital Technologies and Elections" (Rapport joint sur les technologies digitales et les élections), [CDL-AD\(2019\)016](#); 24/06/2019, 5, 18; [CDL-LA \(2018\)002](#) ; 9 (anglais uniquement).

31. Voir également le rapport préparé par M. Hendrik Daems (Belgique, ADLE) pour notre commission sur «Fixation de normes minimales pour les systèmes électoraux afin de créer une base pour des élections libres et équitables» ([Doc. 15027](#)).

32. [CDL-AD\(2019\)016](#) (anglais uniquement).

33. [Recommandation CM/Rec\(2012\)3](#).

convictions religieuses ou autres. La Recommandation appelle à appliquer des principes de protection des données, dont notamment l'encadrement des finalités, la minimisation des données et une limitation de la durée de conservation des données, et à veiller à ce que les intéressés soient informés du traitement des données et reçoivent toutes les informations pertinentes.

44. S'agissant des réseaux sociaux, le Comité des Ministres a recommandé aux États membres de mener des actions pour offrir un environnement qui permette aux utilisateurs de réseaux sociaux de continuer à exercer leurs droits et libertés, sensibiliser les utilisateurs aux éventuelles atteintes à leurs droits fondamentaux et aux moyens d'éviter d'avoir un impact négatif sur les droits d'autrui lorsqu'ils utilisent ces services, ainsi que pour renforcer la transparence quant au traitement des données et proscrire tout traitement illégitime des données à caractère personnel³⁴.

45. Préoccupés par les interférences sur le droit au respect de la vie privée en raison du développement rapide des technologies, le Comité des Ministres a adopté, en 2013, la Déclaration sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux³⁵.

46. Élaboré en 2017, le rapport du Conseil de l'Europe sur les désordres de l'information: Vers un cadre interdisciplinaire pour la recherche et l'élaboration des politiques³⁶, qui a également été présenté à notre commission, propose des moyens de déterminer le type de réponse adaptée à la menace. Compte tenu de l'imprécision du concept de «fausses informations», le rapport établit la distinction entre: la «mésinformation» qui correspond à la diffusion d'une information fautive, sans intention de nuire, la «désinformation» qui correspond à la diffusion délibérée d'une information fautive, dans l'intention de nuire; et «l'information malveillante» qui est une information authentique diffusée dans le but de nuire, souvent en rendant publique des informations destinées à rester privées. Le rapport souligne ce dont nos sociétés ont actuellement besoin, à savoir:

- à court terme, de répondre aux problèmes les plus pressants, par exemple dans le domaine de la sécurité dans les élections;
- à long terme, d'accroître le degré de résilience de la société à l'égard de la désinformation;
- d'une structure à même de vérifier et d'ajuster constamment les réponses.

47. Le rapport souligne également que nos systèmes éducatifs ayant été conçus au XIXe siècle, bien avant l'ère numérique, il convient également de mettre en œuvre de nouvelles réformes de l'éducation pour permettre aux jeunes de faire face à la circulation de l'information sur internet.

48. Les 19 et 20 avril 2018, lors de la 15^{ème} Conférence européenne des administrations électorales sur la sécurité dans les élections, organisée par la Commission de Venise et la Section des élections du ministère des Collectivités locales et de la Modernisation de la Norvège, il est clairement apparu que le droit de suffrage libre était confronté à deux défis liés au numérique, à savoir la liberté des électeurs de se forger une opinion, et celle d'exprimer leur volonté. Il a également été indiqué que si les cyber-attaques devaient faire l'objet d'une sanction pénale, l'efficacité de la réponse juridictionnelle était, à ce jour, relativement faible³⁷.

49. Le 13 février 2019, le Comité des Ministres a adopté une importante Déclaration sur les capacités de manipulation des processus algorithmiques³⁸. Il a invité ses 47 États membres à combattre la menace qui remet en cause le droit des êtres humains à se forger une opinion et à prendre des décisions indépendamment des systèmes automatisés, et à s'attaquer au risque qu'ils puissent faire l'objet de manipulation en raison de l'utilisation de technologies numériques de pointe, en particulier de techniques de microciblage. Les outils d'apprentissage automatique sont de plus en plus capables non seulement de prédire les choix mais aussi d'influencer les émotions et les pensées, parfois de façon subliminale. Le Comité des Ministres a encouragé les États membres à assumer leur responsabilité pour faire face à cette menace croissante, notamment en prenant des mesures législatives appropriées et proportionnées pour lutter contre ces formes d'ingérence illégitimes, et en permettant aux utilisateurs de développer des compétences clés dans la culture numérique.

50. Le Comité des Ministres est allé jusqu'à souligner la nécessité d'évaluer les cadres réglementaires relatifs à la communication politique et aux processus électoraux pour préserver l'équité et l'intégrité des élections et de veiller à ce que les électeurs soient protégés de manière efficace contre les pratiques

34. [Recommandation CM/Rec\(2012\)4](#).

35. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c801b.

36. [Rapport du Conseil de l'Europe sur les désordres de l'information](#).

37. [Site web de la 15e Conférence européenne des administrations électorales](#).

38. [Déclaration du CM sur les capacités de manipulation des processus algorithmiques](#).

déloyales et la manipulation. Il a également mis en avant l'immense pouvoir que le progrès technologique confère à ceux qui sont susceptibles d'utiliser ces outils algorithmiques sans surveillance ou contrôle démocratique approprié et rappelé la responsabilité qui incombe au secteur privé de faire preuve d'équité, de transparence et de responsabilisation, sous la conduite d'institutions publiques indépendantes.

51. Par ailleurs, les 26 et 27 février 2019, la Conférence d'Helsinki intitulée «Maîtriser les règles du jeu – L'impact du développement de l'intelligence artificielle sur les droits de l'homme, la démocratie et l'État de droit», organisée par le Conseil de l'Europe et la Présidence finlandaise du Comité des Ministres, a souligné en particulier:

- que des mécanismes de surveillance effectifs et des structures de contrôle démocratiques doivent être mis en place pour tout ce qui touche à la conception, au développement et au déploiement des systèmes d'IA;
- qu'un processus démocratique fonctionne si la population est informée de manière indépendante et si l'on encourage des débats ouverts et inclusifs. Il convient de sensibiliser davantage la population aux risques et aux bénéfices potentiels de l'IA et de développer les nouvelles compétences nécessaires. Il faut en outre stimuler la confiance du public dans l'environnement de l'information et les applications de l'IA³⁹.

52. Le Forum mondial de la démocratie, qui s'est tenu à Strasbourg du 6 au 8 novembre 2019, était intitulé «Information: la démocratie en péril?», et portait tout particulièrement sur la mesure dans laquelle l'information disponible aide ou entrave la participation des citoyens aux processus démocratiques. Renforcer la résilience face à la désinformation, Intelligence artificielle et information, Vérification des faits et Voter sous influence comptaient parmi les thèmes abordés les plus significatifs dans le cadre de mon rapport.

53. Je souhaiterais rappeler la distinction importante entre «information» et «sensibilisation» qui a été faite par l'un des intervenants du Forum, M. Enrico Letta, ex-Premier ministre italien. M. Letta a souligné que rien n'est plus important que de donner aux jeunes des repères leur permettant de comprendre les informations qui leur sont fournies en abondance et librement sur internet et les médias sociaux. Sans ces repères, il est impossible de comprendre un monde dans lequel le problème ne tient pas au manque d'information, mais plutôt à l'inverse. En fait, l'un des principaux défis consiste à éviter d'être noyé sous une avalanche d'informations ou manipulé par elles. La véritable fracture que nous devons combler est celle qui sépare les personnes «sensibilisées» des simples récipiendaires passifs de l'information (ou de la désinformation) et donc faciles à manipuler.

5. Action de l'Union européenne et Code sur la désinformation autorégulé par l'industrie: est-ce suffisant?

54. L'Union européenne lutte activement contre la désinformation depuis 2015, date à laquelle la [Task Force East Stratcom](#) a été créée au sein du Service européen pour l'action extérieure (SEAE) afin de communiquer efficacement sur l'action de l'Union européenne à l'égard du voisinage oriental⁴⁰, le Conseil européen ayant souligné «la nécessité de contrer les campagnes de désinformation menées par la Russie»⁴¹.

55. En octobre 2018, les représentants des plateformes en ligne, des principaux réseaux sociaux, des annonceurs et du secteur de la publicité sont convenus d'un Code d'autorégulation qui vise à réaliser les objectifs fixés dans la Communication de la Commission européenne datée du 26 avril 2018 «Lutter contre la désinformation en ligne: une approche européenne»⁴². Ils ont pris une série d'engagements, consistant notamment à garantir la transparence de la publicité à caractère politique et la fermeture des faux comptes et à priver de leurs recettes les vecteurs de désinformation. C'est la première fois que l'industrie s'accorde sur un ensemble de normes d'autorégulation pour lutter contre la désinformation, sur une base volontaire⁴³. En résumé, le Code prévoit ce qui suit:

- des publicités à caractère politique clairement libellées en tant que telles et affichées uniquement avec l'autorisation des utilisateurs (ciblés en fonction de leur localisation);

39. [Conclusions de la Conférence.](#)

40. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

41. Réunion du Conseil européen (19 et 20 mars 2015) – Conclusions
<https://www.consilium.europa.eu/media/21874/st00011fr15.pdf>.

42. <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018DC0236&from=EN>.

43. <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

- une commission électorale chargée de mener une évaluation prospective indépendante sur le rôle joué par Facebook dans les élections;
- la suppression des faux comptes;
- l'approbation préalable de contenus et sources spécifiques.

56. Google, Facebook, Twitter, Mozilla et les associations professionnelles représentant le secteur de la publicité ont présenté leurs premiers rapports sur les mesures prises pour se conformer au Code, que la Commission a rendu publics le 29 janvier 2019. Tout en saluant les progrès réalisés, la Commission a également appelé les signataires à intensifier leurs efforts dans la perspective des élections européennes de 2019.

57. Le suivi du Code de pratique fait partie du Plan d'action contre la désinformation, adopté pour accroître les capacités et renforcer la coopération entre les États membres et les institutions de l'Union européenne, afin de s'attaquer en amont aux menaces que fait peser la désinformation. Par ailleurs, un système d'alerte rapide entre les institutions de l'Union européenne et les États membres a été mis en place en vue de faciliter le partage de données liées à des campagnes de désinformation et d'apporter des réponses coordonnées. Ce système, qui fonctionne en source ouverte, est alimenté par les contributions des universités, des vérificateurs de faits, des plateformes en ligne et des partenaires internationaux.

58. En janvier 2019, le Conseil européen a également conclu qu'il convient de s'opposer à la désinformation dans le contexte élargi des ingérences étrangères, des menaces hybrides et de la communication stratégique. Cela passe par le renforcement des trois Task forces sur la communication stratégique du SEAE, créées afin de promouvoir des discours fondés sur des faits concernant l'Union européenne dans les pays du voisinage oriental et méridional et dans les Balkans occidentaux⁴⁴.

59. Le Code de pratique constitue une approche volontaire de la lutte contre la désinformation. Il est encore difficile de dire quel sera son succès. Je salue toutefois l'action menée par la Commission européenne pour s'attaquer à ce problème et tiens à souligner l'importance des conventions européennes et internationales dans le cadre du renforcement des principes de transparence et de responsabilité.

60. Au début de l'année 2019, Facebook s'est engagé à protéger l'intégrité des élections au Parlement européen en lançant de nouvelles mesures pour lutter contre la désinformation stratégique et les ingérences étrangères et s'assurer que la plateforme n'est pas utilisée pour nuire au déroulement équitable du scrutin. Cependant, les entreprises de médias sociaux devraient être tenues d'agir conformément aux normes européennes et internationales en matière de droits de l'homme.

61. Afin de contribuer à prévenir les ingérences étrangères et d'accroître la transparence des publicités à caractère politique, les annonceurs seront tenus de confirmer leur identité et de fournir des informations supplémentaires sur les personnes responsables de leurs publicités⁴⁵. L'entreprise a fait savoir qu'elle continuait d'élargir son programme de vérification des faits pour couvrir les contenus publiés en 16 langues et prévoyait d'ouvrir de nouveaux centres d'opérations, axés sur «l'intégrité des élections» et de solliciter entre autres la collaboration de législateurs, d'universitaires et de commissions électorales⁴⁶.

62. Le fondateur de Facebook a lui-même reconnu que «...décider de ce qui relève de la publicité politique n'est pas toujours évident. Nos systèmes seraient plus performants si la régulation établissait des standards communs pour vérifier l'identité des acteurs politiques. Les lois sur la publicité politique en ligne concernent en priorité les candidats et les élections, plutôt que les sujets politiques qui divisent, et sur lesquels nous avons constaté plus de tentatives d'interférence. Certaines lois ne s'appliquent que pendant les élections

44. https://www.consilium.europa.eu/fr/meetings/fac/2019/01/21/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Foreign+Affairs+Council%2c+21%2f01%2f2019.

45. Afin d'améliorer l'authenticité des articles qui apparaissent dans le Fil d'actualité des électeurs, Facebook supprimera tout contenu qui enfreint les «Standards de la communauté»; réduira la diffusion des contenus qui ne violent pas directement les «Standards de la communauté» mais qui «sapent quand même l'authenticité de la plateforme»; et donnera aux abonnés plus de contexte sur l'information qu'ils visualisent.

46. En Allemagne, par exemple, Facebook s'est associé à l'agence de presse DPA dans le cadre d'une vaste action de lutte contre les fausses informations par la vérification des faits. Il prévoyait de former plus de 100 000 étudiants allemands à l'éducation aux médias. Outre l'intervention humaine, le perfectionnement des méthodes d'apprentissage automatique pour identifier les messages non fiables sur la plateforme sera un élément clé dans la lutte de Facebook contre la désinformation.

<https://www.euronews.com/2019/01/28/facebook-vows-to-fight-fake-news-foreign-interference-in-eu-elections><https://www.euronews.com/2019/03/18/facebook-teams-up-with-german-news-agency-dpa-to-fight-fake-news-ahead-of-eu-elections>.

alors que les campagnes d'influence sont continues. Par ailleurs, d'importantes questions se posent sur la manière dont le ciblage et les données sont utilisés pendant les campagnes politiques. La législation devrait être mise à jour pour refléter la réalité des menaces actuelles et définir des standards pour l'ensemble de l'industrie»⁴⁷.

63. Cependant, comme cela a été souligné lors de l'audition de la commission tenue en novembre 2019, il n'y a aucun moyen de vérifier de manière indépendante la véracité des affirmations de Facebook, les faux comptes qui ont été supprimés, les pays ciblés, la nature de leur contenu et le nombre de comptes ayant présenté des signes d'orchestration à grande échelle. Les chercheurs et les journalistes doivent pouvoir accéder plus facilement aux données relatives aux faux comptes et à la désinformation sans être soumis à un contrôle strict de la part des entreprises de médias sociaux. Les décideurs ne peuvent pas réglementer ce qu'ils ne comprennent pas, ni mettre en œuvre les politiques et sanctionner leur non-respect en l'absence de vérifications et de contrôles indépendants.

64. Malgré cette contribution du secteur privé, de nombreux problèmes de réglementation demeurent non résolus et seule l'adoption de conventions internationales et de législations aux niveaux national et international permettront d'y remédier. En matière de défense d'élections démocratiques, les bonnes pratiques et une meilleure coopération entre les agences de sécurité devraient être la règle⁴⁸.

65. Il est intéressant de noter que, dans les Orientations politiques pour la prochaine Commission européenne 2019-2024, M^{me} Ursula von der Leyen, la présidente de la Commission européenne, a promis de présenter «... un plan d'action pour la démocratie européenne. Il permettra de faire face aux menaces de manipulation des élections européennes venues de l'extérieur. Il contiendra des propositions législatives visant à garantir une plus grande transparence en matière de publicité politique payante et des règles plus claires sur le financement des partis politiques européens»⁴⁹.

66. Le 10 octobre 2019, le Parlement européen a adopté une résolution appelant à renforcer la Task Force East Stratcom de l'Union européenne pour en faire une structure permanente, dotée d'un financement bien plus élevé. Les députés ont aussi appelé les entreprises d'internet et des médias sociaux à coopérer pour lutter contre la désinformation, sans porter atteinte à la liberté d'expression, et l'Union européenne à créer un cadre juridique pour combattre les menaces hybrides et à se pencher sur la question du financement étranger des partis et fondations politiques européens. Fait intéressant, les députés européens ont également estimé que l'on pourrait étudier davantage l'opportunité de l'institution d'une commission spéciale sur les ingérences électorales étrangères et la désinformation au sein du Parlement européen⁵⁰.

6. Réglementation et éducation: les cas de l'Allemagne, de la France et de la Suède

67. Le Rapport final 2018 du Groupe d'experts de haut niveau de la Commission européenne sur les fausses informations et la désinformation en ligne, qui s'appuie sur les contributions d'experts du monde entier, propose une approche inclusive et collaborative de la lutte contre la désinformation. Il recommande toutefois explicitement de ne pas réglementer⁵¹.

68. Les entreprises de réseaux sociaux ont elles-mêmes appelé les décideurs politiques européens, américains et autres à trouver un consensus international sur la manière de «réglementer le monde numérique» afin d'éviter toute fragmentation et clivage d'internet selon les frontières nationales⁵², en s'attaquant notamment à la désinformation dans le cadre d'élections libres et équitables.

47. https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.385878d0e864.

Pour la version française, voir: <https://www.lejdd.fr/Medias/exclusif-mark-zuckerberg-quatre-idees-pour-reguler-internet-3883274>.

48. <https://www.theglobeandmail.com/opinion/article-the-new-rules-for-the-internet-and-why-you-shouldnt-delete-facebook/>.

49. «Une Union plus ambitieuse: mon programme pour l'Europe»: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_fr.pdf.

50. https://www.europarl.europa.eu/doceo/document/B-9-2019-0108_FR.html.

51. <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

52. <https://www.politico.eu/article/facebook-mark-zuckerberg-regulation-tech-europe-privacy-data-protection-washington-nick-clegg/>.

69. Il convient également de garder à l'esprit que les régimes autoritaires peuvent facilement avoir recours à la réglementation pour censurer l'opposition. La Chine, par exemple, dispose de certaines des lois les plus strictes au monde en matière de désinformation et érige en infraction pénale la création ou la propagation de rumeurs qui, sur un plan général, «portent atteinte à l'ordre économique et social». En juin 2018, les législateurs biélorusses ont adopté des amendements controversés à la législation sur les médias, permettant au gouvernement de poursuivre toute personne qui diffuserait de fausses informations en ligne⁵³. Le Comité pour la protection des journalistes a fait valoir que cette mesure pourrait aggraver les poursuites sélectives contre les journalistes, dans un pays où, selon Freedom House, la liberté de la presse fait défaut⁵⁴. Le Vietnam et la Thaïlande se servent également de la protection contre la désinformation à des fins de surveillance de masse.

70. Plusieurs États membres du Conseil de l'Europe ont essayé de s'attaquer au problème de la désinformation et à ses incidences sur nos démocraties, avec toutes les difficultés que cela comporte en termes d'atteinte à la liberté d'expression et d'absence de définition de ce qui constitue une «fausse information», comme il ressort de l'analyse détaillée proposée par le rapport du Conseil de l'Europe sur les désordres de l'information.

71. Pour ne citer que quelques exemples, alors que la France et l'Allemagne ont choisi la voie de la réglementation, la Belgique, le Danemark, les Pays-Bas, le Royaume-Uni et la Suède ont publié des rapports, lancé des campagnes ou produit des manuels d'éducation aux médias, visant à lutter contre la désinformation ou les ingérences étrangères⁵⁵.

72. En ce qui concerne le sujet connexe du discours de haine, l'Allemagne a adopté, en juin 2017, la loi sur l'amélioration de l'application du droit sur les réseaux (NetzDG⁵⁶) pour lutter contre les contenus haineux et extrémistes en ligne. Elle impose aux entreprises de médias sociaux de bloquer ou de supprimer tout contenu qui enfreint les dispositions du Code pénal allemand concernant les propos diffamatoires et haineux. La législation permet de supprimer les mensonges utilisés pour attiser des discours de haine. Le non-respect récurrent de ces dispositions expose les plateformes à une amende pouvant aller jusqu'à 50 millions d'euros. Ce qui rend un contenu «manifestement» illégal est laissé, en premier lieu, à l'appréciation de l'être humain ou d'un algorithme. Par conséquent, la loi NetzDG incite les intermédiaires à supprimer les contenus dégradants susceptibles d'enfreindre le Code pénal⁵⁷. Il convient de noter que le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression des Nations Unies ainsi que des militants de la liberté des médias ont critiqué la loi, jugeant qu'elle était inconstitutionnelle et mettait en danger la liberté d'expression⁵⁸.

73. L'obligation de supprimer les fausses informations dans un délai de 24 heures, similaire dans la loi française, s'avère particulièrement problématique. Elle constitue un défi majeur pour les opérateurs de plateformes, mais aussi pour le système juridique allemand. Sans une réforme des structures judiciaires, cette règle est difficile à mettre en œuvre et peut faire peser une menace sur la liberté d'expression.

74. En décembre 2018, le Parlement français a adopté une loi relative à la lutte contre la manipulation de l'information, permettant aux tribunaux de décider si les informations publiées en période électorale sont dignes de foi ou s'il faut faire cesser leur diffusion. Aux termes de la loi, les candidats aux élections peuvent intenter une action en justice afin de faire retirer des contenus d'information contestés pendant les périodes électorales et les plateformes sociales, comme Facebook et Twitter, sont tenues de divulguer la source de financement de contenus sponsorisés⁵⁹. La loi a essuyé les critiques de militants de la société civile et d'un groupe de 50 sénateurs de l'opposition qui ont fait appel devant la Cour constitutionnelle au motif qu'elle ne respectait pas le principe d'une justice proportionnelle. La Cour constitutionnelle a toutefois ensuite confirmé la constitutionnalité de la loi⁶⁰.

53. <https://www.rferl.org/a/belarus-assembly-passes-controversial-fake-news-media-legislation/29291033.html>.

54. <https://cpj.org/2018/06/belarus-moves-to-prosecute-fake-news-control-the-i.php>.

55. Le *Poynter Institute for Media studies* a publié un «Guide to anti-misinformation actions around the world» (Guide pour lutter contre la désinformation à travers le monde) qu'il met régulièrement à jour: <https://www.poynter.org/ifcn/anti-misinformation-actions/>.

56. *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*, également connue sous l'intitulé «Loi Facebook».

57. <https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech>.

58. <https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf>.

59. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&dateTexte=&categorieLien=id>

60. <https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm>.

75. Les autorités suédoises, que j'ai rencontrées le 15 mai 2019, s'emploient activement à protéger la liberté d'expression, la démocratie et les droits individuels, dans le contexte de la désinformation. Elles mettent en avant le rôle joué par la société suédoise pour faire face à cette menace, le soutien d'organisations indépendantes de vérification des faits, appartenant aux sociétés de médias, et la volonté du gouvernement d'inculquer aux enfants du primaire comment détecter de fausses informations.

76. Les élections suédoises de 2018 permettent également de tirer certains enseignements. Après des tentatives d'ingérences étrangères, l'Agence suédoise de la protection civile a commandé auprès de l'Institute of Strategic Dialogue et de la London School of Economics un rapport électoral intitulé «Smearing Sweden» (Dénigrer la Suède)⁶¹, qui décrit comment des sources attribuées à des acteurs russes ont soutenu et renforcé l'extrême droite aux États-Unis, en Europe et en Suède. Le rapport fait également état de comptes Twitter qui avaient déjà antérieurement apporté leur soutien à M. Trump et M^{me} Le Pen avant d'appuyer désormais le parti suédois d'extrême droite AfS⁶².

77. Tous les interlocuteurs rencontrés à Stockholm m'ont confirmé leur attachement à la liberté d'expression, ainsi qu'à la protection de l'anonymat et des données. Ils jugent suffisantes les lois relatives à la diffamation, à l'incitation à la discrimination ou à la haine et craignent que le durcissement de la société ouverte n'entraîne un renforcement de la radicalisation. Toutefois, selon eux, le système judiciaire devrait être mieux armé pour faire face aux nouvelles menaces et à l'évolution constante de l'environnement internet.

78. Le ministère de la Culture a créé un nouveau service «Médias et démocratie», rapprochant ainsi deux domaines auparavant distincts. Le traitement critique de l'information et la vérification des faits et des sources font partie intégrante des programmes scolaires, et la sensibilisation de l'ensemble de la société est également une priorité. L'Agence suédoise de la protection civile a mis à jour sa brochure sur la préparation de la population aux situations d'urgence afin d'y inclure une section sur les fausses informations. Elle met en garde contre d'éventuelles campagnes de désinformation menées de l'étranger et comprend une liste de ce que peuvent faire les citoyens pour vérifier la véracité des informations en ligne. Le gouvernement s'efforce de comprendre d'où les citoyens, notamment les jeunes, tirent leurs informations, ainsi que les incidences qu'ont par exemple les jeux en ligne sur l'éducation et les comportements politiques. Il collabore également avec des multiplicateurs, dont les syndicats, les municipalités, les clubs sportifs, etc.

79. Dans le prolongement de l'Agence suédoise de la protection civile et de la commission parlementaire chargée de la défense, une autorité indépendante, non contrôlée par le gouvernement, pourrait être prochainement mise en place dans le but de lutter contre la désinformation et les campagnes d'influence étrangère. Elle aura pour vocation d'assurer la communication rapide et efficace d'informations publiques factuelles, même dans des situations difficiles, ainsi que d'identifier, d'analyser et de faire face aux opérations d'influence.

80. D'après Reporters sans Frontières, plutôt que d'adopter des lois normatives, qui viennent d'en haut, nous devrions songer à changer l'environnement dans lequel les lecteurs agissent et leur donner des moyens d'agir, par exemple en affichant à côté des récits controversés des articles connexes, vérifiés, en proposant des applications permettant aux utilisateurs de vérifier la véracité des informations, et des systèmes de certification⁶³.

7. Conclusions

81. Internet imprégnant de plus en plus nos vies politiques, il importe d'améliorer son contenu et son architecture, et de protéger le processus électoral et l'essence même de la démocratie de ses «pirates». La désinformation, les ingérences étrangères, les comportements abusifs, l'intensification des propos haineux, le trolling, le vol d'identité, sont quelques-uns des symptômes du «piratage de la démocratie».

61. <https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf>.

62. Le rapport fait aussi état d'une tentative de «fraude électorale» sur Twitter, bien avant les élections. Plusieurs hashtags de fraude électorale ont, selon le rapport, atteint un chiffre record le 10 septembre, au lendemain de l'élection, avec 13 558 postes. Cette situation a été alimentée par la mise hors service du site Web de l'autorité électorale durant la nuit des élections. Elle n'a eu aucune incidence sur le dépouillement, ni sur la couverture médiatique du décompte, mais a affecté la présentation des résultats sur le propre site de l'autorité électorale. Cependant, pendant la mise hors service du site, le pourcentage de voix des démocrates suédois a diminué. D'où une nouvelle vague d'allégations de «vol des élections» par les socio-démocrates. L'autorité électorale a admis que le site web avait fait l'objet d'une attaque en déni de service distribué. <https://disinfoportal.org/lessons-from-the-2018-swedish-elections/>.

63. <https://www.theguardian.com/media/2018/apr/24/global-crackdown-on-fake-news-raises-censorship-concerns>.

82. De nombreux pionniers du secteur des technologies ont également indiqué qu'ils aspiraient à des structures internet qui inciteraient les utilisateurs à être de «meilleures personnes», à un internet moral⁶⁴. En effet, à «l'ère post-vérité» comme l'ont qualifiée certains, les émotions sont susceptibles d'affecter davantage le processus électoral que les faits, et peuvent être exploitées par des propagandistes et des agents de désinformation⁶⁵.

83. Les conclusions de la Conférence européenne des administrations électorales, coorganisée par la Commission de Venise en avril 2018 ainsi que le rapport plus récent sur les technologies numériques et les élections mentionné précédemment, présentent un intérêt particulier pour mon rapport et je souhaiterais «emprunter» certaines de leurs recommandations.

84. Les médias sociaux représentent un puissant outil de communication. Cependant, le cadre juridique régissant la couverture médiatique des élections n'a pas été conçu pour les médias sociaux et doit être corrigé. Les désordres de l'information pendant les campagnes électorales compromettent l'égalité des chances entre les candidats. Les contrer ne devrait cependant pas se faire au détriment de la liberté d'expression.

85. Par ailleurs, les campagnes électorales axées sur les données tirées des médias sociaux, basées sur la segmentation et le profilage des utilisateurs, en particulier les publicités occultes diffusées sur les plateformes et visant des électeurs potentiels, sont un phénomène croissant qui devrait être mieux régulé afin d'assurer la transparence et la protection des données, et de gagner confiance du public. Il n'y a aucun mal à tenter de convaincre l'électorat flottant mais les personnes visées devraient être sensibilisées au fait qu'elles sont destinataires d'informations à caractère politique.

86. Pour relever les défis de la désinformation, il convient de reconnaître qu'internet et les médias sociaux ont complètement remodelé le paysage démocratique: un nouvel acteur puissant est apparu dans l'équation, défendant ses propres intérêts et droits commerciaux qui tendent à entrer en conflit tant avec les droits individuels (c'est-à-dire la protection de la vie privée, des données à caractère personnel et de la liberté d'expression) qu'avec les principes et droits politiques (l'équité électorale).

87. La coopération avec les intermédiaires et les fournisseurs de services internet est indispensable et mérite d'être renforcée. Les opérateurs de médias sociaux devraient être mieux régulés et interagir avec les institutions et les organes en charge des processus électoraux afin d'encourager les utilisateurs à agir de manière responsable et de leur en donner les moyens; des campagnes d'information spécifiques devraient être menées pour sensibiliser le public aux risques d'échanges irresponsables d'informations. Et la coopération internationale est cruciale à cet égard.

88. Si une autorégulation en ligne sur la base des normes internationales existantes, notamment la [Recommandation CM/Rec\(2018\)2](#) du Comité des Ministres sur les rôles et les responsabilités des intermédiaires d'internet, ne peut-être que bienvenue et encouragée, le Conseil de l'Europe devrait envisager de poursuivre sa réflexion et son action normative⁶⁶.

89. Les électeurs doivent être en mesure de trier les informations et connaissances dignes de confiance. La promesse d'un internet libre et ouvert a pour but de leur permettre d'être mieux informés et plus engagés. Pour ce faire, il convient de briser le monopole des entreprises technologiques qui contrôlent, dans une large mesure, l'accès des citoyens à l'information. L'Europe doit également chercher à accroître la diversité des fournisseurs d'informations et à assurer une concurrence réelle et loyale entre eux.

90. Il est facile d'imputer à l'IA tous les torts du monde (et parfois les échecs électoraux), mais la technologie sous-jacente n'est pas intrinsèquement nuisible en elle-même. Utilisée à bon escient, l'IA peut aider les citoyens à se faire une idée des positions politiques de chaque candidat. Il est essentiel que les publicités politiques personnalisées servent les électeurs et les aident à être mieux informés, plutôt que de nuire à leurs intérêts. Les outils algorithmiques utilisés aujourd'hui pour tromper, mésinformer et embrouiller les électeurs pourraient également être adaptés à d'autres fins, en l'occurrence pour soutenir la démocratie⁶⁷.

64. David D. Clarck, *Designing an Internet*, MIT Press, octobre 2018.

65. Warsaw Institute, *In the Age of Post-Truth: Best Practices in Fighting Disinformation*, avril 2017.

66. <https://www.coe.int/fr/web/electoral-management-bodies-conference/conclusions-emb2018>.

67. Vyacheslav Polonski, *Artificial intelligence can save democracy, unless it destroys it first* (L'intelligence artificielle peut sauver la démocratie, à moins qu'elle ne la détruise d'abord), Oxford Internet Institute – Blog, August 2017, <https://www.oii.ox.ac.uk/blog/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/Medium>.

91. Pour relever ces défis, les gouvernements pourraient mettre en œuvre un certain nombre de stratégies dans une perspective européenne et mondiale et créer un modèle fondé sur la coresponsabilité et de multiples approches réglementaires et de résolution des conflits. Un tel modèle pourrait mettre l'accent sur différentes stratégies exposées plus en détail dans le projet de résolution et visant notamment à renforcer les compétences dans la culture numérique et la transparence des publicités à caractère politique en ligne, à soutenir les initiatives de vérification des faits, les médias de service public et l'accès des chercheurs aux données, à partager les bonnes pratiques et à renforcer la coopération entre les agences de sécurité ainsi qu'à encourager le développement de cadres d'autorégulation et à engager des réformes judiciaires.

92. J'estime qu'il conviendrait de redoubler d'efforts pour mettre également en œuvre les normes juridiques du Conseil de l'Europe dans le cadre des activités politiques menées par le biais des médias sociaux. Les citoyens doivent être en mesure d'identifier les informations non fiables et les manipulations et de percevoir la limite entre les formes de persuasion admissibles et la manipulation inacceptable pendant les campagnes électorales. Notre Assemblée pourrait aussi examiner plus avant la possibilité de recommander l'adoption de conventions contraignantes sur la coopération dans la lutte contre la désinformation et l'influence dans les processus décisionnels étrangers.

93. Je salue l'action menée par l'Union européenne pour lutter contre la désinformation, faire face aux menaces d'ingérence extérieure dans les élections européennes et garantir une plus grande transparence de la publicité politique payante et des règles plus claires concernant le financement des partis politiques européens dans le cadre du prochain plan d'action pour la démocratie européenne pour 2019-2024. Cependant, notre Assemblée devrait aussi appeler l'Union européenne à assurer une synergie avec l'action du Conseil de l'Europe dans ces domaines et à promouvoir une meilleure coopération avec les 47 États membres du Conseil de l'Europe.

94. Enfin, nous devrions soutenir les efforts déployés par la Commission de Venise en vue d'élaborer une liste de principes pour l'utilisation des technologies numériques dans le contexte des élections, et continuer à suivre cette question.