Strasbourg, le 11 décembre 2020 **CDL-AD(2020)037**

Avis n° 974 / 2020

Or. angl.

COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT

(COMMISSION DE VENISE)

PRINCIPES

POUR UN USAGE CONFORME AUX DROITS FONDAMENTAUX DES TECHNOLOGIES NUMÉRIQUES DANS LES PROCESSUS ÉLECTORAUX

Approuvés par le Conseil des élections démocratiques lors de sa 70e réunion (en ligne, 10 décembre 2020) et adoptés par la Commission de Venise lors de sa 125e session plénière (en ligne, 11-12 décembre 2020)

sur la base des observations de

M. Richard BARRETT (membre, Irlande)
Mme Herdís KJERULF THORGEIRSDOTTIR (membre, Islande)
M. Rafael RUBIO NUÑEZ (membre, Espagne)
M. José Luis VARGAS VALDEZ (membre, Mexique)

Table des matières

I. INTRODUCTION

1. Lors de sa 119e session plénière (juin 2019), la Commission de Venise a adopté le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité de la Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections (ci-après : le rapport conjoint), précédemment adopté par le Conseil des élections démocratiques le 20 juin 2019 (CDL-AD(2019)016), et a décidé d'élaborer un ensemble de principes pour une réglementation de l'usage des technologies numériques dans les processus électoraux qui soit conforme aux droits fondamentaux.

2. À l'occasion de l'adoption du rapport conjoint, les rapporteurs ont noté que "l'internet et les médias sociaux ont ouvert de nouvelles possibilités de participation politique et sont devenus essentiels dans le processus électoral". Dans le même temps, "les défis électroniques à la démocratie, y compris la cybercriminalité, étaient néanmoins élevés et extrêmement complexes, en raison notamment de la nature sans frontières d'Internet et de la propriété privée de l'information. Une réponse juridique à ces défis était nécessaire. Une certaine forme de réglementation était nécessaire, mais elle devait respecter les libertés fondamentales, en particulier la liberté d'expression, la liberté économique, le droit à la vie privée et les droits sociaux". [1]

3. Les rapporteurs du rapport conjoint ont également été désignés comme rapporteurs pour les présents principes, à savoir M. Barrett, Mme Kjerulf Thorgeirsdóttir, M. Rubio Nuñez et M. Vargas Valdez.

4. Les présents principes, qui ont été préparés sur la base des commentaires soumis par les experts ci-dessus, ont été approuvés par le Conseil des élections démocratiques lors de sa 70e réunion (en ligne, 10 décembre 2020) et adoptés par la Commission de Venise lors de sa 125e session plénière (en ligne, 11-12 décembre 2020).

II. CONTEXTE

A. Technologies numériques et démocratie

5. Comme indiqué au paragraphe 143 du rapport conjoint, "[l]a la démocratie et les technologies numériques entretiennent des relations complexes. D'une part, internet et les réseaux sociaux sont devenus le premier forum d'échanges politiques dans certaines démocraties ; l'usage de ces outils a aiguisé l'esprit critique des citoyens envers leurs élus, et leur généralisation facilite l'organisation de mouvements sociaux à grande échelle ainsi qu'une interaction plus étroite entre citoyens et partis politiques. D'autre part, les nouveaux outils virtuels peuvent être utilisés lors des élections, et parfois même contre elles, pour faire baisser la participation, modifier les résultats et subtiliser les données des électeurs ; contre les responsables et partis politiques, pour mener des actions de cyberespionnage à des fins de contrainte et de manipulation et discréditer publiquement des personnalités ; et contre les médias, traditionnels et sociaux, pour diffuser désinformation et propagande et façonner les opinions des électeurs. Le nouvel espace numérique ouvre la voie à de nouvelles formes de criminalité et de commercialisation des données qui menacent sérieusement le droit à la vie privée. Il module aussi les interactions sociales en montrant ou en dissimulant de manière sélective (et parfois stratégique) des informations à ses utilisateurs, avec pour résultat de favoriser une vision partielle de la réalité et d'entraver la liberté d'expression." [2]

[1] Voir le compte rendu de la session du 11 juillet 2019, CDL-PL-PV(2019)002rev, page 16.

[2] Il convient de noter qu'outre ces dangers liés à la manipulation délibérée et à l'utilisation abusive des outils et processus électoraux, la technologie comporte également d'autres risques qui ne sont pas liés à des préjudices ou violations intentionnels, par exemple : la fracture numérique dans l'accès aux technologies numériques ou dans leur utilisation ; le manque de connaissance du fonctionnement des nouveaux espaces d'information en ligne (le

6. Sur la base de ce scénario, le débat entre "apocalyptique et intégré" (Eco) s'est emparé de la relation entre technologie et démocratie." Les technologies numériques ont remodelé la manière dont les sociétés traduisent la volonté du peuple en votes et en représentation, et elles ont dans une large mesure modifié les campagnes politiques. Même si les technologies numériques favorisent certains aspects de la compétition démocratique, elles les entravent également. L'omniprésence mondiale des technologies numériques a déplacé l'arène du débat démocratique vers le monde virtuel, soulevant de nombreuses questions sur leur influence sur la participation électorale et la nécessité de superviser et de réguler le comportement social en ligne". [3]

7. Ces dangers, directement liés à la technologie, affectent les différentes phases du processus électoral, telles que : la désignation des candidats, dans laquelle la collecte de signatures pour les candidats indépendants ou la réalisation d'élections primaires peut se faire via des applications qui risquent de créer des problèmes affectant le processus ; l'enregistrement des candidats et des électeurs ; les initiatives d'information des électeurs (campagnes d'éducation des électeurs) ; la campagne électorale, qui empiète sur le libre développement de la volonté de l'électeur ; le financement politique/de la campagne et sa transparence ; le processus de vote lui-même ; le décompte des voix et l'établissement des résultats des élections ; le processus de règlement des litiges électoraux.

8. Nous sommes confrontés à un certain nombre de menaces qui

a) sont développées à différents niveaux (national, local/sous-national et international) ;
b) utilisent un nouveau concept du temps, dans lequel l'immédiateté de l'information influe sur la prise de décision et le fait que certains contenus peuvent se propager très rapidement peut avoir un impact sur l'application efficace des remèdes ;
c) impliquent une variété d'acteurs différents : partis, médias, citoyens et entreprises privées, qui sont en dehors des modèles de régulation exclusivement centrés sur le rôle des médias et des partis ;
d) sont réalisées par des actions qui combinent les avantages de la nouvelle infrastructure technologique, qui évolue rapidement, et le potentiel de manipulation.

9. Comme indiqué précédemment, ces menaces peuvent non seulement entraîner la modification des résultats définitifs des élections, mais aussi porter atteinte à des principes démocratiques fondamentaux tels que la transparence ou le secret du vote, entre autres. Les moyens par lesquels elles érodent la confiance dans le système démocratique et mettent en doute la légitimité des élus sont presque aussi importants. En tout état de cause, les menaces susmentionnées mettent en péril à la fois la "démocratie électorale" - entendue comme les activités institutionnelles et les infrastructures qui rendent les élections possibles, et communément appelée dans le contexte d'Internet "e-gouvernement" -, la "démocratie délibérative" - comprise comme la participation des individus à un débat ouvert dans la conviction qu'il conduira à de meilleures décisions sur des questions d'intérêt commun - et la "démocratie de suivi" - comprise comme la responsabilité publique et le contrôle public des décideurs, qu'ils opèrent dans le domaine des institutions étatiques ou interétatiques ou au sein d'organisations dites non gouvernementales ou de la société civile, telles que les entreprises, les syndicats, les associations sportives et les organisations caritatives. Les cybermenaces aux élections prennent donc différentes formes selon qu'elles concernent la démocratie électorale (par des attaques

rôle des médias, le rôle des plateformes en ligne, l'utilisation de données personnelles pour personnaliser la communication avec les électeurs, etc. Ces sujets ne sont pas analysés en détail dans le présent document, mais il est important de les mentionner pour des études complémentaires, des sous-principes ou d'autres documents qui pourraient être développés à l'avenir, dans les termes du paragraphe 21.

[3] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 47.

contre la confidentialité, l'intégrité et la disponibilité des ordinateurs et des données électorales) ou la démocratie délibérative/de suivi (par des opérations d'information avec violation des règles visant à garantir des élections libres, équitables et propres). [4]

10. D'autre part, les nouvelles technologies offrent des solutions différentes aux défis auxquels sont confrontés les processus électoraux contemporains. Il existe toute une série de perspectives qui s'offrent au système démocratique, depuis les questions logistiques telles que les économies de coûts, la réduction de l'impact sur l'environnement grâce à la diminution de l'utilisation du papier, jusqu'aux questions qui renforcent la légitimité démocratique telles que : le financement des campagnes par les citoyens ; la transparence du financement ; l'inscription électronique sur les listes électorales (dans les pays où l'inscription est nécessaire pour voter) ; la déclaration publique des informations électorales que les gouvernements, les partis politiques et les candidats proposent en ligne - cette déclaration publique vise à garantir les droits d'utiliser, de partager et de commenter ces informations ; la communication rapide des préoccupations électorales à un public mondial (par exemple, la diffusion d'une vidéo sur le bourrage des urnes ou de vidéos sur la violence électorale), qui peut aider à documenter des abus qui auraient pu être cachés. Enfin, la promotion de la participation électorale par les autorités doit être envisagée, par exemple par des campagnes publicitaires utilisant les réseaux sociaux ou par l'utilisation de la technologie pour localiser les bureaux de vote sur une carte.

11. Plus précisément, "[g]râce à internet, chacun peut désormais s'informer sur les élections et exprimer ses opinions, échanger avec les candidats et participer activement aux campagnes électorales. Les réseaux sociaux en particulier, en tant que principal forum de débat politique, sont devenus des sources d'information politique ". [5] De plus, l'nternet permet de s'assurer que l'information parvient aux groupes marginalisés et à la diaspora et leur permet de participer aux débats électoraux.

12. Néanmoins, même si "l'internet a le pouvoir d'être un outil de démocratie... son potentiel à cet égard est menacé... [car la] même technologie qui facilite le discours crée des possibilités de censure de l'information, de surveillance des pratiques en ligne et de modelage et de manipulation subtils des comportements". [6]

13. D'un point de vue, l'internet ne serait qu'un canal de communication, plus ou moins répandu dans la population, et dont le caractère virtuel implique qu'il n'a qu'un impact limité sur la prise de décision. Cette vision ignore l'impact que ce "canal" a sur le reste des canaux et, surtout, les transformations qu'il génère dans la manière dont la société communique et s'organise.

14. L'internet influence clairement la façon dont les gens communiquent, se comportent et se forgent une opinion. La vitesse et la portée de la technologie numérique ont non seulement transformé la façon dont l'opinion publique peut se former, mais ont également fourni les moyens de déformer la réalité dans une mesure inconnue auparavant à l'époque du journalisme traditionnel avec la transmission de nouvelles, d'informations et d'idées. L'utilisation abusive de la technologie numérique pour manipuler les faits, diffuser des informations de manière stratégique et coordonnée, effectuer une surveillance en recueillant des informations auprès des citoyens (et à leur sujet) et en faisant participer les groupes d'acteurs politiques, a affecté la confiance des citoyens dans les institutions démocratiques et l'État de droit. L'impact de la technologie numérique sur l'autonomisation des citoyens et la représentation démocratique est remis en question à la lumière de ce qui précède et la question se pose de savoir si ou comment

[4] Voir ci-dessous le principe 6.

[5] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 35.

[6] Laidlaw 2015, p. 1.

cette technologie peut être gérée pour prévenir les facteurs de distorsion des droits fondamentaux tels que la liberté d'expression, d'opinion et d'information et le droit à la vie privée par une surveillance massive à des fins politiques/financière.

15. Ceux qui affirment que la technologie transforme le sens même de la politique[7] soutiennent que la disponibilité d'un plus grand volume d'informations et d'une plus grande transparence, directement liée, s'accompagne d'une participation, que l'on a appelée la récupération du pouvoir de la part des citoyens. La croissance de l'information à la disposition des citoyens, en plus de la facilité existante de se mettre en relation avec d'autres citoyens, augmente leur capacité à recevoir l'information et à la traiter, leur capacité à s'organiser et leurs possibilités de faire parvenir leurs propositions aux institutions.[8] En bref, cela implique un changement majeur dans la façon de faire de la politique, qui a entraîné l'émergence de nouvelles alternatives dans le cadre de structures politiques informelles ou inhabituelles, même dans le processus électoral. De l'électeur, les citoyens qui le souhaitent sont en passe de s'intégrer dans les processus politiques.

16. Ce changement de protagonistes signifie que la politique, longtemps réservée aux hommes politiques et aux médias, donne de plus en plus de poids aux citoyens. La communication politique, traditionnellement associée à l'information et à la propagande, devient la construction de relations politiques permanentes : une immense conversation de millions de personnes parlant à des millions de personnes (en *tête à tête*), dans leurs propres mots et sur une longue période ; une conversation qui, lorsqu'elle trouve un objectif clair (qu'il s'agisse d'une élection ou d'une décision des autorités) devient une mobilisation sociale.

17. Des éléments commencent à être remis en question en raison de l'impact de la technologie, comme l'excès et la rapidité des informations qui rendent difficile la distinction entre les faits et la fiction et permettent de noyer dans la désinformation stratégique et trompeuse des informations d'un intérêt public crucial pour le processus électoral, que le public est en droit de recevoir. La célèbre citation de James Madison en faveur de la liberté d'expression selon laquelle "le savoir gouvernera toujours l'ignorance ; et un peuple qui veut être son propre gouverneur doit s'armer du pouvoir que donne le savoir" est remise en question par rapport à la technologie numérique et à la démocratie. Les attentes élevées quant aux avantages de l'utilisation de la technologie pour renforcer les démocraties sont maintenant contrées par des préoccupations croissantes quant aux menaces qu'elles représentent : "Algocratie", "Dictadonnées", "Armes de destruction mathématique", ne sont que quelques-uns des nombreux termes utilisés pour décrire cette menace. D'où le rôle important du journalisme de qualité, basé sur l'analyse, qui souffre également de ces évolutions mais reste crucial pour la compréhension des processus électoraux démocratiques par les citoyens.

18. Bien que, comme nous l'avons vu précédemment, ces dangers menacent le processus démocratique en général, ils doivent être analysés avec prudence lorsqu'il s'agit de campagnes électorales. L'innovation a toujours été au cœur des campagnes. Celui qui connaît, comprend et peut utiliser les nouvelles technologies a un avantage concurrentiel, jusqu'à ce que tous les autres adoptent les mêmes pratiques et que celles-ci se normalisent chez tous les candidats. Des problèmes surgissent lorsque la technologie cesse d'être un

[7] Kollock, P., Smith, M., (1995) ; Hagen, M. (1997) ; Castells, M. (1998) ; Bimber, B., (1998) ; Leadbetter, C., (1999) ; Hall, M., (1999) ; Clift, S., (1998) ; Badillo, Á. y Margenghi, P. (2001) ; Subirats, J. (2002) ; Rheingold, H., (2002) ; Savigny, H., (2002) ; Lim, M., (2002) ; Krueger, B. S., (2002) ; Tolbert, C. J., Mcneal, R. S., (2003) ; Bennett, W. L. (2003) ; Chadwick A. (2003, 2006) ; Rogers, R. (2004) ; Dahlgren, P. (2005) ; Simone, M (2006) ; Benkler, Y. (2006) ; Friedland, L., Hove, T. Y Rojas, H., (2006) ; Shirky, C., (2008) ; Drezner, D. y Farrel H., (2008) ; Dutton, W. H. (2010).

[8] D'un autre côté, on peut faire valoir que cela n'entraîne pas nécessairement une plus grande autonomie des utilisateurs, car beaucoup d'entre eux sont mal équipés pour traiter des informations provenant de diverses sources (ils ne reconnaissent pas l'importance de leur diversité), ou ne souhaitent pas s'engager avec des sources qui pourraient s'opposer à leurs croyances et opinions.

avantage concurrentiel et se transforme en une menace pour l'intégrité des élections, limitant le droit à des élections libres.

19. Aujourd'hui plus que jamais, la transmission de messages entraîne un changement radical dans la communication. Nous assistons à la prolifération parallèle de l'information et à sa pollution à l'échelle mondiale. Les partis politiques et les candidats se sont vu attribuer de nouvelles plates-formes leur permettant de communiquer directement avec leur électorat, et les citoyens eux-mêmes se sont vu attribuer des plates-formes qui étaient auparavant l'apanage des partis politiques. La publicité traditionnelle a été remplacée par de nouvelles formes de communication qui tentent d'adapter les messages à des sections spécifiques de l'électorat ainsi que par de nouveaux canaux de communication. En conséquence, les messages sont devenus de plus en plus personnalisés. Ceux qui conçoivent les campagnes ne doivent plus penser aux masses, car la plupart des individus sont déjà soit convaincus, soit perdus. Ils doivent donc plutôt se concentrer sur le petit groupe d'électeurs qui ont un pouvoir d'influence, pour lesquels les techniques de campagne sont axées sur le "one-to-one" ou le "many-to-many". Ce changement créé par la technologie a des conséquences directes sur les différents acteurs qui sont soumis à la législation électorale. Elles concernent la spécificité de la réglementation en matière de protection des données, l'utilisation des recensements et des bases de données, l'achat de publicité en ligne, notamment sur les médias sociaux en période électorale, l'activité des individus sur les médias sociaux la veille du scrutin ou la publication des sondages électoraux sur des pages web qui ne sont pas ancrées dans le territoire national.

20. Ce flux constant et simultané d'informations en temps réel sur de multiples plateformes représente un énorme défi pour la surveillance des comportements et des ressources pendant les campagnes politiques. Il existe, en gros, deux formes différentes de campagnes électorales problématiques qui sont facilitées dans ce contexte : premièrement, la manipulation par les partis politiques, les candidats et leurs campagnes et, deuxièmement, les activités malveillantes telles que les campagnes de désinformation concertées, les comptes problématiques (bots amplifiant les faux messages, comptes se faisant passer pour des acteurs légitimes, etc.) ou le cyber-espionnage, qui impliquent des activités potentiellement illégales. En outre, la création de contenus dispersés et anonymes entrave sérieusement l'identification et l'attribution des responsabilités pour les comportements illégaux en ligne, où les électeurs peuvent être gravement affectés dans leurs décisions par des informations trompeuses, manipulatrices et fausses destinées à influencer leur vote, ce qui compromet l'exercice du droit à des élections libres et crée des risques considérables pour le fonctionnement d'un système démocratique. En outre, les algorithmes qui régissent les moteurs de recherche et les médias sociaux peuvent favoriser une compréhension partielle et parfois illusoire de la politique et de la démocratie. [9]

21. Comme on peut le conclure de cette section, les technologies numériques ont un impact différent, tant positif que négatif, sur les différents types de démocratie (électorale, délibérative et de suivi) et sur toutes les étapes des processus électoraux. En tenant compte de cela, les sections suivantes se concentreront principalement sur l'impact d'Internet et des médias sociaux sur les campagnes électorales. Bien que les principes soient applicables au cycle électoral dans son ensemble et soulignent l'importance de la libre communication pendant les périodes électorales, cette approche ouvre la possibilité de développer d'autres rapports, principes ou sous-principes qui pourraient se concentrer sur les technologies utilisées à d'autres stades des processus électoraux, dans de futurs documents.

[9] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 37, qui fait référence à Quintana 2016 ; Fidler 2017 ; Van Dijck 2013 ; McChesney 2013.

B. Acteurs impliqués

22. Traditionnellement, les campagnes électorales ont été comprises comme une série d'actions menées par les candidats, les partis politiques ou leurs membres pour obtenir le soutien des citoyens, et c'est cette définition que la législation a principalement abordée. Dans cette perspective, la campagne est avant tout identifiée comme l'ensemble des mesures qui trouvent leur origine dans le parti politique (telles que les lettres, les affiches, les réunions, les spots ou les déclarations publiques), tandis que l'État a un rôle dans l'organisation et la surveillance du processus électoral.

23. L'une des caractéristiques les plus importantes concernant l'impact des nouvelles technologies sur les campagnes électorales est l'augmentation significative du nombre d'acteurs de la campagne, indépendants des partis. La communication n'est plus centralisée, avec une seule source individuelle (qu'il s'agisse d'un homme politique, d'un parti ou d'un organe de presse) communiquant avec un large public de particuliers, mais décentralisée, avec de nombreuses sources individuelles communiquant avec le public de particuliers. Aujourd'hui, n'importe qui peut montrer son soutien à un candidat particulier en ligne, télécharger une vidéo au contenu critique ou envoyer des courriels promouvant une candidature sans aucun lien officiel avec la campagne. Toutefois, ces activités peuvent avoir un impact beaucoup plus important sur le résultat final de la campagne, en provoquant un changement qualitatif, et peuvent conduire à des controverses.

24. De nouveaux acteurs, issus d'organisations de la société civile ou de particuliers, peuvent jouer un rôle clé dans la campagne, non seulement en diffusant les messages du candidat en ligne, mais aussi en achetant des annonces pour renforcer ou affaiblir les positions des candidats. Ces acteurs peuvent agir sans lien avec la campagne officielle et même travailler en dehors des barrières nationales. Dans ce contexte, la responsabilité des plateformes de médias sociaux dans le cadre des régimes politiques / de financement des campagnes actuels, qui consiste à assurer la transparence et la responsabilité du placement, des dépenses et de l'attribution des annonces afin de mieux informer les citoyens du contexte dans lequel les choix électoraux sont faits, gagne en importance critique.

25. Avec ces nouveaux acteurs, sont apparus des profils anonymes autorisés par les plateformes sociales. Le poids que prend la communication interpersonnelle à travers les réseaux sociaux a conduit à la création massive de bots, des comptes anonymes, automatisés et parfois factices qui agissent comme des individus en ligne et augmentent la diffusion massive d'informations spécifiques, visant à créer des courants d'opinion publique, d'acceptation ou de rejet de personnes ou d'idées, de manière artificielle. En donnant l'impression qu'ils bénéficient d'un large soutien, ces dispositifs créent un effet de vague, et d'autres acceptent les idées partagées par cette majorité apparente. Cela génère un comportement grégaire, par lequel les individus négligent leur responsabilité personnelle et se soumettent à la volonté du collectif.

26. Le processus décisionnel des électeurs est contrecarré par la création et la diffusion massive de fausses informations par le biais de faux profils, dont beaucoup sont automatisés. L'anonymat mentionné ci-dessus permet même aux candidats et aux partis de développer des campagnes non officielles, en profitant de la liberté de ne pas être soumis à la réglementation électorale - car ils peuvent apparaître comme des citoyens ordinaires ou utiliser de fausses identités afin d'avoir un plus grand impact sur la campagne électorale. Ces options ont créé de nouveaux et graves défis pour les régimes politiques / de financement des campagnes existants.

27. Les nouvelles technologies provoquent le passage de campagnes basées sur l'information ou la propagande, clairement différenciées selon l'auteur, le parti politique ou la source médiatique, à un format dans lequel la conversation devient un élément clé, gagnant de plus en plus d'importance, et dans lequel les opinions, les informations personnelles, les réunions non officielles et les émissions de propagande officielles ou non officielles fusionnent. La combinaison

de cet aspect avec la prolifération des acteurs dans les campagnes génère des problèmes concernant l'extension éventuelle de la responsabilité des hommes politiques devant les citoyens pour le contenu de leurs communications.

28. Un autre groupe d'acteurs à prendre en compte est celui des médias de masse, notion dont la portée a été remise en cause du fait de l'émergence d'Internet : s'étend-elle encore aux seules versions en ligne des médias écrits ou audiovisuels, ou encore aux blogueurs individuels qui publient des informations ou des opinions en utilisant les nouvelles technologies avec leurs propres pages web, qui sont leur propriété et leur responsabilité ? [10]

29. Par conséquent, la distinction entre les médias et les individus sur l'internet devenant moins pertinente, l'accent devrait être mis sur le contenu plutôt que sur les sujets. Par exemple, les moyens traditionnels de solliciter des votes la veille d'une élection, comme par le biais d'une conversation, diffèrent grandement de ceux proposés par les nouvelles technologies, qui permettent à une même personne d'envoyer une chaîne anonyme de SMS, de "bombarder" des courriels et des commentaires ou même de créer de la publicité payante sur une page web ou un blog. L'expansion des campagnes politiques sape les filtres traditionnels fondés sur les valeurs journalistiques de vérité, de vérification des faits et de séparation des opinions et des faits. Cela a affaibli l'efficacité des règles traditionnelles régissant les allégations fausses et trompeuses.

30. Enfin, les intermédiaires tels que les moteurs de recherche et, peut-être plus encore, les plates-formes de médias sociaux, [11] ont acquis de nouvelles positions puissantes de "gatekeeper" qui leur permettent d'influencer le résultat des processus électoraux. Les moteurs de recherche, considérés comme fiables par une majorité, ont le potentiel d'influencer l'attention et les préférences de vote de l'électorat. Un classement biaisé des résultats des moteurs de recherche peut faire pencher les électeurs indécis vers un seul candidat. Cela pourrait conduire à de nouvelles formes d'influence dans les élections qui ne sont pas prises en compte par les règles existantes.

31. Comme le souligne le rapport conjoint, [12] " [p]eu nombreux, les très puissants acteurs privés littéralement propriétaires des autoroutes de l'information défendent leurs propres droits et intérêts commerciaux, qui tendent à heurter à la fois les droits civils et politiques et les principes électoraux. Ces prestataires d'internet assument désormais le rôle de gardiens autrefois dévolu aux médias traditionnels, mais sans avoir adopté les engagements éthiques de ces médias. Ainsi, des entreprises privées censurent les contenus qu'elles jugent « nuisibles » sans rendre de comptes et sans transparence sur leurs actions. Certes, des entreprises de réseaux sociaux ont récemment adopté une série de mesures destinées à lutter contre les fausses actualités et à enrayer leur propagation, en particulier en période électorale. [...] Cependant, de telles initiatives sont volontaires et sporadiques et ne s'appuient pas sur un cadre juridique reconnu. " [13]

---

[10] Voir par exemple l'arrêt de la Cour de justice de l'Union européenne (grande chambre) du 16 décembre 2008 (affaire C 73/07), qui indique que l'importance de la liberté d'expression exige une interprétation large de la notion de "journalisme", précisément pour mieux protéger la diffusion de contenus en ligne ; les exceptions à la protection des données "s'appliquent non seulement aux entreprises de médias mais aussi à toute personne exerçant une activité journalistique" (point 58) ; "le support utilisé pour transmettre les données traitées, qu'il soit de nature classique, comme le papier ou les ondes radio, ou électronique, comme l'internet, n'est pas déterminant pour déterminer si une activité est exercée "uniquement à des fins journalistiques"" (point 60).

[11] Jusqu'à présent, les plateformes de médias sociaux se sont révélées plus problématiques, peut-être parce qu'elles permettent à des tiers d'accéder à leurs bases de données d'utilisateurs, qu'elles permettent l'extraction d'une énorme quantité de données personnelles des utilisateurs et, en même temps, qu'elles ne se limitent pas aux résultats de recherche mais peuvent offrir des messages spécifiques et personnalisés dans un espace personnalisé.

[12] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 145.

[13] En outre, les cadres réglementaires nationaux varient considérablement et ont eu un impact différent tant sur les entreprises technologiques que sur leur propre impact sur les processus électoraux.

C. De nouveaux défis en termes de temps et d'espace

32. Les campagnes électorales limitées aux territoires où se déroulaient les élections, ont été radicalement modifiées avec les possibilités d'internet. En conséquence, nous sommes confrontés au problème de la transformation du monde numérique en monde réel, en termes traditionnels. Dans ce processus, le législateur devra tenir compte d'éléments tels que le serveur dans lequel la page web est hébergée (ce qui n'affecte pas sa disponibilité), l'adresse IP (lieu de la connexion qui facilite l'activité) ou la propriété du site, et la nationalité du propriétaire.

33. Cependant, ces réalités "physiques" n'influencent pas l'impact que peut avoir une publication sur Internet, dans un territoire donné. Aujourd'hui, le fait que les médias et les individus soient situés "virtuellement" au-delà de nos frontières est susceptible d'entraîner l'interdiction de certaines activités, notamment la publication de publicité en ligne la veille des élections, ou la publication d'informations confidentielles le jour du scrutin, comme les résultats des sondages de sortie des urnes. Ces possibilités démontrent qu'il est nécessaire d'établir les critères qui empêcheraient même les partis ou les candidats eux-mêmes de développer des campagnes en fournissant des informations provenant de l'extérieur du territoire national, soit en hébergeant le site web, soit en étant le lieu où les personnes menant la campagne en ligne peuvent se connecter.

34. Il est également difficile d'appliquer les critères de proportionnalité et d'égalité de l'espace informatif dans les systèmes qui l'exigent. Si les espaces internet et les médias sociaux (en particulier dans les médias publics) doivent garantir l'équité, il semble assez compliqué d'appliquer les critères traditionnels à un espace d'information aussi ouvert qu'internet.

35. L'internet offre aux partis et aux candidats la possibilité de maintenir des "bureaux d'information permanente", qui donnent aux citoyens la possibilité d'accéder à une quantité infinie d'informations sous différents formats. Cette "intemporalité", assurée par les nouvelles technologies, influence également les campagnes électorales. Deux éléments essentiels de l'internet sont son instantanéité et son interactivité, qui influent considérablement sur le calendrier établi pour la réalisation de la campagne électorale. Il serait intéressant de reconsidérer le concept de sollicitation de votes, un processus qui se divise entre les périodes de pré-campagne (ou campagne permanente) et de campagne. De même, l'opportunité de distinguer entre le financement des campagnes et le financement des partis politiques semble discutable.

36. Il est également nécessaire d'aborder la question de l'interdiction des campagnes politiques pendant la veille des élections, dont la nature se heurte à celle de l'internet en tant que média asynchrone, dont le contenu est permanent et accessible à tous à tout moment, sans que les partis politiques aient besoin de prendre quelque mesure que ce soit : les événements politiques, les messages, les vidéos, la propagande, etc. de l'ensemble de la campagne sont à la disposition du citoyen, y compris la veille des élections. Le problème est de nature quantitative, car on peut constater un problème similaire en ce qui concerne les affiches électorales qui remplissent les rues pendant toute la campagne et dont le retrait immédiat la veille du scrutin est non seulement impossible mais n'a jamais été proposé comme garantie du processus électoral. Il semble également évident que l'envoi massif de courriels et de SMS dans le cadre de la campagne ou d'une autre publicité électorale la veille du scrutin serait contraire à la logique de la législation actuelle.

37. Enfin, l'intemporalité et l'extraterritorialité des nouvelles technologies posent un défi pour l'enquête, la poursuite et la sanction des activités illégales liées aux processus électoraux. Ce défi a déjà été décrit dans le rapport conjoint et doit être relevé.

D. Normes internationales et droits en conflit

38. Les menaces susmentionnées interfèrent avec un certain nombre de droits fondamentaux protégés au niveau européen et universel par plusieurs déclarations et conventions internationales, telles que la Déclaration universelle des droits de l'homme (ci-après dénommée "DUDH"), le Pacte international relatif aux droits civils et politiques (ci-après dénommé "PIDCP"), la Déclaration américaine des droits et devoirs de l'homme, la Convention américaine des droits de l'homme, la Charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme (ci-après dénommée "CEDH").

39. Le rapport conjoint comprend un aperçu des normes et instruments européens et internationaux pertinents, en mettant l'accent sur la CEDH et d'autres instruments juridiques élaborés par le Conseil de l'Europe. Il est fait référence à cette vue d'ensemble dans le présent contexte.[14] Les normes et politiques du Conseil de l'Europe dans ce domaine sont également présentées dans le Compendium "Elections, technologies numériques, droits de l'homme". [15]

40. Le rapport conjoint conclut que "la tenue d'élections démocratiques, et donc l'existence même de la démocratie, serait impossible sans le respect des droits de l'homme, dont notamment les libertés d'expression, de la presse, de réunion et d'association à des fins politiques, dont la création de partis politiques. Le respect de ces libertés devient encore plus crucial en période de campagne électorale. Les restrictions à ces droits fondamentaux doivent respecter la Convention européenne des droits de l'homme et, plus généralement, être prévues par la loi, obéir à l'intérêt général et respecter le principe de proportionnalité. Lorsque des droits entrent en conflit, des critères clairs pour les mettre en balance devraient être énoncés dans la législation et effectivement mis en oeuvre à travers les dispositifs électoraux et la justice ordinaire ". [16]

41. A cet égard, le rapport conjoint souligne qu' "au niveau du Conseil de l'Europe, beaucoup a déjà été fait pour relever les défis évoqués plus haut. Entre autres, la Convention de Budapest prévoit une série d'outils de prévention de la cybercriminalité – y compris en période électorale – et de coopération internationale en vue de recueillir des preuves électroniques ; point à noter, les travaux actuels sur un deuxième Protocole additionnel à cette Convention devraient y ajouter de nouvelles possibilités de coopération internationale renforcée et d'accès aux données dans le cloud. Par ailleurs, il existe déjà une série de normes juridiques sur la protection de la vie privée et des données personnelles dans le contexte des réseaux sociaux. En particulier, la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, qui est ouverte à tous les pays du monde et fixe des normes internationales, devrait constituer le traité universel en matière de protection des données. Enfin, plusieurs instruments juridiques ont été élaborés pour assurer des élections libres, en prévoyant notamment la réglementation du financement des campagnes électorales et des mesures contre les inégalités de couverture médiatique, en ligne et hors ligne, en période électorale. " [17]

42. " Dans le même temps, plusieurs documents du Conseil de l'Europe pointent d'autres améliorations possibles. En particulier, le rapport *Les désordres de l'information*, paru en 2017, formule plusieurs recommandations à l'attention des pouvoirs publics, des ministères de

[14] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphes 48 et suivants.
[15] Voir https://edoc.coe.int/fr/elections/8142-elections-digital-technologies-human-rights-compendium.html .
[16] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 142.
[17] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 150.

l'Éducation, des médias, des entreprises de technologies et de la société civile pour réagir aux difficultés posées par la montée de la mésinformation, de la désinformation et de l'information malveillante et à son impact sur les processus démocratiques ; et l'étude *Internet et campagnes électorales*, également parue en 2017, conclut que le cadre réglementaire actuel ne suffit plus à assurer l'équité des règles du jeu politique et à limiter le rôle de l'argent dans les élections et suggère plusieurs mesures pour remédier à cette situation. " [18]

43. Plusieurs facteurs rendent toute réglementation dans ce domaine particulièrement difficile : comme mentionné précédemment, la nature sans frontières de l'internet ; l'implication de divers acteurs - en particulier privés - ; le fait que certaines réglementations - par exemple dans le domaine du financement des campagnes - ne sont pas applicables ou sont inadéquates dans le contexte en ligne. En outre, plusieurs droits et libertés fondamentaux sont en jeu et peuvent, dans certaines situations, entrer en conflit les uns avec les autres, notamment la liberté d'expression, la protection des données personnelles et de la vie privée, le droit à des élections libres, l'égalité et la liberté du commerce.

44. Par exemple, comme le souligne le rapport conjoint, [19] selon la Cour européenne des droits de l'homme (ci-après la CourEDH), les droits à la liberté d'expression (article 10 de la CEDH) et à des élections libres (article 3 du protocole n°. 1 à la CEDH) sont, d'une part, des conditions préalables l'un à l'autre, [20] mais d'autre part, ils peuvent entrer en conflit et il peut être jugé nécessaire, dans la période précédant ou pendant une élection, d'imposer certaines restrictions à la liberté d'expression, d'un type qui ne serait généralement pas acceptable, afin de garantir la "libre expression de l'opinion du peuple dans le choix du corps législatif".[21] En même temps, toute restriction à la liberté d'expression doit être proportionnée au but légitime poursuivi et nécessaire dans une société démocratique.

III. ENSEMBLE DE PRINCIPES

45. Pour faire face aux défis posés par l'utilisation des technologies numériques à la "démocratie électorale", à la "démocratie délibérative" et à la "démocratie du suivi", le rapport conjoint comprend plusieurs recommandations à prendre dans une perspective interdépendante et globale. Il souligne en particulier que "le fait qu'internet ne connaisse pas de frontières et que les autoroutes de l'information se trouvent entre les mains d'acteurs privés rend particulièrement complexes les défis que rencontrent aujourd'hui la démocratie et les processus électoraux. Une coopération internationale, et la participation des acteurs privés concernés, s'avèrent donc indispensables pour relever ces défis et préserver à l'avenir le droit à des élections libres et le fonctionnement même de la démocratie. " [22]

46. En gardant ces considérations à l'esprit, la Commission de Venise a élaboré plusieurs principes qui devraient être respectés par les législateurs, les régulateurs et les autres acteurs[23] impliqués dans l'utilisation des technologies numériques dans les élections et qui sont exposés

[18] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 151.
[19] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 151.
[20] Plaizier, 2018.
[21] CourEDH, *Bowman c. Royaume-Uni,* 19 février 1998, n° 24839/94 ; CourEDH, *Orlovskaya Iskra c. Russie*, 21 février 2017, n° 42911/08.
[22] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 153.
[23] À cet égard, l'attention est également attirée sur L'Initiative mondiale des réseaux (« Global Network Initiative) et ses « Principes de liberté d'expression et de respect de la vie privée » qui visent à fournir des orientations et des conseils au secteur des TIC et à ses parties prenantes : https://globalnetworkinitiative.org/gni-principles/

ci-dessous. Ils soulignent la nécessité d'une approche conforme aux droits de l'homme ; les droits de l'homme et les libertés fondamentales doivent être traduits dans l'environnement numérique. Afin de garantir une réponse globale et cohérente aux défis susmentionnés, il pourrait s'avérer nécessaire d'aller plus loin et d'élaborer de nouveaux instruments juridiques internationaux. Dans cette perspective, la Commission de Venise soutient les travaux actuels entrepris par les organes compétents du Conseil de l'Europe, notamment le Comité ad hoc sur l'intelligence artificielle (CAHAI), le Comité européen sur la démocratie et la gouvernance (CDDG) et le Comité d'experts sur l'environnement des médias et la réforme (MSI-REF).

Principe 1
Les principes de la liberté d'expression impliquant un débat public solide doivent être traduits dans l'environnement numérique, en particulier en période électorale.

47. La protection de la liberté d'expression, d'opinion et d'information est essentielle pour le processus politique démocratique. Dans la jurisprudence de la Cour européenne des droits de l'homme, le concept de société démocratique est particulièrement pertinent en ce qui concerne les délibérations politiques précédant les élections. Le discours politique bénéficie de la plus haute protection, qui étend à tous les individus le droit de participer au débat.[24] C'est pourquoi le flux d'information est protégé des deux côtés, celui de la transmission et de la réception et non seulement verticalement mais aussi horizontalement, c'est-à-dire entre les utilisateurs du réseau eux-mêmes.

48. La Cour européenne des droits de l'homme a estimé que les principes de la jurisprudence de la Cour concernant la liberté d'expression doivent être traduits dans l'environnement numérique : L'article 10 ne protège pas seulement le contenu des informations mais aussi les moyens de leur diffusion, car toute restriction fondée sur ces derniers interfère nécessairement avec le droit de recevoir et de communiquer des informations.[25] Sur la place publique numérique, les politiques de contenu doivent être conformes aux principes de la liberté d'expression. Garantir un débat public ouvert est la question clé à cet égard : Le "libre échange des opinions et des idées" souligné par la Grande Chambre de la CourEDH[26] est crucial pour l'environnement démocratique.

49. L'article 10 est la seule disposition de la CEDH qui assortit les droits qu'elle contient de devoirs et de responsabilités. Dans la jurisprudence de la CEDH, la presse (presse écrite, médias audiovisuels, médias en ligne, etc.) est l'organisme public de surveillance qui joue un rôle crucial pour la démocratie. Elle a le devoir de communiquer au public des informations et des idées de toutes sortes d'intérêt public, et c'est en outre le droit corollaire du public de recevoir des informations et des idées de toutes sortes - également celles qui heurtent, choquent ou inquiètent[27] et peuvent donc "faire des vagues" ; les opinions exprimées dans un langage fort et exagéré, les satires exagérant et déformant la réalité dans le but de provoquer et d'agiter sont protégées en vertu de l'article 10. [28] Non seulement la presse est protégée dans son rôle spécial de surveillance publique, mais le rôle d'autres surveillants sociaux est également reconnu, notamment les ONG, les militants politiques, l'opposition politique, les scientifiques, les intellectuels, les blogueurs et tous ceux qui veulent contribuer à un discours public critique ainsi qu'à des informations et des idées controversées. [29]

[24] Herdís Thorgeirsdóttir, Journalism Worthy of the Name, Freedom within the Press and the Affirmative Side of Article 10 of the European Convention on Human Rights, Martinus Nijhoff Publishers, 2005.
[25] Voir CourEDH, *Autronic AG c. Suisse*, 22 mai 1990, n° 12726/87.
[26] CourEDH, *Gillberg c. Suède*, 3 avril 2012, n° 41723/06.
[27] CourEDH, *Handyside c. Royaume-Uni*, 7 décembre 1976, n° 5493/72.
[28] CourEDH, *Eon c. France,* 14 mars 2013, n° 26118/10 ; CourEDH, *Kuliś et Różycki c. Pologne*, 6 octobre 2009, n° 27209/03 ; CourEDH, *Alves da Silva c. Portugal,* 20 octobre 2009, n° 41665/07.
[29] Voir CourEDH, *Observer et Guardian c. Royaume-Uni*, 26 novembre 1991, n° 13585/88 ; CourEDH, *Guerra et autres c. Italie*, 19 février 1998, n° 116/1996/735/932.

50. L'observation générale n° 34 du Comité des droits de l'homme des Nations unies sur l'article 19 du PIDCP précise à ce sujet :

> *"“43. Toute restriction imposée au fonctionnement des sites Web, des blogs et de tout autre système de diffusion de l'information par le biais de l'Internet, de moyens électroniques ou autres, y compris les systèmes d'appui connexes à ces moyens de communication, comme les fournisseurs d'accès à Internet ou les moteurs de recherche, n'est licite que dans la mesure où elle est compatible avec le paragraphe 3. Les restrictions licites devraient d'une manière générale viser un contenu spécifique; les interdictions générales de fonctionnement frappant certains sites et systèmes ne sont pas compatibles avec le paragraphe 3. Interdire à un site ou à un système de diffusion de l'information de publier un contenu uniquement au motif qu'il peut être critique à l'égard du gouvernement ou du système politique et social épousé par le gouvernement est tout aussi incompatible avec le paragraphe 3. ". [30]*

51. La Cour européenne des droits de l'homme a reconnu qu'Internet est devenu l'un des principaux moyens d'exercer le droit à la liberté d'expression et d'information. Par conséquent, les mesures de blocage de l'accès ne sont compatibles avec la CEDH que si un cadre juridique strict est en place, qui réglemente la portée de l'interdiction et offre la garantie d'un contrôle judiciaire pour prévenir d'éventuels abus.[31] En outre, la Recommandation CM/Rec(2016)5 sur la liberté d'internet prévoit que l'internet doit être disponible, accessible et abordable pour tous les groupes de la population sans aucune discrimination, et que toutes les mesures prises par les autorités de l'Etat ou les acteurs du secteur privé pour bloquer ou restreindre de toute autre manière l'accès à une plate-forme internet entière (médias sociaux, réseaux sociaux, blogs ou tout autre site web) ou aux outils des technologies de l'information et de la communication (TIC) (messagerie instantanée ou autres applications), ou toute demande des autorités de l'Etat de mener de telles actions doivent respecter les conditions de l'article 10 de la Convention concernant la légalité, la légitimité et la proportionnalité des restrictions.

52. Le 1er juillet 2016, le Conseil des droits de l'homme des Nations unies a adopté une résolution non contraignante condamnant les pays qui perturbent intentionnellement l'accès à Internet de leurs citoyens. La résolution s'appuie sur les déclarations précédentes des Nations unies sur les droits numériques, réaffirmant la position de l'organisation selon laquelle "les mêmes droits que les personnes ont hors ligne doivent également être protégés en ligne", en particulier la liberté d'expression couverte par l'article 19 du PIDCP et de la DUDH. [32]

53. De nombreux gouvernements (même des régimes associés à la démocratie plutôt qu'à un régime autoritaire) ont adopté une tactique de plus en plus répandue pour fermer l'internet afin d'étouffer la dissidence.[33] La justification que les autorités utilisent souvent est qu'elles essaient d'arrêter la diffusion de fausses informations haineuses et dangereuses, qui peuvent circuler plus rapidement sur Facebook, WhatsApp et d'autres services que leur capacité à les contrôler. Mais à mesure qu'Internet devient plus intégré à tous les aspects de la vie, les fermetures touchent bien plus de gens que les seuls manifestants ou les personnes impliquées dans la politique. [34]

54. La légalité des coupures d'internet n'est pas souvent testée devant les tribunaux. Dans les affaires concernant le blocage de l'accès à Internet, la Cour européenne des droits de l'homme a estimé qu'il y avait eu violation de l'article 10 de la CEDH lorsque la mesure en question

---

[30] Adopté par le Comité des droits de l'homme des Nations unies lors de sa 102e session (-1129 juillet 2011).
[31] CourEDH, *Ahmet Yıldırım c. Turquie,* 18 décembre 2012, n° 3111/10.
[32] Résolution n° 32/13, voir https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13 .
[33] Voir par exemple le Wall Street Journal, https://www.wsj.com/articles/internet-shutdowns-become-a-favorite-tool-of-governments-its-like-we-suddenly-went-blind-11582648765 ; Freedom House, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.
[34] Les fermetures peuvent même être dévastatrices pour les personnes qui essaient simplement de gagner leur vie, voir https://www.nytimes.com/2019/12/17/world/asia/india-internet-modi-protests.html.

produisait des effets arbitraires et que le contrôle juridictionnel du blocage de l'accès avait été insuffisant pour prévenir les abus. [35]

Principe 2
Pendant les campagnes électorales, un organe d'administration électorale (EMB) ou un organe judiciaire impartial et compétent devrait être habilité à exiger des entreprises privées qu'elles retirent de l'internet des contenus de tiers clairement définis, sur la base des lois électorales et conformément aux normes internationales.

55. La jurisprudence de la Cour européenne des droits de l'homme reconnaît le droit des individus à accéder à l'internet[36] et précise que sur la place publique numérique, les politiques de contenu doivent être conformes aux principes de liberté d'expression découlant de l'article 10 de la CEDH. Le discours politique, en particulier, bénéficie de la plus haute protection.

56. Toutefois, ce droit n'est pas illimité. En particulier, pendant les campagnes électorales, les autorités de l'État doivent être en mesure de demander aux entreprises privées de retirer les contenus de tiers insérés en violation de la législation électorale, conformément aux conditions de restriction de la liberté d'expression définies dans les traités relatifs aux droits de l'homme. [37]

57. L'organe compétent pour introduire une telle demande doit être soit un organe impartial d'administration électorale[38], soit un tribunal et agir rapidement. La décision de l'organe d'administration électorale devrait être soumise à un contrôle juridictionnel ; ce contrôle devrait également être exercé très rapidement afin de ne pas rendre la demande inefficace au cas où elle aurait un effet suspensif ou, au contraire, d'exclure en pratique tout recours contre une violation de la liberté d'expression si elle n'a pas un tel effet.

58. Le principe de la liberté d'expression ne doit pas être interprété dans le sens que les entreprises privées n'ont aucune responsabilité dans la divulgation d'informations politiques provenant de tiers. Comme l'explique le rapport conjoint, "les quelques acteurs privés qui possèdent les autoroutes de l'information sont suffisamment puissants et déréglementés pour dicter les conditions des libertés sociales, individuelles et politiques, devenant ainsi un troisième acteur dans l'arène démocratique", et "l'utilisation et l'abus de données à caractère personnel à des fins électorales, sous couvert de liberté du commerce, pourraient constituer une menace sérieuse pour les élections libres et l'équité électorale, au moins à trois égards : premièrement, parce que des acteurs privés pourraient utiliser ces informations pour exercer directement une influence indue sur la compétition électorale ; deuxièmement, parce que les sociétés Internet et de médias sociaux, arguant de la liberté du commerce, pourraient restreindre l'accès à ces informations en fonction de leurs préférences politiques, accordant ainsi un avantage opaque à certains partis ou candidats par rapport à d'autres ; et troisièmement, parce que la marchandisation des données à caractère personnel représente un défi pour la surveillance de l'argent dans les campagnes politiques." Tous ces comportements pourraient faciliter, dissimuler ou même constituer des atteintes à la démocratie qui doivent être poursuivies et sanctionnées.

[35] CourEDH, *Ahmet Yıldırım c. Turquie*, 18 décembre 2012, n° 3111/10.
[36] CourEDH, *Ahmet Yıldırım c. Turquie,* 18 décembre 2012, n° 3111/10.
37 Recommandation CM/Rec(2016)5 sur la liberté d'internet (Lignes directrices 2.2.1 - 2.2.2) ; Recommandation CM/Rec(2018)2 sur les rôles et responsabilités des intermédiaires d'internet (Ligne directrice 1.3.1).
[38] Dans certains pays, ce ne sont pas seulement les organes d'administration des élections (EMB), mais aussi les autorités de régulation des médias et/ou les autorités de protection des données (APD) qui sont chargées de certains aspects des activités de campagne électorale. Dans de telles situations, les États devraient permettre une coopération continue entre les organes concernés.

Principe 3
Pendant les périodes électorales, l'internet ouvert et la neutralité du réseau doivent être protégés.

59. Comme déjà indiqué dans le rapport conjoint, le défi consistant à protéger simultanément la liberté d'expression, les droits commerciaux et l'égalité électorale sans affecter les autres droits de l'homme exige la reconnaissance de (1) la nature transnationale du problème ; (2) le rôle essentiel joué par les gardiens des autoroutes de l'information ; et (3) la nécessité de renforcer le cadre juridique international "afin d'établir des mécanismes plus efficaces de coopération transnationale entre les nations et les acteurs privés et, si possible, de parvenir à une plus grande uniformité des législations nationales". En outre, les États et les acteurs privés doivent travailler sur des modèles de réglementation fondés sur la coresponsabilité de chacun et sur la promotion de l'autorégulation[39] "comme l'adoption obligatoire de codes d'éthique et de responsabilité sociale des entreprises, parmi les fournisseurs de services Internet et les entreprises de moteurs de recherche et de médias sociaux". Ceci est essentiel pour garantir les droits à l'égalité des chances et à la liberté d'opinion des électeurs, dont le respect est indispensable à la tenue d'élections conformes aux normes internationales. [40]

60. Le principe de neutralité du réseau signifie que les fournisseurs de services internet (FSI) doivent traiter toutes les communications internet de la même manière, c'est-à-dire qu'ils ne peuvent pas discriminer ou donner l'avantage à un contenu particulier en imposant des barrières économiques (par exemple en faisant payer un contenu spécifique) ou des obstacles structurels en bloquant ou en ralentissant. Cela signifie qu'il faut garantir des conditions de concurrence équitables pour les utilisateurs et les fournisseurs de contenu et empêcher les FAI de décider unilatéralement de la disponibilité des contenus en ligne. C'est la raison pour laquelle la neutralité du Net est essentielle pour un dialogue démocratique ouvert, [41] en particulier pendant la période cruciale des élections. Certains pays ont cependant choisi de poursuivre les objectifs d'un accès libre, ouvert et universel par d'autres stratégies réglementaires.

61. La Recommandation CM/Rec(2016)1 du Comité des Ministres du Conseil de l'Europe invite les Etats membres à sauvegarder le principe de neutralité des réseaux dans l'élaboration des cadres juridiques nationaux, afin de garantir la protection du droit à la liberté d'expression et à l'accès à l'information, ainsi que du droit à la vie privée. En outre, le règlement (UE) 2015/2120 établit des mesures concernant l'accès ouvert à l'internet. [42]

62. Cependant, la question de la neutralité du réseau est assez complexe. Il a été dit qu' "il n'existe pas d'instrument politique unique qui permette de réaliser simultanément l'ensemble des objectifs politiques et économiques appréciés. Contrairement à certaines des affirmations avancées dans le débat actuel, la sauvegarde d'objectifs multiples nécessite une combinaison d'instruments qui impliquera probablement des mesures gouvernementales et non gouvernementales. En outre, la promotion d'objectifs tels que la liberté d'expression, la participation politique, l'investissement et l'innovation nécessite des politiques complémentaires". [43]

---

[39] Récemment, le discours concernant les responsabilités des acteurs privés dans le contexte électoral a évolué vers des modèles de corégulation, dans lesquels l'État soit (i) imposerait certaines obligations de base (allant au-delà de l'éthique, comme des obligations spécifiques de transparence), mais dont la mise en œuvre relèverait d'organes d'autorégulation, avec la possibilité d'une surveillance de l'État ; soit (ii) n'introduirait qu'une législation d'appui pour assurer la surveillance des mesures d'autorégulation.
[40] Commission de Venise, CDL-AD(2002)023rev-cor, Code de bonne conduite en matière électorale, I.2.4 et I.3.1.
[41] Cf. Paolo Damiani, *The Open Internet vs. Net Neutrality and the Free Internet*. Federalismi. 2019 : La neutralité du Net protège la liberté contre la discrimination entre les types ou les sources de trafic Internet, sans tenir compte d'intérêts concurrents ou de considérations compensatoires".
[42] Disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.
[43] Johannes M. Bauer & Jonathan A. Obar (2014) Reconciling *Political and Economic Goals in the Net Neutrality Debate,* The Information Society, 30:1, 1-19, DOI ; voir 10.1080/01972243.2013.856362.

63. Une initiative remarquable pour traiter les questions de manipulation politique, de désinformation, de fausses nouvelles, de violations de la vie privée et d'autres forces malveillantes sur Internet est la proposition de contrat pour le Web de la World Wide Web Foundation.[44] Une telle initiative, si elle est largement soutenue et mise en œuvre au niveau mondial, pourrait avoir l'avantage particulier d'éviter les situations où le propriétaire d'une plate-forme de médias sociaux peut seul déterminer ce qui constitue un discours autorisé.

64. En tout état de cause, la Commission de Venise réitère ses recommandations antérieures, [45] qui visent, en période électorale, à garantir la neutralité du réseau, à envisager de renforcer juridiquement le droit des utilisateurs à un internet ouvert, à veiller à ce que les restrictions d'accès à des contenus internet reposent sur un cadre juridique strict et prévisible réglementant le champ de ces restrictions et à assurer une surveillance judiciaire pour prévenir les éventuels abus.

Principe 4
Les données personnelles doivent être protégées efficacement, en particulier pendant la période cruciale des élections.

65. L'article 8 de la CEDH prévoit la protection du droit à la vie privée. Ce droit assure "l'épanouissement de la personnalité des individus".[46] Sur cette base, la Cour européenne des droits de l'homme a développé une jurisprudence étendue en matière de protection des données à caractère personnel.[47] En outre, une série de normes juridiques ont été élaborées par le Conseil de l'Europe pour la protection de la vie privée et des données à caractère personnel, notamment dans le contexte des médias sociaux.[48] En particulier, la Convention modernisée du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+),[49] qui est ouverte à tout pays du monde et qui fixe des normes internationales, devrait servir de traité universel pour la protection des données. [50]

66. Les citoyens doivent être protégés lors du traitement des données à caractère personnel, en particulier pendant la période électorale où de grandes quantités de données personnelles sont traitées, y compris celles qui figurent dans les registres électoraux. En ce qui concerne les registres, la confidentialité des données doit être mise en balance avec la transparence requise pour l'intégrité électorale. Les nouvelles technologies font peser de nouvelles menaces sur la vie privée des électeurs, qui comprend actuellement le droit de garder son vote confidentiel, mais qui devrait être étendu pour inclure le droit de recueillir des informations avant de prendre une décision, ainsi que le droit à la navigation privée en ligne et à la communication libre sur l'internet. Le comportement en ligne de l'individu ne peut être surveillé sans le consentement libre,

---

[44] Cette initiative a été lancée par l'inventeur du web, Sir Tim Berners-Lee. Voir https://webfoundation.org/2019/11/launching-the-contract-for-the-web/ .

[45] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 152.

[46] CourEDH (Chambre), *A.-M.V. c. Finlande,* 23 mars 2017, n° 53251/13, paragraphe 76, disponible sur https://hudoc.echr.coe.int/eng#{%22itemid%22 : [%22001-172134%22]}

[47] Jurisprudence de la Cour européenne des droits de l'homme concernant la protection des données à caractère personnel, disponible à l'adresse suivante : https://rm.coe.int/case-law-on-data-protection/1680766992. Voir également la CEDH, 2018, "Guide sur l'article 8 de la Convention européenne des droits de l'homme - Droit au respect de la vie privée et familiale", disponible à l'adresse suivante : https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[48] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphes 76 et suivants.

[49] Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel modernisée par le protocole d'amendement STCE 223, disponible à l'adresse suivante : https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[50] Le préambule de cette convention fait explicitement référence au "droit à l'autonomie personnelle et au droit de contrôler ses données personnelles", soulignant l'importance de la liberté de choix.

spécifique, informé et non ambigu de la personne concernée ou tout autre fondement légitime prévu par la loi, conformément à l'article 5, paragraphe 2, de la Convention 108+. En outre, lorsque le traitement concerne des catégories de données sensibles telles que des informations révélant des opinions politiques, un consentement explicite peut également être requis à titre de protection complémentaire (article 6 de la Convention 108+).

67. Le traitement des données dans le cadre de la publicité électorale et politique (en particulier la publicité de microciblage) doit être conforme aux principes de protection des données prévus à l'article 5 de la Convention 108+. Ces données à caractère personnel doivent être traitées dans le respect des principes de limitation de la finalité et de minimisation des données. En particulier, conformément à la Recommandation CM/Rec(2012)4 du Comité des Ministres sur la protection des droits de l'homme à l'égard des services de réseaux sociaux, les réseaux sociaux doivent obtenir le consentement éclairé de leurs utilisateurs avant que leurs données à caractère personnel ne soient partagées avec d'autres catégories de personnes ou d'entreprises ou utilisées de manière autre que celle nécessaire aux fins spécifiées pour lesquelles elles ont été initialement collectées. Afin de garantir le consentement valable des utilisateurs, ceux-ci devraient pouvoir "opter" pour un accès plus large à leurs données à caractère personnel par des tiers (par exemple, lorsque des applications tierces sont exploitées sur le réseau social). De même, les utilisateurs devraient également pouvoir retirer leur consentement.

68. Considérant que les données à caractère personnel relatives aux informations qu'elles révèlent concernant les opinions politiques entrent dans le champ d'application de catégories spéciales de données au titre de l'article 6 de la Convention 108+, ce type de traitement est soumis à un régime plus strict. Le responsable du traitement des données dans le cadre de la publicité électorale et politique traite ce type de données à caractère personnel dans le respect des garanties supplémentaires appropriées prévues par la loi.

69. Selon l'article 9, paragraphe 1, point a), de la Convention 108+, toute personne a le droit de ne pas être soumise à une décision l'affectant de manière significative prise sur le seul fondement d'un traitement automatisé de données, sans que son avis soit pris en considération. Le profilage mis en œuvre par une décision uniquement automatisée peut être considéré comme "affectant de manière significative les individus s'il comporte un risque de manipulation".[51] Le profilage pour le microciblage peut, dans certains cas, être soumis à cette restriction. Les responsables du traitement des données doivent tenir compte de ce droit lorsqu'ils utilisent ce type de publicité.

70. Compte tenu de ces facteurs, un changement radical à l'échelle mondiale serait nécessaire. Tout d'abord, il serait nécessaire que toutes les entités politiques existantes élaborent des politiques de protection de la vie privée. Les autorités de réglementation devraient établir les critères d'utilisation autorisée des informations personnelles dans le cadre des processus électoraux. Toute modification de la politique de protection des données devrait être communiquée aux autorités électorales responsables du processus, et le non-respect de ces règles entraînerait des sanctions. En outre, toutes les personnes incluses dans la base de données devraient être tenues informées et il devrait être possible de les retirer de la base de données à tout moment.

71. Dans tous les cas, conformément aux recommandations précédentes de la Commission de Venise, il est nécessaire d'affirmer et de protéger le droit à l'anonymat sur Internet, de réglementer et de limiter strictement la création et l'utilisation de profils et d'envisager l'élaboration d'un instrument juridique spécifique (international/Conseil de l'Europe) pour faire face aux risques que l'utilisation des technologies numériques dans les élections représente pour la protection des

[51] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le profilage et la Convention 108+ : Suggestions pour une mise à jour. Strasbourg : 7 novembre 2019.

données personnelles.[52] Il est également essentiel de garantir un accès facile des utilisateurs aux données personnelles qui sont entre les mains des fournisseurs de services Internet, y compris les données personnelles pour les informations qu'ils révèlent concernant les opinions politiques en particulier.

Principe 5
L'intégrité électorale doit être préservée grâce à des règles et réglementations périodiquement révisées sur la publicité politique et sur la responsabilité des intermédiaires Internet.

72. Comme l'indique le rapport conjoint, il existe toute une série de normes internationales et du Conseil de l'Europe qui visent à protéger l'intégrité des élections, à garantir qu'elles soient libres et équitables et qu'elles ne soient pas influencées par un éventail étroit d'intérêts. Toutefois, les mesures législatives prises dans le passé, axées sur le contexte hors ligne, ainsi que leur applicabilité et leur efficacité, se sont révélées très limitées à l'ère de l'information - où la démocratie doit elle aussi s'adapter à l'environnement électronique ("démocratie électronique"). Entre autres, les limites de dépenses imposées à la radiodiffusion sont devenues moins significatives à l'époque de la publicité numérique, tandis que les réglementations en matière de transparence garantissant que les citoyens sont informés du financement et des dépenses des campagnes sont difficiles, voire impossibles à mettre en œuvre au-delà des frontières dans l'environnement numérique. Les problèmes dans ce domaine comprennent, entre autres, une réglementation dépassée des campagnes électorales du point de vue de la couverture médiatique, ainsi que dans la perspective plus large de la communication électorale ; le rôle accru des intermédiaires Internet sans responsabilités accrues ; le manque de transparence des dépenses numériques ; les difficultés à suivre les sources de financement des campagnes ; le « redlining » politique - ne s'engager qu'avec les électeurs considérés comme dignes de faire campagne (swing, électeurs indécis) ; le déclin du filtre éthique du journalisme ; et les préoccupations relatives à la vie privée.

73. La Commission de Venise a donc émis deux recommandations[53] qui restent très pertinentes et doivent être mises en œuvre :

- Révision des règles et l'encadrement de la publicité politique, au niveau de l'accès aux médias (mise à jour des quotas de diffusion, des limites et des catégories de supports médiatiques, adoption de nouvelles mesures couvrant les médias, plateformes et autres services en ligne, prise en compte des implications du micro-ciblage) et au niveau des dépenses (élargissement du champ des canaux de communication couverts par la législation pertinente, ajustement des capacités de surveillance des autorités nationales) ;
- Garantir la responsabilité des intermédiaires de l'internet, [54] en termes de transparence et d'accès aux données ; améliorer la transparence des dépenses, en particulier pour la publicité politique. En particulier, les intermédiaires internet devraient donner accès aux données sur la publicité politique payante, afin d'éviter de faciliter la participation illégale (étrangère) aux élections et d'identifier les catégories de publics cibles.

[52] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 152.
[53] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 152.
[54] Voir également les exigences de transparence et de responsabilité fixées par la Recommandation CM/Rec(2018)2 sur les rôles et responsabilités des intermédiaires Internet (Ligne directrice 2.2).

74. Dans la même veine, l'Assemblée parlementaire du Conseil de l'Europe[55] a récemment appelé les États membres à renforcer "la transparence de la publicité politique en ligne, de la diffusion de l'information et des algorithmes et modèles commerciaux des opérateurs de plateformes", notamment 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 termes de conditions et de tarifs pratiqués" et en "élaborant des cadres réglementaires spécifiques pour le contenu de l'internet en période électorale et en incluant des dispositions sur la transparence en ce qui concerne le contenu sponsorisé sur les médias sociaux, afin que le public soit informé de la source qui finance la publicité électorale ou toute autre information ou opinion [...]." [56]

75. Les mesures visant à résoudre les problèmes susmentionnés devraient s'efforcer d'accroître la transparence de la communication électorale afin de contrer les pratiques manipulatrices, de favoriser la transparence des dépenses électorales, d'assurer la transparence et le contrôle des algorithmes dans l'intérêt de l'exposition à la diversité, de garantir la protection de la vie privée afin de contrer le microciblage des électeurs et d'assurer une information précise et fiable afin de donner aux électeurs les moyens de leurs choix et de surveiller les processus électoraux.

76. Différentes mesures ont été prises par l'UE, les États membres de l'UE, les États-Unis, le Canada et les entreprises technologiques elles-mêmes pour accroître la transparence et limiter l'influence indue des acteurs malveillants. Ces tentatives de réglementation de la publicité politique en ligne comprennent des dispositions exigeant de révéler qui est derrière la publicité, qui l'a créée et le montant dépensé ; l'interdiction pour les étrangers de dépenser pour des campagnes ; et des mesures volontaires de transparence par les réseaux sociaux et autres plateformes internet.

77. Cela dit, on peut se demander si la transparence de la publicité politique payante est suffisante ou s'il en faut davantage pour faire reculer la situation où le pouvoir financier peut manipuler le processus électoral au point de menacer gravement la démocratie. Les publicités politiques payantes ne donnent pas seulement aux annonceurs un avantage déloyal en proliférant des messages très ciblés et souvent trompeurs, mais leur permettent de mettre sérieusement en danger ce qui devrait être "des élections libres, à intervalles raisonnables, au scrutin secret, dans les conditions qui assurent la libre expression de l'opinion du peuple dans le choix du corps législatif", comme le prévoit l'article 3 du Protocole n° 1 à la CEDH. L'interdiction de la publicité politique payante sur les médias sociaux peut donc être considérée comme une option afin de garantir un processus électoral équitable.

78. Le débat porte également sur la manière de remédier à la situation actuelle où quelques entreprises privées "ont un contrôle mondial sur le flux d'informations et sont donc en mesure de façonner le discours politique et la formation de l'opinion" et qui, en tant que propriétaires des autoroutes de l'information, "sont assez puissants et déréglementés pour imposer leur définition des libertés sociales, individuelles et politiques et devenir un troisième acteur de la scène politique ".[57] L'Assemblée parlementaire du Conseil de l'Europe[58] a récemment appelé les États membres "à briser le monopole des entreprises technologiques qui contrôlent, dans une large mesure, l'accès des citoyens à l'information et aux données" afin de garantir un "Internet ouvert et libre" qui "sert l'objectif des électeurs de s'informer et de s'engager davantage". La Commission

[55] Voir la résolution 2326 (2020) "La démocratie piratée ? Comment y répondre", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=28598&lang=EN&search=Kjoq.
[56] Conformément à la résolution 2254 (2019) "La liberté des médias comme condition d'élections démocratiques", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=25409&lang=en.
[57] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 13.
[58] Voir la résolution 2326 (2020) "La démocratie piratée ? Comment y répondre", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=28598&lang=EN&search=Kjoq.

de Venise soutient cet appel. Le principe 8 concernant l'adoption de mécanismes d'autorégulation développe cette question.

Principe 6
L'intégrité électorale doit être garantie en adaptant les réglementations internationales spécifiques au nouveau contexte technologique et en développant les capacités institutionnelles de lutte contre les cybermenaces.

79. Le Conseil de l'Europe a identifié deux types de cybermenaces aux élections.[59] Premièrement, les menaces à la démocratie électorale, à savoir les "attaques contre la confidentialité, l'intégrité et la disponibilité des ordinateurs et des données électorales", qui compromettent les bases de données ou les systèmes d'inscription des électeurs ; l'altération des machines de vote pour manipuler les résultats ; l'interférence avec le fonctionnement des systèmes le jour du scrutin ; et l'accès illégal aux ordinateurs pour voler, modifier, diffuser des données sensibles. Deuxièmement, les menaces pour la démocratie délibérative, c'est-à-dire les "opérations d'information avec violation des règles visant à garantir des élections libres, équitables et propres" liées à la protection des données, aux finances politiques, à la couverture médiatique des campagnes électorales et à la diffusion et la publicité politique. Ces menaces sont traitées par la Convention du Conseil de l'Europe sur la cybercriminalité STE 185 de 2001 ("Convention de Budapest"). [60]

80. Un problème majeur est que les données - et donc les preuves électroniques - sont volatiles et souvent détenues par des prestataires de services dans des juridictions étrangères ou stockées dans des juridictions multiples, changeantes ou inconnues. Une coopération internationale efficace et une coopération avec les prestataires de services sont nécessaires. Si la Convention de Budapest, dans sa forme actuelle, comprend des dispositions détaillées sur la coopération internationale combinant des mesures provisoires accélérées pour sécuriser les données et des dispositions sur l'entraide judiciaire, elles ne traitent pas suffisamment du problème de l'informatique dématérialisée et des problèmes de juridiction qui y sont liés, ni du fait que les prestataires de services d'un État offrent leurs services dans de nombreux autres États sans être présents ou responsables juridiquement ou physiquement dans ces derniers. Pour cette raison, les parties à la Convention de Budapest ont lancé la négociation d'un deuxième protocole additionnel pour permettre des options supplémentaires pour une coopération internationale renforcée et un accès aux données dans le cloud. [61]

81. Afin de garantir le droit à des élections libres "dans des conditions qui assurent la libre expression de l'opinion du peuple dans le choix du corps législatif", comme le prévoit l'article 3 du Protocole n° 1 à la CEDH, la Commission de Venise a émis trois recommandations concernant les cybermenaces[62] qui restent pertinentes et doivent être mises en œuvre :

- Eriger en infractions pénales les cyberattaques contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques électoraux, conformément à la Convention de Budapest sur la cybercriminalité ;
- Habiliter les autorités pénales à recueillir les preuves électroniques des atteintes aux règles sur la protection des données personnelles, le financement de la vie politique, la couverture médiatique ou la diffusion radiotélévisée d'informations électorales ;

[59] Voir le document concernant "La *cybercriminalité dans le processus électoral : le rôle de la Convention de Budapest*", 15e Conférence européenne des organes d'administration des élections "La sécurité dans les élections", Oslo, Norvège, 19-20 avril 2018 : https://rm.coe.int/coe-cyber-vc-oslo-april-2018-v1/16807bc437.
[60] Voir https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[61] Voir https://www.coe.int/en/web/cybercrime/t-cy-drafting-group .
[62] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 149.

- Préparer les administrations électorales (EMB) aux situations d'urgence et mettre en place une politique de gestion des crises. Les administrations électorales devraient être dotées des ressources et des formations nécessaires pour adopter les technologies numériques et traiter les risques de cybersécurité.

82. Dans ce domaine, qui est soumis à des évolutions techniques extrêmement rapides et aux nouvelles menaces qui pèsent sur le droit à des élections libres et équitables, il est nécessaire de revoir et d'actualiser constamment les lois et les outils disponibles pour leur mise en œuvre effective. Dans le même temps, il est crucial que les solutions juridiques trouvent un équilibre entre le droit à des élections libres et d'autres droits fondamentaux tels que la liberté d'expression et la protection des données, comme souligné ci-dessus dans le cadre des principes précédents.

83. En outre, des mécanismes de résolution des conflits (MRC) dans ce domaine doivent être définis. La nature transnationale et extraterritoriale des technologies numériques pose plusieurs défis : la définition ou la création d'autorités compétentes adéquates, les différentes réglementations nationales, les questions d'extraterritorialité, etc. En outre, la nature privée et commerciale des entreprises de l'internet exige des MRC plus adaptés à la logique du marché (c'est-à-dire des mécanismes alternatifs de résolution des conflits tels que l'arbitrage) - sans exclure des procédures juridictionnelles devant les tribunaux internationaux.

84. Il n'existe aucun critère établi au niveau international sur la manière de résoudre les problèmes de compétence pour poursuivre les cybercrimes et les comportements illicites en ligne. Une analyse comparative [63] montre que certains pays résolvent les revendications de territorialité en se fondant sur les catégories suivantes : lieu des actes, lieu des personnes, lieu de l'effet, nationalité de l'auteur ou nationalité de la victime.

85. Un autre défi est la conception de multiples approches réglementaires et de résolution des conflits qui engloberaient à la fois des modèles alternatifs et juridictionnels. En outre, la nature transnationale des comportements en ligne exige une autorité internationale (par exemple, un tribunal international) compétente pour résoudre les conflits au-delà des frontières nationales et régionales.

86. Enfin, les capacités institutionnelles doivent être renforcées pour prévenir les cybermenaces à la démocratie et aux processus électoraux. Les élections devraient être déclarées comme une infrastructure critique, et les capacités technologiques et les attributions juridiques des autorités électorales pour contrôler, enquêter et poursuivre les comportements illégaux en ligne devraient être renforcées.

Principe 7
Le cadre de coopération internationale et la coopération entre les secteurs public et privé devraient être renforcés.

87. Étant donné la nature transnationale du problème et le rôle essentiel joué par les acteurs privés, en particulier par les intermédiaires de l'internet (c'est-à-dire principalement les sociétés de moteurs de recherche et de médias sociaux, mais aussi les fournisseurs d'accès à l'internet), la Commission de Venise a recommandé[64] de renforcer le cadre international (1) pour établir des mécanismes plus efficaces de coopération transnationale entre les autorités nationales et les acteurs privés et, si possible, (2) pour apporter plus d'uniformité dans les législations nationales.

[63] Brenner, Susan & Koops, Bert-Jaap. (2005). *Approches de la juridiction en matière de cybercriminalité*. Journal of High Technology Law. 4.
[64] Voir le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 149.

Des objectifs similaires ont été fixés par le Programme mondial des Nations unies sur la cybercriminalité. [65]

88. En ce qui concerne la coopération internationale, comme il a déjà été souligné dans le cadre du principe précédent, il est nécessaire de créer des mécanismes pour rendre plus efficaces l'échange d'informations ainsi que les enquêtes, les poursuites et les sanctions relatives aux comportements illégaux en matière de démocratie et de nouvelles technologies. Cela implique également de déterminer dans quels domaines il est prioritaire de promouvoir l'homologation des législations dans plusieurs pays. L'efficacité des poursuites des infractions contre la démocratie est particulièrement pertinente pendant un processus électoral, car ces irrégularités peuvent avoir un impact direct sur la validité de l'élection.

89. Des suggestions pour une collaboration transnationale efficace ont été faites, par exemple en ce qui concerne les formats de demande standardisés, la clarté juridique des règles de procédure, l'authentification de l'identité du demandeur et du destinataire, l'établissement de normes de transparence dans les rapports, la détermination des normes qui doivent guider la prise de décision, un système de recours transnational et l'établissement de canaux de dialogue officiels et efficaces entre les parties prenantes. [66]

90. La nature transnationale des cybermenaces à la démocratie exige la collaboration active des gouvernements, des entreprises et des particuliers. La coopération public-privé est un aspect important de l'utilisation des nouvelles technologies dans les élections.[67] Les opérateurs et les plateformes doivent coopérer avec les autorités électorales, tant pour détecter les menaces que pour diffuser des informations officielles. Il convient également d'encourager la recherche et la coopération entre les autorités électorales, les universitaires et les praticiens afin d'évaluer l'impact réel des technologies numériques sur les processus électoraux et l'efficacité des mesures adoptées. Un aspect important est la clarification des responsabilités respectives.

91. Une autre idée de coopération pourrait être la création d'un "certificat numérique de responsabilité des entreprises" qui serait décerné aux intermédiaires de l'internet par une organisation internationale à laquelle participeraient des experts de gouvernements, d'entreprises et de la société civile du plus grand nombre de pays possible. Une telle initiative pourrait suivre l'exemple des certifications délivrées par l'ISO (Organisation internationale de normalisation) dont les experts élaborent des normes internationales pertinentes pour le marché qui favorisent l'innovation et apportent des solutions aux défis mondiaux. La norme ISO 26000 définit la "responsabilité sociale" comme "la responsabilité d'une organisation en ce qui concerne les impacts de ses décisions et activités sur la société et l'environnement" et inclut les principes suivants : responsabilité, transparence, comportement éthique, respect des intérêts des parties concernées, respect du principe de légalité, respect des règles internationales de comportement et respect des droits de l'homme. [68]

---

[65] Nations Unies. *Programme mondial sur la cybercriminalité*, voir https://bit.ly/358EsaD.

[66] De la Chapelle, Bertrand & Fehlinger, Paul. *La juridiction sur Internet : De la course aux armements légale à la coopération transnationale*. Centre pour l'innovation dans la gouvernance internationale et Chatham House. 2016. Disponible à l'adresse suivante : https://www.cigionline.org/sites/default/files/gcig_no28_web.pdf.

[67] Voir par exemple le code de pratique de l'UE en matière de désinformation. D'autres exemples de cette coopération sont mentionnés dans le rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphes 105f., notamment le Conseil consultatif pour l'Internet et les élections du Brésil, la coopération des opérateurs et des plateformes avec les autorités électorales du Mexique et du Panama, ainsi que diverses initiatives de vérification des faits. Notez également qu'en septembre 2019, Facebook, Twitter et Microsoft ont rencontré des représentants du gouvernement américain pour discuter d'éventuelles stratégies de collaboration pour les élections fédérales américaines de 2020, principalement pour éviter toute interférence étrangère ; voir Isaac, Mike. *Réunion des grandes entreprises technologiques avec des représentants du gouvernement américain sur la sécurité des élections de 2020*. New York Times. 2019. Disponible à l'adresse : https://nyti.ms/33IIwhm.

[68] Voir ISO 26000, disponible à l'adresse suivante : https://www.iso.org/iso-26000-social-responsibility.html

92. La Commission de Venise a également recommandé [69]

- de favoriser une éducation destinée à renforcer la culture juridique et démocratique chez les citoyens, sur la base de la coresponsabilité des acteurs privés et publics
- de donner aux électeurs les moyens d'évaluer de façon critique la communication électorale, mener des actions ciblées pour prévenir l'exposition à des informations fausses, trompeuses ou néfastes par l'éducation et la sensibilisation.

93. L'éducation doit permettre aux citoyens de se confronter à la nouvelle réalité numérique, non seulement en termes de fonctions de la technologie, mais aussi en termes de ses effets, en leur apprenant à distinguer l'important de l'insignifiant, la vérité du mensonge. Au-delà des stratégies éducatives de l'État, les entreprises et les organisations de la société civile pourraient conclure des alliances à la fois pour éduquer les internautes et pour évaluer l'efficacité des contrôles mis en place par les entreprises. [70]

94. Enfin, dans une démocratie mature et pleine, les médias doivent garantir la liberté d'expression et être transparents pour le public qui l'écoute, le voit ou le lit. C'est pourquoi la Commission de Venise a recommandé[71] de promouvoir une plus grande qualité dans le journalisme, en renforçant l'exactitude et la fiabilité des informations et des échanges avec le public, en renforçant les médias de service public et les médias locaux, et en renforçant l'autorégulation en mettant davantage l'accent sur la transparence des informations en ligne et leur diffusion.

95. À cet égard, il convient de noter que les caractéristiques de l'environnement numérique posent de sérieux défis tant pour la conception et la mise en œuvre de codes de déontologie journalistique[72] que pour la vérification de la véracité des informations, car les canaux numériques privilégient l'immédiateté et l'anonymat à la véracité, l'exactitude et la responsabilité. Les questions et considérations spécifiques au numérique devraient être intégrées de manière appropriée dans les codes d'éthique existants, ou des codes d'éthique journalistique numériques devraient être adoptés. Les États, les organes d'administration des élections, les médias et les plateformes devraient également être encouragés à collaborer à des projets de vérification.

Principe 8
L'adoption de mécanismes d'autorégulation devrait être encouragée.

96. Il existe des préoccupations valables concernant la prolifération de contenus illégaux ou abusifs en ligne tels que la diffusion de campagnes de désinformation ; les gouvernements (nationaux ou étrangers) ou les entreprises puissantes qui parrainent des groupes pour influencer les élections ; les entreprises ou acteurs puissants qui parrainent des attaques contre les opposants lors des élections ; ou les acteurs non étatiques qui exploitent le discours politique. À l'instar du marché mondial, l'internet est beaucoup plus difficile à gérer, à superviser et à contrôler que n'importe quelle entité nationale. D'une part, il convient d'éviter une réglementation

[69] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphes 149 et 152.
[70] La responsabilité partagée de l'État et du secteur privé est également soulignée, par exemple, dans le *Livre blanc sur les préjudices en ligne* (2019) présenté par le pouvoir exécutif au Parlement britannique : Le secrétaire d'État britannique pour le numérique, la culture, les médias et le sport et le secrétaire d'État pour le ministère de l'intérieur. *Livre blanc "Online Harms"*. 2019. Disponible à l'adresse suivante : https://bit.ly/32L4ajH.
[71] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 152.
[72] Si le contenu des médias et l'engagement envers les principes de l'éthique journalistique professionnelle ne diffèrent pas beaucoup selon le média utilisé, dans l'environnement numérique, il existe plusieurs considérations éthiques supplémentaires, telles que la manière de s'engager avec le contenu généré par l'utilisateur, la manière de garantir un droit de réponse, etc.

des contenus qui n'a pas de comptes à rendre et une censure trop large de la part des entreprises technologiques - qui les transformerait en semi-tribunaux (laissant les utilisateurs du réseau sans aucun contrôle judiciaire ni droit de recours). D'autre part, les sociétés de médias sociaux et les FSI ont des responsabilités en matière de droits de l'homme envers leurs utilisateurs.

97. En conséquence, la Commission de Venise a précédemment recommandé de promouvoir, *entre autres,* l'autorégulation, par exemple l'adoption obligatoire de codes de déontologie et de responsabilité sociale des entreprises par les prestataires de services internet et les entreprises de moteurs de recherche et de réseaux sociaux.[73] De même, l'Assemblée parlementaire du Conseil de l'Europe a appelé les professionnels et les organisations du secteur des médias à élaborer des cadres d'autorégulation qui contiennent des normes professionnelles et éthiques relatives à leur couverture des campagnes électorales, y compris le respect de la dignité humaine et le principe de non-discrimination.[74] Des mesures telles que l'adoption de codes d'éthique numérique pour les entreprises et de mécanismes d'autorégulation pour résoudre les conflits entre les entreprises et les utilisateurs permettraient également une plus grande flexibilité réglementaire au profit des intérêts des utilisateurs et des entreprises, tout en dépressurisant la relation avec le gouvernement et en favorisant la coresponsabilité des comportements en ligne.

98. Selon le guide d'autorégulation des médias en ligne de l'OSCE, [75] "la règle de base qui doit être respectée est que plus le processus d'autorégulation est interne, plus il sera efficace, proportionné et respectueux des droits fondamentaux". Dans le même temps, le guide met également en garde contre plusieurs risques, notamment en ce qui concerne l'efficacité (en fin de compte, les entreprises ne peuvent forcer personne à se conformer à leurs codes), les priorités (les intermédiaires Internet sont des entreprises privées dont la priorité est de faire des bénéfices et de rester en activité, et non de protéger la liberté d'expression) et les incitations indésirables (les autorités chargées de l'application des lois, dont les ressources sont limitées, ne donneront plus la priorité à certaines infractions en ligne si elles pensent pouvoir compter sur les intermédiaires Internet).

99. Dans une démocratie mature et pleine, une plate-forme de contenu ou un réseau social doit, dans la mesure du possible, garantir la véracité du contenu publié, ou au moins avertir des risques potentiels qu'impliquent certaines publications ou sources. Les plateformes ont déjà adopté une série de mesures telles que l'obligation de signaler clairement les annonces politiques et les annonces de diffusion et de les limiter aux utilisateurs autorisés ; la suppression des faux comptes ; l'approbation de certains contenus et sources ; l'amélioration de la transparence du processus d'achat d'annonces politiques (acheteurs, montant, contenu, etc.). Si ces initiatives - qui ont été adoptées soit volontairement, soit pour se conformer à la loi - sont généralement les bienvenues, elles risquent également de placer la responsabilité de la garantie des droits fondamentaux entre les mains de particuliers. [76]

100. En tout état de cause, il est crucial que la réponse aux défis posés par les technologies numériques sur la démocratie et les droits de l'homme ne soit pas laissée aux seuls mécanismes d'autorégulation. Comme l'a récemment déclaré l'Assemblée parlementaire du Conseil de l'Europe, [77] "malgré cette contribution du secteur privé, de nombreux problèmes de réglementation restent sans solution et ne peuvent être résolus que par des conventions

[73] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale des droits de l'homme et de l'État de droit (DGI) sur l'utilisation des technologies numériques et les élections, CDL-AD(2019)016, paragraphe 149.
[74] Conformément à la résolution 2254 (2019) "La liberté des médias comme condition d'élections démocratiques", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=25409&lang=en .
[75] Organisation pour la sécurité et la coopération en Europe (OSCE). *Le guide d'autorégulation des médias en ligne*. 2013. Lien : https://www.osce.org/fom/99560.
[76] Il convient toutefois de noter que des pratiques très similaires peuvent déjà être constatées dans le domaine du droit de la propriété intellectuelle.
[77] Voir l'exposé des motifs de la résolution 2326 (2020) "La démocratie piratée ? Comment y répondre", http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=28598&lang=EN&search=Kjoq.

internationales ainsi que par la législation au niveau national et international. Les meilleures pratiques et une meilleure coopération entre les agences de sécurité devraient devenir normatives dans la défense des élections démocratiques". En outre, "les chercheurs et les journalistes doivent avoir un meilleur accès aux données sur les faux comptes et la désinformation sans que les sociétés de médias sociaux ne les contrôlent strictement. Les décideurs politiques ne peuvent pas réglementer ce qu'ils ne comprennent pas, ni les mettre en œuvre et sanctionner le non-respect des règles sans vérifications et contrôles indépendants". Cela devrait également s'appliquer aux observateurs électoraux indépendants (nationaux mais aussi internationaux), tout en assurant la protection de la liberté d'expression et de la vie privée des utilisateurs. En outre, il convient de garantir la transparence et l'accessibilité des réglementations des entreprises privées (par exemple, les politiques de contenu électoral), y compris les mécanismes de recours, et la transparence des données qu'elles suppriment ou autorisent.

101. À cet égard, il a également été déclaré à juste titre[78] que toute solution proposée par les entreprises technologiques doit être "prudente, adaptable et innovante, tout en respectant pleinement les normes internationales en matière de liberté d'expression". Les codes de conduite spécifiques adoptés conjointement par les entreprises et les institutions publiques, par exemple le code de pratique de l'UE en matière de désinformation et le code de conduite sur la lutte contre les discours de haine illégaux en ligne, qui a été élaboré par la Commission européenne en collaboration avec plusieurs grandes entreprises de technologie numérique (Facebook, Microsoft, Twitter et YouTube), constituent des exemples de ces solutions. La tâche la plus ambitieuse dans ce domaine serait la création d'un organisme d'autorégulation indépendant pour les médias sociaux au niveau international. [79]

102. En outre, les sociétés de médias sociaux, les moteurs de recherche, les agrégateurs de contenu et les autres intermédiaires internet concernés doivent, par exemple, indiquer dans leurs accords les règles que les utilisateurs doivent respecter, les conditions de service régissant l'utilisation des plateformes de médias sociaux et le type de contenu que la société interdira (à condition que cette interdiction soit générale et n'interdise pas un discours autrement légal), et offrir une procédure de recours rapide et fiable aux utilisateurs qui estiment que leur contenu a été illégalement ou incorrectement bloqué ou retiré. Comme déjà mentionné, les sites de médias sociaux ont déjà mis en œuvre des politiques de modération de contenu en vertu desquelles ils suppriment certains contenus.[80] L'incitation directe à la violence ou à une activité illégale n'est pas un discours protégé, et elle peut et doit être interdite sur les plateformes de médias sociaux et sur l'internet. [81]

[78] Article 19. *Autorégulation et "discours de haine" sur les plateformes de médias sociaux*. 2018. Londres. Disponible à l'adresse : https://bit.ly/2Wx4y3X.
[79] Ibid.
[80] Cf. le rapport "Free Speech and the Regulation of Social Media Content" du service de recherche du Congrès américain, du 27 mars 2019. Disponible à l'adresse suivante : https://fas.org/sgp/crs/misc/R45650.pdf.
[81] Voir le raisonnement de la CEDH dans l'affaire *Delfi AS c. Estonie* (requête n° 64569/09, CEDH, 16 juin 2015).