Strasbourg, 24 juin 2019 **CDL-AD(2019)016**

Avis n° 925 / 2018 Or. angl.

COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT

(COMMISSION DE VENISE)

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 LES TECHNOLOGIES NUMÉRIQUES ET LES ÉLECTIONS

Adopté par le Conseil des élections démocratiques lors de sa 65e réunion (Venise, 20 juin 2019)

Adopté par la Commission de Venise lors de sa 119e session plénière (Venise, 21-22 juin 2019)

sur la base des observations de
M. Richard BARRETT (membre, Irlande)
Mme Herdís KJERULF THORGEIRSDOTTIR (membre, Islande)
M. Rafael RUBIO NUÑEZ (membre suppléant, Espagne)
M. José Luis VARGAS VALDEZ (membre suppléant, Mexique)
Mme Krisztina ROZGONYI (experte de la DGI, Division Médias et gouvernance de l'internet)
Mme Nevena RUZIC (experte de la DGI, Division de la Protection des données)

Table des matières

I. Introduction

1. Lors de sa 59e réunion (15 juin 2017), à l'initiative de M. José Luis Vargas Valdez, déjà auteur d'une étude sur le rôle des réseaux sociaux et d'internet dans le développement de la démocratie (CDL-LA(2018)001), le Conseil des élections démocratiques a décidé d'entreprendre une étude sur l'utilisation des technologies numériques lors des processus électoraux, en coopération avec le Service de la société de l'information du Conseil de l'Europe.

2. Mmes Krisztina Rozgonyi et Nevena Ružić sont intervenues en qualité d'expertes, respectivement pour la Division des médias et de la gouvernance d'internet (Direction de la société de l'information et de la lutte contre la criminalité) et pour la Division de la protection des données. M. Alexander Seger, directeur de la Division de la Cybercriminalité, a également contribué aux passages pertinents de ce rapport conjoint.

3. Le présent rapport conjoint a été préparé sur la base de l'étude initiale de M. Vargas Valdez et des observations soumises par les rapporteurs et les experts ; il a été examiné lors de la réunion de la Sous-commission sur l'Amérique latine le 30 novembre 2018, adopté par le Conseil des élections démocratiques lors de sa 65e réunion (Venise, 20 juin 2019) puis adopté par la Commission de Venise lors de sa 119e session plénière (Venise, 21 et 22 juin 2019).

II. Généralités

4. Les technologies numériques (ou « nouvelles technologies ») et les réseaux sociaux – définis comme des « plateformes en ligne permettant des échanges de contenus générés par leurs utilisateurs[1] » – ont révolutionné nos échanges et notre manière d'exercer notre liberté d'expression et d'information, ainsi que d'autres droits fondamentaux – parfois difficiles à concilier[2]. Les personnes inscrites sur des réseaux sociaux utilisent parfois internet pour s'organiser et exiger de meilleurs services, plus de transparence et une véritable participation à la vie politique[3]. Dans le monde entier, de simples individus peuvent désormais faire évoluer les mentalités, mettre un thème en lumière au niveau national ou appeler au militantisme politique[4]. Cette évolution est en train de transformer les rapports entre les États et leurs citoyens.

5. D'après le Rapport digital global 2018, plus de la moitié du trafic web mondial passe désormais par les téléphones mobiles. Sur les 7,6 milliards d'habitants que compte la planète, 4 milliards environ utilisent internet (soit 53 % de la population) et 3,2 milliards utilisent activement les réseaux sociaux (soit 42 % de la population).

6. Entre 2017 et 2018, le nombre d'utilisateurs d'internet s'est accru de 7 % et celui des réseaux sociaux, de 13 %. L'internaute moyen passe environ six heures par jour en ligne. Une bonne

[1] Aux fins de cette étude, les réseaux sociaux sont définis comme « des plateformes sur internet ou sur mobile permettant la communication entre utilisateurs et des échanges de contenus générés par les utilisateurs. Les réseaux sociaux ne sont donc pas des médias à source unique, ou diffusés depuis un site internet statique. Ils sont conçus pour permettre aux utilisateurs de créer (« générer ») des contenus et d'interagir avec les informations et avec leur source » (International IDEA 2014 : 11). Bien que les réseaux sociaux passent par internet, il faut noter que tous les sites et toutes les plateformes internet ne correspondent pas à la définition d'un réseau social. Certains sites ne prévoient pas d'interactivité avec leur public ; d'autres n'autorisent les utilisateurs qu'à poster des commentaires en réaction à un contenu publié, ouvrant une série d'échanges (« fils de discussion ») qui sont modérés et contrôlés (International IDEA 2014 : 11).

[2] Assemblée parlementaire du Conseil de l'Europe, Résolution 1987 (2014) sur le droit d'accès à internet.

[3] Santiso, 2018.

[4] On peut citer plusieurs exemples notables, des adolescents égyptiens qui ont appelé sur Facebook à se rassembler place Tahrir au poids de la désinformation sur l'issue de l'élection présidentielle au Kenya ; des Chiliens qui ont milité en ligne pour que le vote par correspondance devienne un enjeu électoral majeur, via la campagne « Haz tu voto volar », au projet mexicain de vérification de faits « Verificado2018 ».

partie de ce temps est consacrée aux réseaux sociaux comme Facebook (2,167 milliards d'utilisateurs), YouTube (1,5 milliard), Instagram (800 millions) ou Twitter (330 millions).

7. Aujourd'hui, quelque deux milliards d'internautes utilisent quotidiennement les réseaux sociaux[5], devenus un élément indispensable des campagnes politiques modernes. Leur impact sur les électeurs dépend de facteurs multiples : variables spécifiques aux réseaux utilisés (par exemple, Twitter ou Instagram ?), caractéristiques et prédispositions du public, motivations des utilisateurs et contexte global de la campagne[6].

8. Bien qu'à première vue, « tout le monde » utilise internet et les réseaux sociaux, les différents groupes d'âges en font un usage différent. D'après le *Digital News Report 2017* du Reuters Institute, les réseaux sociaux tendent à constituer la principale source d'actualités pour les personnes de 18 à 34 ans, tandis que la télévision reste plus importante pour les personnes de plus de 55 ans.

9. D'après la même étude du Reuters Institute, plus de la moitié des personnes interrogées (54 %) préfèrent choisir leurs informations via des canaux utilisant des algorithmes (moteurs de recherche, réseaux sociaux, agrégateurs) plutôt que des rédacteurs ou des journalistes (44 %). Il se peut, par conséquent, que les jeunes citoyens opèrent leurs choix politiques sur la base d'informations filtrées par des algorithmes et non par des journalistes appliquant les normes de leur profession. Cependant, il faut noter que selon des recherches récentes[7], les recommandations personnalisées à l'aide d'algorithmes pourraient aboutir à une offre d'actualités aussi diversifiée qu'une sélection éditoriale humaine.

10. D'après le *Digital News Report* 2018 du Reuters Institute, le recours aux réseaux sociaux pour consulter l'actualité aurait décru en 2017. La confiance des internautes envers ce type de source semble avoir diminué. Le rapport observe aussi qu'« internet, à l'origine avant tout utilisé pour consulter des informations, s'est rapidement mué en environnement participatif, reflétant davantage la participation démocratique telle qu'on la connaît dans le monde physique[8] ». L'usage massif d'internet et des réseaux sociaux dans le monde entier est donc en train de modifier de nombreux aspects de notre vie sociale et politique. Les mécanismes sociaux permettant d'apprendre et de se forger une opinion sont devenus plus collaboratifs et autorégulés (comme sur Wikipedia ou Facebook) et le militantisme politique a trouvé de nouvelles modalités, très efficaces, d'organisation et d'expression[9].

11. On a vu en internet, à ses débuts, une promesse d'égalité et de liberté. Ce pouvait être l'aube d'une *nouvelle sphère publique*, lieu d'échanges démocratiques ouverts où chacun pourrait participer au débat public, les discussions sur les réseaux sociaux permettant d'éclairer les citoyens et de rendre plus efficace l'exercice de la démocratie politique. La sphère publique avait auparavant une structure hiérarchisée, avec différentes fonctions bien établies et réparties entre différents acteurs : État, médias, Église ou établissements éducatifs – qui ont tous, aujourd'hui, perdu le contrôle sur les échanges horizontaux d'informations et d'opinions entre utilisateurs. Les réseaux sociaux promettaient de permettre à chacun de s'exprimer. Contrairement aux médias classiques, internet offre une architecture multidirectionnelle et sans bornes, pour un coût d'accès relativement faible. Ces qualités en font un média particulièrement bien placé pour que le citoyen lambda, au lieu de simplement recevoir l'information, contribue activement ; elles ont créé une sphère publique en réseau dans laquelle les individus peuvent

[5] Statista, enquête sur les réseaux sociaux les plus populaires du monde en octobre 2018. Disponible sur : https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[6] Dimitrova et Matthes, 2018.
[7] Voir https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1444076 et https://www.thatseemsimportant.com/content/blame-the-algorithm/.
[8] Laidlaw 2015, p. 7.
[9] Castells 2011 ; Cohen et al. 2012.

surveiller – et troubler – l'usage du pouvoir médiatique grâce à un accès immédiat à plusieurs sources d'information et de diffusion.

12. À travers leurs pratiques éditoriales et leurs obligations éthiques, les journalistes ont été par le passé les « gardiens des communications ». Ils décidaient ce qui méritait d'être imprimé ou publié, tout en veillant au respect de la loi : obligation faite aux médias publics d'assurer une couverture juste et équilibrée, respect de périodes de silence le cas échéant et/ou droit de réponse et autres recours pour les partis et les candidats. Ce rôle de gardien échoit aujourd'hui de plus en plus à de nouveaux intermédiaires, notamment les prestataires de services internet (ISP), les moteurs de recherche et les réseaux sociaux. On appelle *intermédiaires d'internet*[10] les organisations (principalement des entreprises à but lucratif) qui « réunissent des tiers sur internet ou facilitent les échanges entre eux. Ils mettent à disposition, hébergent, transmettent et indexent sur internet des contenus, produits et services provenant de tiers ou offrent à des tiers des services en ligne ». Ces intermédiaires ont donc mis la main sur la circulation, la disponibilité et l'accessibilité des informations et des autres contenus en ligne, et sur la possibilité même de les trouver[11].

13. Internet a suscité de grands espoirs parce qu'il contournait les monopoles de communication existants ; mais en réalité, de grands groupes multinationaux[12] contrôlent le flux des informations dans le monde entier et sont donc en mesure de façonner le discours politique et les opinions. Les forces à l'œuvre sont les mêmes que dans le paysage médiatique traditionnel, mais les réseaux sociaux amplifient désormais leurs voix, qui peuvent atteindre chaque recoin du monde et transformer des vies et des sociétés entières. L'idée qu'il devrait y avoir sur internet un minimum de concurrence, un peu de place pour de nouveaux arrivants, ne semble plus de mise. Les quelques acteurs privés propriétaires des super-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 ; et la production de contenus est devenue si « démocratique » et anonyme qu'il est extrêmement difficile de distinguer les informations fiables et d'attribuer les responsabilités en cas de comportements illégaux en ligne.

14. Les réseaux sociaux, comme Facebook, dépendent autant des forces du marché que les médias traditionnels. La valeur boursière de Facebook, comme celle de tous les grands groupes médiatiques, est fonction de ses recettes publicitaires. Or, la publicité sur Facebook, qui permet au site de croître et de conserver sa valeur, fonctionne par détermination des centres d'intérêt de ses utilisateurs sur la base des données collectées à partir de leur navigation, de leurs « j'aime », etc., à travers un procédé de haute technologie. Les sites gagnent de l'argent au clic et créent, via une régulation algorithmique, des chambres d'écho et des bulles de filtres où les internautes reçoivent les types d'informations qu'ils ont présélectionnés ou – plus inquiétant – celles dont les algorithmes estiment qu'ils ont envie de les connaître. C'est ainsi que les publicités politiques deviennent de plus en plus sur mesure et ciblées. Internet n'est pas une place publique

[10] Le terme « intermédiaires d'internet » désigne les opérateurs de plateformes médiatiques en ligne, de moteurs de recherche, de réseaux sociaux et de banques d'applis (van der Noll, Helberger et Kleinen-von Königslöw, 2015). D'après la Recommandation CM/Rec(2018)2 du Conseil de l'Europe sur les rôles et les responsabilités des intermédiaires d'internet, ces acteurs facilitent les interactions sur internet entre les personnes physiques et entre les personnes physiques et morales en exerçant des fonctions diverses et en proposant des services variés. Certains connectent les utilisateurs à l'internet, assurent le traitement d'informations et de données ou hébergent des services en ligne, y compris pour du contenu généré par les utilisateurs. D'autres agrègent des informations et permettent de faire des recherches ; ils donnent accès à des contenus et des services conçus ou gérés par des tiers, les hébergent et les indexent. Certains facilitent la vente de biens et de services, notamment de services audiovisuels, et rendent possibles d'autres transactions commerciales, y compris les paiements.

[11] https://www-cdn.law.stanford.edu/wp-content/uploads/2017/04/07_28.2_Persily-web.pdf

[12] Voir par exemple : https://www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/#372d73d92318

où résonnent de multiples voix ; c'est de plus en plus un lieu d'isolement où chacun se trouve coupé du reste de la population.

15. La « démocratisation » de la production de contenus et la centralisation des canaux de diffusion en ligne ont eu pour effet indésirable la prolifération des fausses informations et des tactiques de désinformation, publiques et privées. En effet, tout avènement d'un nouveau moyen de communication 1) élargit la diffusion des informations et les rend plus accessibles (liberté de communication), 2) entraîne un risque d'abus (contenus malveillants), 3) relance la censure, et 4) ouvre la voie à des manipulations de la part de puissants acteurs publics et privés.

16. Internet et les réseaux sociaux ont amplifié la communication de masse et le processus d'échange d'informations dans des proportions sans précédent depuis l'invention de l'imprimerie. Par conséquent, la diffusion de fausses informations et les tactiques de désinformation par des acteurs publics et privés ont connu ces dernières années un essor accompagné d'une sophistication technique croissante : « bots », propagandistes et sites spécialisés dans la désinformation exploitent les réseaux sociaux et les algorithmes de recherche pour s'assurer une forte visibilité et s'intégrer discrètement dans des contenus fiables, trompant de vastes cohortes de consommateurs d'actualités et – surtout – d'électeurs. Bien que le recours à la désinformation pour discréditer les opposants et multiplier ses soutiens politiques n'ait rien de nouveau, les technologies numériques en ont renforcé les effets néfastes, pour plusieurs raisons : les informations (y compris fausses) circulent très vite sur internet[13], l'architecture actuelle des moteurs de recherche et des réseaux sociaux facilite concrètement la désinformation, on manque d'outils (juridiques, sociaux et techniques) pour l'identifier et la stopper, et il s'avère difficile d'enquêter sur ces comportements en ligne et d'en poursuivre les auteurs.

17. Ces dernières années, les interventions étrangères dans des élections à travers les réseaux sociaux sont aussi devenues sources d'inquiétude pour les démocraties. Des ressources technologiques comme les campagnes de cyberespionnage à faible coût, les utilisateurs rémunérés ou les bots, les révélations sélectives ou la création d'informations fausses ont modifié les règles du jeu pendant les campagnes électorales. Elles ont aussi érodé la confiance envers les gouvernements démocratiques.

18. À l'échelle mondiale, les pratiques mentionnées ci-dessus – facilitées par les technologies numériques – pourraient menacer la démocratie et remettre en question la vision d'internet comme outil technologique au service d'une meilleure gouvernance démocratique.

19. L'existence des technologies numériques et leur application à presque tous les aspects de la vie, élections comprises, sont aujourd'hui un fait. La présente étude ne vise pas à en jauger les aspects positifs et négatifs, mais à examiner les difficultés que ces technologies soulèvent dans le domaine électoral. Elle insistera donc plus sur les problèmes soulevés par cette innovation, et sur les solutions envisageables, que sur ses avantages.

20. Le présent rapport ne prétend pas offrir de solutions concrètes et universelles à tous les problèmes que l'usage d'internet et des réseaux sociaux peut poser aux processus électoraux. Les particularités de chaque pays et de chaque démocratie rendraient une telle tâche impossible[14]. Son but est d'identifier les problèmes juridiques les plus prégnants suscités par l'usage de ces technologies, d'en décrire la logique et les pistes possibles pour les résoudre, de

[13] Certains résultats d'études montrent aujourd'hui que les utilisateurs sont plus susceptibles de partager des nouvelles lorsqu'elles sont fausses. En outre, d'après la plus vaste enquête consacrée à ce jour à ce phénomène dans les médias numériques, réalisée par le MIT, les fausses informations ont plus tendance à circuler sur les supports numériques. Il semble que les histoires vraies mettent environ six fois plus de temps à toucher le public que les histoires fausses (Vosoughi, Roy and Aral, 2018). D'après le rapport Edelman Trust Barometer 2018, près de 70 % des internautes dans le monde redoutent que les « fake news » ne soient employées comme une arme.

[14] Pour des exemples des différentes approches adoptées face à des problèmes similaires, voir le document de référence CDL-AD(2019)016.

pointer les lacunes identifiées à ce jour et de suggérer plusieurs principes et lignes directrices qui pourraient aider à adapter la démocratie et ses lois aux nouvelles réalités technologiques. En ce sens, la conclusion de ces travaux est plus proche d'une feuille de route, indiquant les principes de régulation et de coopération à suivre à l'avenir, que d'un manuel de résolution des problèmes.

21. Cette étude vient compléter les travaux précédents du Conseil de l'Europe sur ce thème, dont notamment le rapport de 2017 intitulé *Les désordres de l'information*[15] (ci-après : CdE 2017 : Les désordres de l'information) et l'*Étude relative à l'utilisation d'internet dans le cadre des campagnes électorales* (ci-après : CdE 2017 : Internet et campagnes électorales[16]).

III. Information et nouvelles technologies

22. Dans la société en ligne, la principale matière première est l'information, au niveau de la production, mais aussi dans les interactions sociales et la gouvernance. L'impact d'internet sur le monde réel est universel et touche même ceux qui ne l'ont jamais utilisé. Il affecte directement l'opinion publique en tous lieux et a déjà modifié nos façons de penser et d'agir. Il donne la parole à tous ceux qui souhaitent contribuer au débat public – de façon négative ou positive. Face à un enjeu majeur, il permet à de véritables « escouades de relations publiques » d'intervenir pour tenter d'inverser le cours des événements. Dans cette équation entre virtuel et physique, il arrive même que la fiction intervienne[17]. Des personnalités s'aperçoivent que leurs équivalents fictionnels sont encore plus influents que leur propre personne[18]. L'humour peut avoir un effet similaire : en ouvrant, par exemple, de faux comptes satiriques au nom de personnalités, les internautes modifient l'image de la personne imitée et finissent parfois par jeter le trouble dans le public et les médias[19].

23. L'information se transmet avant tout par l'image, laquelle, contrairement aux mots, est traitée automatiquement. En l'absence de culture écrite et de langage verbal, nous risquons d'être incapables de transformer les informations en connaissances et les images en jugements et en idées, pour devenir des récepteurs passifs submergés de couleurs, de formes, de séquences et de bruits de fond. Le risque est que nos capacités d'abstraction se diluent progressivement. De plus en plus, *homo sapiens*[20] devient un *homo videns*, créature qui regarde sans penser et voit sans comprendre. Même les textes écrits, positifs ou négatifs, qui entourent les images se muent eux-mêmes en images et, comme les autres informations, sont traités dans l'immédiat et non de manière réfléchie[21].

---

[15] Rapport du Conseil de l'Europe DGI(2017)09.
[16] Étude du Conseil de l'Europe DGI(2017)11.
[17] La stratégie de communication de Daesh montre clairement ce brouillage des limites entre fiction et réalité. En imitant sciemment les jeux vidéo et les blockbusters, ces communications attirent l'attention, humanisent l'image du terroriste et dépersonnalisent les victimes (Javier Lesaca, *Armas de seducción masiva*, Peninsula, Atalaya, 2017). Les médias classiques, quant à eux, ne montrent pas dans toute leur dureté les conséquences de sa barbarie.
[18] Le soutien à Kevin Spacey, ou à son incarnation du Président des États-Unis d'Amérique dans la série *House of Cards*, a suscité une forte polémique. Le catcheur Hulk Hogan est allé jusque devant la justice étasunienne et a finalement eu gain de cause du fait de la distinction entre les actes de son personnage de fiction, sur le ring et en dehors, et ceux de l'homme qui incarnait ce personnage.
[19] Les faux comptes abondent sur les différents sites de réseaux sociaux ; qu'ils affichent ou non leur caractère satirique, ils créent par l'humour un stéréotype de la personnalité qui les inspire. Certains finissent par avoir plus d'abonnés que le véritable compte de la personne parodiée. Parmi les exemples les plus connus en politique espagnole, citons @EspeonzaAguirre et @NanianoRajoy.
[20] Giovanni Sartori, *Homovidens*, Taurus, 1989.
[21] À cet égard, une célèbre réflexion d'E.M. Forster prend un éclairage nouveau : *« Les livres sont des faits à lire (et c'est ennuyeux, car cela prend beaucoup de temps) ; c'est la seule manière de savoir ce qu'ils contiennent. Quelques tribus sauvages les mangent, mais en Occident, la lecture est la seule technique connue ».*

24. Lorsque les informations se réduisent à de simples stimuli qui affectent leur destinataire[22], on réagit davantage à la persuasion, et moins à l'information. La domination de l'image rend également difficile d'expliquer des notions complexes nécessitant un certain degré d'abstraction. Les stimuli sont presque exclusivement audiovisuels ; ceux qui les reçoivent les présument vrais, et ne réagissent qu'aux images qui réussissent à les émouvoir. La teneur émotionnelle des rumeurs devient plus importante que les faits et provoque des réactions viscérales – haine ou calomnie, le plus souvent. Ce phénomène est de plus en plus mis à profit par les agences de relations publiques, rémunérées par les acteurs politiques pour utiliser les thèmes susceptibles de provoquer de telles réactions.

25. Le phénomène baptisé « fake news[23] » a fait parler de lui dans le sillage de l'élection présidentielle de 2016 aux États-Unis. L'expression recouvre plusieurs phénomènes distincts. Il s'agit, le plus souvent, de la combinaison d'éléments issus des actualités classiques avec des traits extérieurs au journalisme professionnel[24]. Les fake news sont caractéristiques de l'effondrement des actualités traditionnelles (bien que la désinformation, la mésinformation ou le sensationnalisme ne soient pas des nouveautés) et du chaos qui règne dans les communications sur les réseaux sociaux. Elles relancent la vieille bataille sur la définition de la vérité, et les forces politiques et financières mènent des guerres de propagande en utilisant les fake news comme arme principale.

26. La diffusion massive d'images a contribué décisivement au succès des « fake news », en donnant aux informations l'apparence de l'infaillibilité. La communication finit par se transformer en spectacle, récompensant les idées simples, les titres trompeurs et tout ce qui attire l'attention du lecteur (et le fait cliquer), au risque de devenir réductrice. La forme l'emporte sur le fond et les images sur les idées ; on aspire à des réponses simples, à un monde divisé entre noir et blanc, oui ou non, et qui exclut les nuances. La brièveté, l'importance de l'image et la facilité à partager les contenus, typiques des réseaux sociaux, favorisent toutes la diffusion de techniques qui déforment la réalité.

27. Aujourd'hui, l'attente de mises à jour et même de prédictions[25] constantes fait que l'information est élaborée dès l'événement, sans vérification ni réflexion. Cette dynamique récompense la rapidité aux dépens de la qualité et crée des cycles d'information qui, souvent, ne durent pas même 24 heures ; l'information est épuisée sans avoir eu le temps de paraître dans la presse écrite le lendemain. En outre, disponibilité et capacité de stockage infinie font que des déclarations peuvent être retrouvées en quelques secondes sur leur site internet d'origine des mois, voire des années plus tard. Les contradictions ainsi dévoilées font aussi l'objet d'une diffusion de masse et parfois de « fake news », lorsqu'elles sont sorties de leur contexte.

28. Sur chaque événement, des milliers d'analyses, d'opinions et de données s'accumulent chaotiquement sur les réseaux sociaux et se diffusent presque à l'infini, par capillarité, sur les différents terminaux auxquels les citoyens sont connectés. Or, cette surcharge d'informations entrave la communication, et certains faits passent inaperçus dans l'ombre de réalités plus simples et plus voyantes. Rétablir les faits ne constitue donc pas un moyen suffisant pour corriger les informations erronées.

---

[22] Tony Schwartz, *La respuesta emocional*, éd. Liderazgo democrático 2, Quito, 2001, p. 37.

[23] Le rapport du Conseil de l'Europe *Les désordres de l'information* (2017) s'abstient délibérément d'utiliser le terme « fake news », jugeant qu'il ne décrit pas le phénomène de pollution de l'information dans toute sa complexité et qu'il est devenu de plus en plus politisé.

[24] R.R. Mourao et C.T. Robertson : *Fake News as Discursive Integration : An Analysis of Sites that Publish False, Misleading, Hyperpartisan and Sensational Information*, paru en ligne le 13 janvier 2019.

[25] En Espagne, en particulier sur Wikipedia, la tendance actuelle est à évoquer la mort de personnes qui se trouvent en fait en bonne santé. Par exemple, une infirmière ayant contracté Ebola a été incinérée avant de ressusciter miraculeusement.

29. Les individus créent leur propre écosystème informationnel ou monde personnel, constitué d'éléments d'information circulant en boucle et qui n'ont besoin d'être cohérents ni avec les textes précédents, ni avec la réalité. Leur vision de ceux qui ne partagent pas le même écosystème informationnel est donc fortement déformée. Des sources d'information nouvelles et variées confortent les individus dans leurs positions et accentuent ainsi le biais de confirmation, c'est-à-dire la tendance à consulter et à croire avant tout ce qui coïncide avec nos propres idées. Les algorithmes utilisés par les outils de communication personnels et les réseaux sociaux détectent les préférences des utilisateurs et les affichent plus souvent, renforçant ainsi certaines connaissances et l'adhésion à certains thèmes. Ainsi, malgré la masse d'informations disponibles, la majorité d'entre elles ne sont pas consultées ou ne le sont que par des personnes qui les jugent d'avance douteuses. Les réalités fâcheuses ou indésirables sont parfois ignorées au profit de récits personnalisés. Les informations et leurs correctifs sont sélectionnés pour prouver qu'une opinion donnée est juste, et les autres fausses[26]. Cela peut même concerner les informations avérées, qui sont beaucoup plus partagées lorsqu'elles renforcent des idées antérieures que lorsqu'elles les remettent en question[27].

30. Les environnements sociaux déterminent aussi la manière dont les informations sont reçues, en particulier lorsqu'elles permettent aux personnes de s'identifier à un groupe et dissimulent ce qui pourrait nuire à la position du groupe ou ne pas coïncider avec elle. Le « suivisme », par exemple, s'explique par le besoin d'appartenance et la honte d'être différent. Les personnes tendent à se fier à l'opinion de la majorité, créant une chambre d'écho au sein de laquelle les opinions se renforcent mutuellement.

31. Ce biais de confirmation entraîne une fragmentation des bulles informationnelles[28] et crée des mondes d'information parallèles, au point qu'il devient difficile de trouver des espaces de débat communs. La sphère publique en vient à se réduire à une série de petits blocs très mobilisés et isolés les uns des autres. La communication et l'information sélectives, presque personnalisées, facilitées par la technologie et les réseaux sociaux créent des micro-communautés fonctionnant en vase clos, où l'impossibilité de connaître les autres et de se mettre à leur place favorise les positions les plus radicales et le manque de dialogue et fait obstacle à l'empathie[29]. Pris ensemble, ces deux phénomènes encouragent la polarisation et autorisent la création d'un système de valeurs unique, du moins au sein des groupes fermés qui finissent par faire taire et exclure les dissidents. Lorsque différents écosystèmes informationnels interagissent, c'est souvent pour se heurter, ce qui renforce encore cette polarisation ; en effet, chaque position radicale perd en crédibilité lorsqu'elle rencontre l'opinion contraire… et réagit en se réaffirmant[30].

32. La technologie affecte non seulement le mode de diffusion, mais aussi tout le processus communicationnel (collecte, archivage, organisation et diffusion des informations). Les citoyens ne se limitent pas à suivre les actualités, ils deviennent des acteurs majeurs du processus communicationnel. Ils créent leurs propres sources d'information – en l'absence des modérateurs et régulateurs traditionnels. L'abondance et la diversité des informations ainsi produites font perdre aux médias leur statut de références : ils ne font plus autorité. En outre, la confusion des sources et les erreurs commises par certains médias traditionnels en raison du caractère immédiat – déjà évoqué – du processus informationnel ont accéléré la

---

[26] C. Sunstein, A. Scala, W. Quattrociocchi : *Echo Chambers on Facebook. 2016*, disponible sur : https://ssrn.com/abstract=2795110 (consulté le 25 janvier 2018).
[27] Shin, Jieun, Thorson, Kjerstin : « Partisan Selective Sharing : The Biased Diffusion of Fact-Checking Messages on Social Media », *Journal of Communication*, vol. 67, 2017, disponible sur http://onlinelibrary.wiley.com/doi/10.1111/jcom.12284/full (consulté le 25 janvier 2018).
[28] Eli Parisier : *The filter bubble*, The Penguin Press, New York, 2011.
[29] C. R. Sunstein : « The law of group polarization », *Journal of political philosophy* 10, 175–195 (2002).
[30] https://www.buzzfeed.com/charliewarzel/2017-year-the-internet-destroyed-shared-reality (consulté le 25 janvier 2018)

perte de crédibilité des médias[31]. À cet égard, médias et individus se trouvent souvent logés à la même enseigne. Face aux contenus qui déferlent sur eux, ils se réfugient dans des espaces d'information personnels, réduits, gérables, sûrs et fiables, où dominent les relations avec leurs proches et leurs collègues et la répétition des mêmes idéologies.

33. En partageant des informations, les citoyens deviennent des protagonistes de la communication et remettent en cause l'intérêt des grands médias. De plus en plus de citoyens utilisent internet comme source d'information[32] et, ce faisant, ne distinguent pas les sources d'information originales, plus crédibles, des contenus provenant de leur famille et de leurs amis[33]. Ils sont 79 % à considérer ces contenus comme une source d'information crédible, suivie par les opinions d'experts universitaires (72 %), d'employés d'entreprises (60 %) et d'entreprises dont ils utilisent les services (59 %). En fin de liste, on trouve les informations émanant de journalistes (48 %), de directeurs d'entreprises (43 %), de personnalités connues en ligne (42 %) et de célébrités (29 %)[34].

34. Le poids conféré par les réseaux sociaux aux communications interpersonnelles a entraîné la création en masse de « bots », comptes anonymes, automatiques et parfois contrefaits qui agissent comme des individus en ligne et accroissent la diffusion massive de certaines informations, en vue de créer artificiellement des courants d'opinion publique et d'acceptation ou de rejet de personnes ou d'idées[35]. En donnant l'impression d'un large soutien, ils créent un effet d'entraînement : de plus en plus de personnes adhèrent aux idées soutenues par cette majorité apparente. Négligeant leur responsabilité personnelle, les individus adoptent un comportement grégaire et se soumettent à la volonté du collectif, s'imitent les uns les autres et refusent la contradiction. À force d'être martelée, la mésinformation, en particulier lorsqu'elle est relayée par les médias traditionnels, devient une « croyance », et ceux qui la nient courent le risque d'être exclus du groupe.

IV. Impact des réseaux sociaux et d'internet sur la démocratie et les processus électoraux

35. Grâce à internet, chacun peut désormais s'informer sur les élections et exprimer ses opinions, échanger avec les candidats et participer activement aux campagnes électorales[36]. Les réseaux sociaux en particulier, en tant que principal forum de débat politique, sont devenus des sources d'information politique[37]. Des études montrent que le flux croissant d'informations favorisé par les réseaux sociaux aiguise l'esprit critique des citoyens à l'égard des pouvoirs publics[38] et qu'il existe une forte corrélation positive (0,71) entre l'usage d'internet et des réseaux sociaux, d'une part, et le soutien à la démocratie comme forme de gouvernement souhaitable, d'autre part[39]. En outre, de nombreux auteurs avancent que l'usage généralisé d'internet et des

---

[31] Le président Trump a utilisé certaines de ces erreurs, réelles ou apparentes, pour décerner son propre « prix des fake news » : https://www.elconfidencial.com/mundo/2018-01-18/trump-fake-news-awards-noticias-falsas-premios_1508101 (consulté le 25 janvier 2018). Pour un exemple, voir : https://theintercept.com/2017/12/09/the-u-s-media-yesterday-suffered-its-most-humiliating-debacle-in-ages-now-refuses-all-transparency-over-what-happened (consulté le 25 janvier 2018).

[32] 46 % des citoyens de l'Union européenne ont suivi l'actualité sur les réseaux sociaux en 2016 : Reuters Institute, *Digital News Report 2016*, disponible sur http://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Digital%2520News%2520Report%25202016.pdf (consulté le 25 janvier 2018).

[33] D'après le rapport *I saw the news on Facebook* (Reuters Institute for the Study of Journalism, Université d'Oxford), plus de la moitié des Britanniques s'étaient informés sur les réseaux sociaux en 2017. Sur cette moitié, plus de 50 % ne se rappelaient pas la source d'information exacte.

[34] Edelman Trust Barometer 2016.

[35] http://agendapublica.elperiodico.com/desde-rusia-bots/

[36] CdE 2017 : Internet et campagnes électorales, p. 7.

[37] Democracy Reporting International 2017.

[38] Gainous et al. 2016.

[39] Basco 2018.

réseaux sociaux permet de mieux connaître les attentes des citoyens et facilite l'organisation de mouvements sociaux de grande ampleur[40].

36. Néanmoins, même si « internet peut constituer un outil démocratique […], son potentiel dans ce domaine est menacé […] [car] cette technologie qui facilite la parole permet aussi de censurer des informations, de surveiller les pratiques en ligne et d'orienter et manipuler subtilement les comportements[41] », menaçant l'authenticité du scrutin, l'équité de la compétition électorale et, à terme, la capacité à traduire la volonté du peuple en représentation institutionnelle et en décisions gouvernementales[42]. Il faut noter que les ingérences indues dans l'authenticité et la liberté du scrutin peuvent affecter non seulement la traduction de la volonté populaire en actions concrètes, mais aussi la protection des minorités, l'équilibre entre les droits de l'homme les plus fondamentaux et la possibilité de demander des comptes aux élus et aux partis politiques. Certes, de telles menaces existaient déjà, mais les méthodes plus élaborées rendues possibles par les technologies les ont renforcées.

37. Les flux continus d'informations qui circulent simultanément sur de multiples plateformes compliquent énormément le suivi des comportements et des ressources en période électorale. En outre, l'éparpillement et l'anonymat des créations de contenus gênent sérieusement l'identification des auteurs et l'attribution des responsabilités en cas de comportement illégal en ligne. Le recours croissant aux bots et aux trolls pour orienter les discussions sur les réseaux sociaux, ainsi que la diffusion massive de fausses informations, nuisent à l'équité des compétitions électorales et permettent à des acteurs extérieurs de manipuler le discours politique et les préférences des électeurs[43]. Quant aux algorithmes utilisés par les moteurs de recherche et les réseaux sociaux, ils peuvent favoriser une vision partielle, voire trompeuse de la vie politique et de la démocratie[44].

38. L'impact de l'environnement numérique sur les élections a été mis en lumière par les controverses autour du référendum sur le Brexit, au Royaume-Uni, et de l'élection présidentielle de 2016 aux États-Unis. Les règles en matière de publicité payante n'ont guère été appliquées ; les données personnelles d'électeurs ont été collectées et traitées à des fins électorales sans leur accord et sans base juridique ; la communication politique est passée par des plateformes de réseaux sociaux non réglementées, ne garantissant pas l'équité de la couverture médiatique. Tout cela a mis à mal les institutions et les principes établis de réglementation des communications en période électorale, comme la liberté d'association, les plafonds de dépenses et la réglementation de la publicité politique[45], et sapé la capacité de la réglementation actuelle à garantir l'équité des règles du jeu pour tous les candidats. Ces failles dans la communication électorale ont ouvert la voie à d'éventuelles pratiques de corruption.

39. La réorganisation des communications depuis l'avènement d'internet et les nouveaux modes de transmission des messages politiques ont permis à des informations inexactes d'être « diffusées aux électeurs potentiels à une échelle sans précédent sans qu'aucun contrôle ne soit exercé et sans qu'aucun démenti ne puisse être formulé»[46]. D'où certains *désordres de l'information*, qui peuvent revêtir trois formes différentes :

- la mésinformation, information fausse mais dont la diffusion n'est pas destinée à nuire ;
- la désinformation, information fausse délibérément diffusée pour nuire ;
- l'information malveillante, information authentique diffusée dans le but de nuire, souvent en rendant publiques des informations destinées à rester privées[47].

[40] Castells 2011 ; Metaxas et Mustafaraj 2012 ; Cohen et al. 2012 ; Union européenne 2015.
[41] Laidlaw 2015, p. 1.
[42] Cf. CdE 2017 : Internet et campagnes électorales, pp. 7-9. Voir aussi Tambini 2018, pp. 265-293.
[43] Quintana 2016 ; Fidler 2017.
[44] Van Dijck 2013 ; McChesney 2013.
[45] CdE 2017 : Internet et campagnes électorales, p. 13.
[46] CdE 2017 : Internet et campagnes électorales, p. 15.
[47] CdE 2017 : Les désordres de l'information.

40. Dans certains cas, la diffusion d'informations fausses est *stratégique* : elle a pour but de *peser sur l'issue des élections*. Des études montrent que les « cyberbataillons » actifs sur internet sont souvent des *équipes gouvernementales, militaires ou mises en place par des partis politiques* pour manipuler l'opinion publique via les réseaux sociaux. La *manipulation organisée des réseaux sociaux* a fait sa première apparition en 2010 ; en 2017, des manipulations de ce type étaient avérées dans 28 pays différents[48].

41. Les réseaux sociaux ne sont pas les seuls à permettre la manipulation des informations, avec ou sans l'intention d'orienter l'issue d'un scrutin en faveur de tel ou tel parti. C'est aussi le cas des moteurs de recherche. Il a récemment été montré que *la manipulation des résultats de requêtes par les fournisseurs de moteurs de recherche* pouvait faire basculer les choix de vote chez 20 % des électeurs indécis, voire plus dans certains groupes démographiques[49].

42. Il est arrivé que des organismes publics mobilisent des bataillons de « façonneurs d'opinion » pour répandre les points de vue du gouvernement et contrer les critiques sur les réseaux sociaux ; citons aussi le cas de Cambridge Analytica, entreprise visée par une enquête car elle aurait, à l'occasion de l'élection présidentielle de 2016 aux États-Unis et du référendum sur le Brexit, détourné et utilisé les données privées de 50 millions d'utilisateurs de Facebook[50]. Contrairement à la censure directe, comme les blocages de sites ou les arrestations de cybermilitants, la manipulation des contenus en ligne est difficile à détecter et plus difficile encore à stopper, compte tenu de sa dispersion et de l'énorme quantité de personnes et de bots qui y travaillent.

43. Comme les messages ciblés n'atteignent pas le grand public, mais uniquement certains groupes ou individus, et ne font l'objet d'aucun contrôle et d'aucun examen journalistique, candidats et partis politiques peuvent modifier leurs promesses en fonction des personnes, fragmentant leurs objectifs politiques en messages distincts (voire inconciliables). Des recherches montrent en effet une montée des campagnes numériques sur les sujets dits « clivants », c'est-à-dire très controversés mais susceptibles de mobiliser les électeurs (politique migratoire, protection sociale, mariage des personnes homosexuelles, etc.). De plus en plus, ce travail de ciblage cherche à optimiser les moyens de campagne disponibles, et se concentre donc sur les électeurs volatils ou indécis. Les personnes que les messages des partis ne ciblent pas se trouvent privées de tout un éventail de déclarations politiques ; cela crée des inégalités entre électeurs, incapables d'opérer leur choix sur la base des mêmes informations.

44. Enfin, dans le monde entier, des États et des acteurs privés peuvent utiliser les technologies numériques pour porter atteinte aux droits de l'homme ou même comme des armes, pour attaquer des pays et leurs institutions au moyen de logiciels malveillants, espions ou de rançon et autres programmes sophistiqués[51]. Ces méthodes de *cyberguerre* ont déjà été utilisées avec succès contre des projets et des systèmes publics ; citons par exemple l'attaque de Stuxnet contre l'installation nucléaire de Natanz (Iran[52]).

45. En plus d'être accessibles, populaires et très sophistiqués, les outils cybernétiques fonctionnent dans un environnement sans frontières. Or, ce qui a été créé légalement en vertu d'une législation nationale peut devenir illégal en vertu d'une autre, et inversement. En outre,

[48] Bradshaw et Howard, 2017. Voir aussi le rapport 2017 de Freedom House, selon lequel les tactiques de manipulation et de désinformation ont joué un rôle important dans les élections dans au moins 17 autres pays au cours de l'année en question. D'après le Centre de la sécurité des télécommunications (CSE) du gouvernement canadien, pour la seule année 2017, 13 % des pays organisant des élections fédérales ont vu leurs processus démocratiques ciblés par des hacktivistes, des cybercriminels et même des acteurs politiques publics ou privés, toujours dans l'intention de manipuler les informations pour retourner l'opinion publique, voire déstabiliser les institutions démocratiques.
[49] Epstein et Robertson, 2015.
[50] P. Mccausland et A. Schecter, 2018 ; BBC, 2018.
[51] Quintana 2016.
[52] Quintana 2016 ; Mecinas Montiel 2016, pp. 404, 418 et 419.

avec la montée de l'*informatique en cloud*, les informations en ligne sont devenues encore plus fragmentées, ce qui rend extrêmement difficile d'identifier leur origine et leurs auteurs. La cybercriminalité et les cybermenaces ignorent toutes les frontières nationales. Cette situation complique les enquêtes et les poursuites pénales ; d'où l'urgence d'aborder le phénomène d'un point de vue transnational[53].

46. Pour conclure, nous voyons aujourd'hui proliférer simultanément, à l'échelle mondiale, l'information et la pollution de l'information. Les services en ligne ont enrichi et diversifié les sources d'actualités ; ils aident les citoyens à s'informer et à prendre des décisions sur des thèmes essentiels en démocratie, dont le choix de leurs représentants. Au même moment, toutefois, une nouvelle ère de désordres de l'information déforme l'écosystème des communications au point de grever sérieusement les décisions des électeurs, trompés, manipulés et abreuvés de fausses nouvelles destinées à peser sur leur vote. Un tel environnement pourrait saper l'exercice du droit à des élections libres et menace gravement le fonctionnement des régimes démocratiques.

47. Les technologies numériques ont modifié la manière dont nos sociétés traduisent la volonté du peuple en suffrages et en représentation, et largement rebattu les cartes des campagnes électorales. Si internet favorise certains aspects de la compétition démocratique, il a aussi des effets néfastes. L'omniprésence des technologies numériques a fait basculer la scène du débat démocratique dans le monde virtuel, soulevant de nombreuses questions sur le poids de ces technologies dans les élections et sur la nécessité de surveiller et de réglementer les comportements en ligne. En outre, il devient impératif d'assurer une protection adéquate contre les actes de cyberguerre.

V. Normes et instruments pertinents au niveau européen et international

48. Les phénomènes évoqués plus haut portent atteinte à plusieurs droits fondamentaux protégés au niveau européen et mondial par plusieurs déclarations et conventions internationales, comme la Déclaration universelle des droits de l'homme, le Pacte international relatif aux droits civils et politiques, la Déclaration américaine des droits et devoirs de l'homme, la Convention américaine relative aux droits de l'homme, la Charte des droits fondamentaux de l'Union européenne ou la Convention européenne des droits de l'homme (ci-après : « CEDH »).

A. Droit à des élections libres et à la liberté d'expression

1. Principes fondamentaux

49. En vertu de la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme (ci-après : « Cour eur. DH »), les États membres du Conseil de l'Europe sont tenus de reconnaître à toute personne relevant de leur juridiction les droits et libertés définis dans la Convention. Le *droit à des élections libres* affirmé à l'article 3 du Protocole n° 1 à la CEDH n'est pas seulement un principe essentiel pour toute société démocratique, mais aussi un droit individuel fondamental dont tout citoyen doit pouvoir jouir, et celui qui favorise le mieux une « véritable démocratie»[54].

[53] Davara 2003 ; Salt 2017, pp. 520-521.
[54] Herdis Thorgeirsdóttir (2005), *Journalism Worthy of the Name : the Affirmative Side of Article 10 of the ECHR*, Kluwer Law International. Lécuyer, 2014. Voir *Mathieu-Mohin et Clerfayt c. Belgique*, requête n° 9267/81 (Cour eur. DH, 2 mars 1987) ; *Ždanoka c. Lettonie*, requête n° 58278/00 (Cour eur. DH, 16 mars 2006). Voir aussi Cour eur. DH, 2018 : « Guide sur l'article 3 du Protocole n° 1 à la Convention européenne des droits de l'homme – Droit à des élections libres », disponible sur https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_FRA.pdf

50. Le droit à des élections libres comprend le droit de voter et celui de se porter candidat à des élections[55]. Il emporte aussi pour les États membres l'obligation positive d'assurer les conditions voulues pour que les citoyens puissent librement former et exprimer leurs opinions et choisir leurs représentants. Cette obligation est de la plus haute importance pour la santé (bonne ou mauvaise) du contexte communicationnel du scrutin. Le droit à des élections libres oblige les États membres à « organiser, à des intervalles raisonnables, des élections libres au scrutin secret, dans les conditions qui assurent la libre expression de l'opinion du peuple sur le choix du corps législatif », ce qui indique que le droit à la liberté d'expression et celui à des élections libres ne peuvent aller l'un sans l'autre[56]. Cette interprétation a été confirmée par la Cour eur. DH, pour laquelle « des élections libres et la liberté d'expression, notamment la liberté du débat politique, constituent l'assise de tout régime démocratique» [57].

51. La Cour affirme en outre que ces deux droits sont interdépendants et se renforcent l'un l'autre, la liberté d'expression étant l'une des conditions nécessaires à des élections libres. Pour être effectifs, les droits garantis par l'article 3 du Protocole n° 1 doivent être protégés y compris en période de campagne électorale. C'est pourquoi, il est particulièrement important, avant des élections, de permettre aux opinions et aux informations de tous ordres de circuler librement[58]. D'après la Cour eur. DH, les États membres ont l'obligation positive d'assurer effectivement la liberté d'expression : ils sont tenus de créer un environnement favorable à la participation aux débats publics de toutes les personnes concernées, leur permettant d'exprimer sans crainte leurs opinions et idées. L'État ne doit pas seulement se garder de toute ingérence dans la liberté d'expression individuelle, il a aussi l'obligation positive de protéger le droit à la liberté d'expression contre les atteintes, y compris de la part de personnes privées[59].

52. La Cour reconnaît toutefois que dans certaines circonstances, les droits garantis par l'article 10 CEDH et par l'article 3 du Protocole n° 1 peuvent entrer en conflit et qu'il peut être jugé nécessaire, avant ou pendant une élection, de prévoir certaines restrictions à la liberté d'expression, alors qu'elles ne seraient habituellement pas admissibles, afin de garantir « la libre expression de l'opinion du peuple sur le choix du corps législatif» [60]. La Cour reconnaît que pour ménager un équilibre entre ces deux droits, les États membres disposent d'une marge d'appréciation, comme c'est généralement le cas s'agissant de l'organisation de leur système électoral. Dans le même temps, elle souligne que toute restriction à la liberté d'expression doit être proportionnée au but légitime poursuivi et nécessaire dans une société démocratique. La Cour précise, par exemple, que l'article 10 CEDH en tant que tel ne met pas obstacle à la discussion ou à la diffusion d'informations reçues, même en présence d'éléments donnant fortement à croire que les informations en question pourraient être fausses[61]. Par ailleurs, il faut souligner la décision de la Cour concernant le droit d'une ONG de diffuser des annonces politiques à la radio et à la télévision, où ont été mis en balance, d'une part, le droit de l'ONG requérante à communiquer des informations et des idées d'intérêt général que le public a le droit de recevoir et, d'autre part, le souci des autorités d'empêcher que le débat et le processus démocratiques ne soient faussés par des groupes financièrement puissants bénéficiant d'un

[55] *Mathieu-Mohin et Clerfayt c. Belgique* ; *Ždanoka c. Lettonie*.
[56] Plaizier, 2018.
[57] *Bowman c. Royaume-Uni*, requête n° 24839/94 (Cour eur. DH, 19 février 1998), par. 42.
[58] *Bowman c. Royaume-Uni*, requête n° 24839/94 (Cour eur. DH, 19 février 1998) ; *Orlovskaya Iskra c. Russie*, requête n° 42911/08 (Cour eur. DH, 21 février 2017). Lors des élections européennes de 2019, Facebook a autorisé le Parlement européen à publier des annonces politiques dans toute l'UE : https://www.politico.eu/article/facebook-allows-eu-wide-political-ads-for-european-parliament/ ; https://techcrunch.com/2019/04/26/facebook-says-its-open-to-advertising-u-turn-for-the-eu-elections-enabling-cross-border-campaigns/?renderMode=ie11.
[59] *Dink c. Turquie*, requêtes n° 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09 (Cour eur. DH, 14 septembre 2010).
[60] *Bowman c. Royaume-Uni*, requête n° 24839/94 (Cour eur. DH, 19 février 1998) ; *Orlovskaya Iskra c. Russie*, requête n° 42911/08 (Cour eur. DH, 21 février 2017).
[61] *Salov c. Ukraine*, requête n° 655118/01 (Cour eur. DH, 6 septembre 2005).

accès privilégié aux médias influents[62]. Dans son arrêt, la Cour reconnaît que de tels groupes peuvent s'assurer un avantage concurrentiel dans le domaine de la publicité payante et ainsi porter atteinte à la liberté et au pluralisme du débat, dont l'État demeure l'ultime garant. Ainsi, le risque de déséquilibre entre les forces politiques en lice doit être pris en compte pour conserver un débat libre et pluraliste.

53. Les droits affirmés à l'article 3 du Protocole n° 1 ne sont cependant pas absolus : il peut y avoir des « limitations implicites[63] », et les États membres jouissent à cet égard d'une grande marge d'appréciation. Lorsqu'elle examine le respect de l'article 3 du Protocole n° 1, la Cour se concentre principalement sur deux critères : l'existence ou non d'une mesure arbitraire ou disproportionnée, et la question de savoir si cette mesure a porté atteinte à la libre expression de l'opinion du peuple[64].

54. La Cour eur. DH a reconnu le droit individuel d'accéder à internet ; se prononçant contre le blocage total de contenus en ligne, elle affirme qu'« internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information : on y trouve des outils essentiels de participation aux activités et débats relatifs à des questions politiques ou d'intérêt public»[65] . Elle rappelle que l'article 10 CEDH garantit la liberté d'exprimer, de recevoir et de partager des informations et des idées sans considération de frontière. Le blocage de l'accès à des sites tiers ou hébergés en plus de ceux concernés par la procédure rend de nombreuses informations inaccessibles et restreint donc les droits des internautes. La Cour considère en outre qu'une restriction d'accès à une source d'information n'est compatible avec la Convention qu'en présence d'un cadre juridique strict, prévoyant une procédure de recours de nature judiciaire pour éviter les éventuels abus.

55. La Cour eur. DH considère en outre que « compte tenu de ce que les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la diffusion de l'information (*Delfi AS c. Estonie* [GC], n° 64569/09, § 133, CEDH 2015), la fonction des blogueurs et des utilisateurs populaires des médias sociaux peut aussi être assimilée à celle de « chien de garde public » en ce qui concerne la protection offerte par l'article 10» [66] . Cette protection peut s'étendre à l'accès aux informations (y compris détenues par les pouvoirs publics) s'il est essentiel à l'exercice du droit à la liberté d'expression : les informations demandées doivent relever de l'intérêt général. Cependant, comme évoqué plus haut, l'article 10 ne garantit pas une liberté d'expression illimitée ; des restrictions sont autorisées, par exemple pour protéger le droit à la vie privée (article 8 CEDH), à condition que les moyens employés soient proportionnés au but poursuivi.

56. Les principes fondamentaux relatifs aux élections sont en outre réunis dans le Code de bonne conduite en matière électorale, adopté en 2002 par la Commission de Venise[67]. Ce sont notamment :

- l'égalité des chances entre les partis et les candidats ;
- la neutralité des autorités publiques relativement à la campagne électorale, à la couverture par les médias et au financement public des partis et des campagnes ;

[62] *Animal Defenders International c. Royaume-Uni*, requête n° 48876/08 (CEDH, 2013).
[63] L'article 3 ne s'accompagne pas d'une liste de « buts légitimes » tels que ceux énumérés dans les articles 8 à 11 CEDH, et la Cour eur. DH ne lui applique pas les traditionnels critères de « nécessité » et de « besoin social impérieux » utilisés dans le contexte de ces articles.
[64] *Mathieu-Mohin et Clerfayt c. Belgique* ; *Ždanoka c. Lettonie*.
[65] *Ahmet Yıldırım c. Turquie*, requête n° 3111/10 (Cour eur. DH, 18 décembre 2012). Voir aussi *Cengiz et autres c. Turquie*, requêtes n° 48226/10 et 14027/11 (Cour eur. DH, 1er décembre 2015).
[66] *Magyar Helsinki Bizottság c. Hongrie*, requête n° 18030/11 (Cour eur. DH, 8 novembre 2016). Voir aussi *Animal Defenders International c. Royaume-Uni*, requête n° 48876/08 (Cour eur. DH, 2013).
[67] CDL-AD(2002)023rev-cor. Voir aussi les Lignes directrices conjointes visant à prévenir et à répondre à l'utilisation abusive de ressources administratives pendant les processus électoraux (CDL-AD(2016)004), qui réaffirment les principes de neutralité et d'égalité des chances dans l'accès aux médias du secteur public.

- l'égalité des chances peut être stricte ou proportionnelle, et porte notamment sur « le temps de parole à la radio et à la télévision » ;
- dans le respect de la liberté d'expression, la loi devrait prévoir que les médias audiovisuels privés assurent un accès minimal aux différents participants aux élections, en matière de campagne électorale et de publicité ;
- le financement des campagnes doit être transparent ;
- le principe de l'égalité des chances peut conduire à limiter les dépenses des partis, notamment dans le domaine de la publicité.

57. Le recours à des méthodes de vote électronique soulève des difficultés particulières au regard des principes fondamentaux en matière électorale. Le Conseil de l'Europe reste la seule organisation à avoir fixé des normes intergouvernementales dans le domaine du vote électronique. La Recommandation Rec(2004)11 du Comité des Ministres, qui a été utilisée dans les jurisprudences nationales d'États membres et même d'États non membres, ainsi que par d'autres acteurs internationaux pertinents, a été récemment mise à jour : une nouvelle recommandation – composée de l'actuelle Recommandation sur les normes relatives au vote électronique (CM/Rec(2017)5), de lignes directrices sur la mise en œuvre de ses dispositions et d'un exposé des motifs – est venue compléter la Rec(2004)11 et traite de l'aspect le plus sensible des technologies électorales, à savoir le vote électronique, défini comme l'utilisation de moyens électroniques pour enregistrer et/ou dépouiller les suffrages. Cette catégorie comprend des systèmes tels que les machines à voter à enregistrement électronique direct (EED), les scanners de bulletins, les stylos numériques et le vote par internet. Le but de la Recommandation est de veiller à ce que le vote électronique garantisse un suffrage universel, égal, libre et secret ; elle comprend des dispositions sur les exigences d'organisation, les moyens de rendre des comptes, la fiabilité et la sécurité du système.

58. À cet égard, il faut aussi tenir compte des documents pertinents de la Commission de Venise. Le Code de bonne conduite en matière électorale affirme clairement que « le vote électronique ne doit être admis que s'il est sûr et fiable ; en particulier, l'électeur doit pouvoir obtenir confirmation de son vote et le corriger, si nécessaire, dans le respect du secret du vote ; la transparence du système doit être garantie»[68].

2. Financement des campagnes électorales

59. Il existe une série de normes reconnues contre la corruption dans le financement des partis politiques et des campagnes électorales (qu'il est recommandé d'étendre aux entités liées à des partis, comme les fondations politiques). Elles sont énoncées dans la Recommandation 1516 (2001) de l'Assemblée parlementaire sur le financement des partis politiques, qui a été suivie de la Recommandation Rec(2003)4 du Comité des Ministres sur les règles communes contre la corruption dans le financement des partis politiques et des campagnes électorales. Les normes à appliquer sont notamment les suivantes : a) assurer un *équilibre raisonnable* entre les financements publics et privés des partis politiques ; b) octroyer les aides de l'État aux partis selon des *critères équitables* ; c) encadrer par des règles strictes les dons privés, notamment en *interdisant ou en limitant les contributions* de donateurs étrangers et d'organisations religieuses et en limitant les dons d'entreprises et les dons anonymes ; d) *plafonner les dépenses des partis* relatives aux campagnes électorales ; e) prévoir la *transparence* sur les dépenses des partis politiques et sur leurs sources de financement, et f) mettre en place un *organisme indépendant* et des *sanctions* appropriées pour ceux qui contreviennent aux règles.

[68] Code de bonne conduite en matière électorale, CDL-AD(2002)023rev-cor, chapitre I.3.2.iv. ; voir aussi les paragraphes 42 à 44 du rapport explicatif. Voir aussi le Rapport de la Commission de Venise sur la compatibilité du vote à distance et du vote électronique avec les standards du Conseil de l'Europe, CDL-AD(2004)12.

60. De même, dans leurs Lignes directrices sur la réglementation des partis politiques[69], la Commission de Venise et l'OSCE/BIDDH affirment que la réglementation des campagnes électorales devrait :

- prévenir les influences indues exercées sur les décisions politiques au moyen de soutiens financiers (et assurer l'indépendance des partis) ;
- prévoir la transparence sur les dépenses des partis politiques, et
- veiller à ce que tous les partis puissent se mesurer conformément au principe de l'égalité des chances.

61. Afin d'atteindre ces objectifs, « c'est surtout dans la législation électorale que la communication de campagne a été réglementée, par un plafonnement des dépenses et le contrôle du financement des campagnes ; des aides publiques à la communication électorale ; un arrêt de la communication de campagne juste avant le scrutin ; une réglementation des médias, notamment l'octroi de licences de diffusion ; des règles applicables à la publicité politique (impartialité, financement public et temps d'antenne gratuit) ; l'autorégulation et le code de déontologie de la presse» [70].

62. Les normes en vigueur sont exigeantes, afin de « protéger l'intégrité des élections, de veiller à ce qu'elles soient libres et équitables et d'empêcher qu'elles soient captées au service d'un petit nombre d'intérêts[71] ». Cependant, les mesures législatives adoptées par les États membres et les règles mises en œuvre se sont concentrées sur le contexte hors ligne[72]. Par conséquent, elles se sont avérées *très peu applicables et efficaces à l'heure de la publicité politique numérique*. Comme déjà évoqué, les décideurs politiques, les gouvernements et la société tout entière ont rencontré ces dernières années *des difficultés à faire respecter sur internet la réglementation en vigueur*, et les règles en matière électorale ne font pas exception.

63. En effet, le plafonnement des dépenses de campagne imposé par la législation a été mis à mal par de nouvelles formes de publicité numérique qui sont par nature moins transparentes que les plus anciennes, rendant obsolètes les définitions et les limites associées à tel ou tel type de média. Les garanties anti-corruption, fondées sur des méthodes spécifiques de calcul des dépenses et sur des déclarations de dépenses ventilées par type de média traditionnel, perdent de leur sens à mesure que les campagnes politiques basculent sur internet. En conséquence, même les plafonds absolus de dépenses médiatiques deviennent moins pertinents, et les règles de transparence visant à ce que les citoyens connaissent les montants et les modes de financement des campagnes deviennent difficiles, voire impossibles à mettre en œuvre dans le monde numérique, qui ne connaît pas de frontières[73].

3. Discours politique et couverture médiatique des campagnes électorales

64. Bien que la liberté d'expression soit la sève de la démocratie, tous les systèmes juridiques prévoient aujourd'hui une réglementation et un encadrement du financement des campagnes et des obligations de transparence. Dans la sphère individuelle, il se peut que la liberté d'expression mérite d'être protégée indépendamment de la teneur des messages ; mais cela ne vaut pas pour une campagne politique. La grande majorité des régimes constitutionnels, sinon tous, prévoient des limites à la liberté d'expression en période de campagne électorale : période de silence, cordon sanitaire autour des bureaux de vote, règles de financement des campagnes et obligations de transparence, par exemple. Toutes les restrictions applicables aux campagnes, même celles qui visent la transparence, sont à voir avant tout comme des ingérences qui doivent

[69] CDL-AD(2010)024, p. 40, par. 159.
[70] CdE 2017 : Internet et campagnes électorales, p. 9.
[71] CdE 2017 : Internet et campagnes électorales, p. 9.
[72] Dans ce contexte, le recours aux campagnes de financement participatif, principalement sur internet, contribue de plus en plus à modifier les moyens de financement des campagnes électorales.
[73] CdE 2017 : Internet et campagnes électorales, pp. 20-21.

être justifiées, dans les régimes européens, par des critères de nécessité et de proportionnalité. En principe, l'encadrement de la publication d'annonces politiques semble juridiquement possible, et peut prendre la forme a) d'une réglementation sur la transparence plutôt que sur le contenu, b) d'une réglementation des campagnes politiques et c) d'une réglementation applicable au scrutin, ou liée aux mécanismes de financement, ou destinée à identifier les origines extérieures au milieu politique. Malgré la difficulté à définir certains concepts, il est clairement possible de concevoir un régime applicable à la presse traditionnelle, à la télévision, à la radio ou à l'affichage. Mais dans le monde numérique, qu'est-ce qu'une publication est qui en est l'auteur ? Quand un message cesse-t-il d'être l'expression individuelle d'une opinion devenue « virale » pour se transformer en « publicité » ?

65. La Cour européenne des droits de l'homme a clairement pointé la responsabilité de l'État dans la prévention des inégalités de couverture médiatique en période électorale[74], en ligne et hors ligne, avec toutefois d'importantes différences dues à l'*influence* respective des médias traditionnels et des nouveaux médias[75]. L'enjeu consiste aujourd'hui à définir précisément ces différences – pour déterminer s'il s'est produit *un transfert d'influence suffisamment important*[76]. Il s'avère crucial d'estimer l'ampleur de ce « transfert » pour déterminer si la responsabilité positive qu'a l'État d'assurer aux candidats et aux partis une exposition égale doit s'appliquer aux nouveaux intermédiaires de l'information et si oui, de quelle manière.

66. Les normes et autres instruments du Conseil de l'Europe dans ce domaine visent à créer un *contexte de communication favorable à l'exercice du droit à des élections libres*. Elles reflètent l'obligation positive qu'a l'État de veiller à ce que ses citoyens reçoivent les informations fiables dont ils ont besoin sur les partis politiques afin de choisir démocratiquement leurs représentants.

67. La Recommandation CM/Rec(2007)15[77] s'applique à un large éventail de médias, indépendamment des moyens et des technologies utilisés pour diffuser leurs contenus ; elle offre des lignes directrices en vue d'une couverture libre et indépendante des campagnes politiques, avec des normes renforcées pour les médias de service public. La Recommandation comporte plusieurs lignes directrices visant à assurer une couverture responsable, exacte et équitable des campagnes électorales ; cependant, les médias de service public ont pour responsabilité particulière de couvrir les élections « de manière équitable, équilibrée et impartiale, sans discriminer ou soutenir un parti politique ou un candidat particulier ». Concernant les possibilités générales ouvertes aux candidats et aux partis politiques pour s'adresser à l'électorat, la Recommandation laisse à la discrétion de chaque État membre l'autorisation ou l'interdiction de la publicité politique payante. Cependant, lorsque des partis ont la possibilité d'acheter des espaces publicitaires à des fins de campagne électorale, ils doivent pouvoir le faire dans des conditions et à des tarifs égaux.

68. En outre, la Recommandation énonce quelques règles générales à observer pour assurer des campagnes équitables et transparentes ; par exemple, les candidats et/ou les partis devraient disposer d'un *droit de réponse*, ou de recours équivalents, pour pouvoir réagir aux déclarations susceptibles de leur porter préjudice pendant la durée relativement brève d'une campagne électorale. Les modalités de diffusion des sondages d'opinion devraient donner au public des informations suffisantes pour juger de la valeur de ces sondages, et face à l'impact potentiel des messages électoraux juste avant le scrutin, une disposition prévoit que les États membres envisagent d'en interdire la diffusion la veille du vote (« jour de réflexion »). Par ailleurs, la Recommandation énonce des *critères de transparence* sur la publicité politique payante et sur les *propriétaires* des médias (critères détaillés par la Recommandation CM/Rec(2018)1[78]). Ces

[74] *Parti communiste de Russie et autres c. Russie*, requête n° 29400/05 (Cour eur. DH, 19 juin 2012).
[75] *Animal Defenders International c. Royaume-Uni*, requête n° 48876/08 (Cour eur. DH, 22 avril 2013).
[76] *Ibid.,* par. 119.
[77] Recommandation CM/Rec(2007)15 du Comité des Ministres aux États membres sur des mesures concernant la couverture des campagnes électorales par les médias.
[78] Recommandation CM/Rec(2018)1 sur le pluralisme des médias et la transparence de leur propriété.

lignes directrices visent avant tout les services audiovisuels linéaires (des médias privés comme publics), mais s'étendent aux services non linéaires des médias publics. Cependant, le basculement des campagnes politiques vers les réseaux sociaux en ligne ces dix dernières années en a réduit la pertinence.

69. Ce basculement se reflète dans la Recommandation CM/Rec(2018)1, qui affirme clairement que le contrôle des plateformes en ligne sur le flux, la disponibilité, la facilité de recherche et l'accessibilité des informations pourrait s'avérer délétère pour le *pluralisme des médias*. L'exposition sélective aux contenus médiatiques et la fragmentation qu'elle peut entraîner sont identifiées comme particulièrement inquiétantes, en particulier en période électorale. Par conséquent, la Recommandation appelle les États à assumer leurs obligations positives et, en tant que garants en dernier ressort du pluralisme, à *assurer le pluralisme dans la totalité de l'écosystème multimédia*.

70. Cette interprétation est renforcée par la Recommandation CM/Rec(2018)2[79], qui traite du rôle des intermédiaires d'internet et de leurs responsabilités à l'égard de leurs utilisateurs et des États membres, compte tenu de leur pouvoir croissant sur les communications et sur la diffusion des informations. Il convient de placer dans ce contexte l'éventuelle coresponsabilité des intermédiaires à l'égard des contenus qu'ils stockent, s'ils n'agissent pas avec la diligence voulue pour restreindre l'accès aux contenus ou aux services dès qu'ils ont connaissance de leur caractère illégal (conformément aux principes de légalité, de nécessité et de proportionnalité). En revanche, les intermédiaires ne devraient pas être tenus de surveiller tous les contenus auxquels ils donnent simplement accès, qu'ils transmettent ou qu'ils stockent. Sur ce point, rappelons que la Recommandation CM/Rec(2016)1 appelle les États membres à sauvegarder le principe de la neutralité du réseau dans leurs cadres de politique générale, afin de protéger la liberté d'expression, le droit d'accès aux informations et le droit à la vie privée[80].

71. Dans sa Déclaration Decl(13/02/2019)1 du 13 février 2019[81] sur les capacités de manipulation des processus algorithmiques, le Comité des Ministres souligne « la nécessité d'évaluer les cadres réglementaires relatifs à la communication politique et aux processus électoraux pour préserver l'équité et l'intégrité des élections aussi bien en ligne que hors ligne, conformément aux principes établis. En particulier, il conviendrait de veiller à ce que les électeurs aient accès à des niveaux d'information comparables pour l'ensemble du spectre politique, à ce qu'ils aient conscience des dangers du *redlining* politique, qui se produit lorsque les campagnes politiques se limitent aux personnes les plus influençables, et à ce qu'ils soient protégés de manière efficace contre les pratiques déloyales et la manipulation ».

72. L'Assemblée parlementaire, dans sa Résolution 2254 (2019) sur la liberté des médias en tant que condition pour des élections démocratiques[82], appelle les États membres à mettre en œuvre des stratégies afin de protéger le processus électoral de la manipulation de l'information et de la propagande indue à travers les réseaux sociaux. Elle propose des mesures telles que le développement de cadres de régulation spécifiques concernant les contenus internet en période électorale, ou l'établissement d'une responsabilité juridique claire pour les sociétés de réseaux sociaux qui publient des contenus illégaux préjudiciables aux candidats – tout en évitant les mesures extrêmes, comme le blocage de sites web entiers. L'Assemblée parlementaire invite en outre les organismes du secteur des médias à développer des cadres d'autorégulation affirmant des normes professionnelles et éthiques concernant leur couverture des campagnes électorales, et les intermédiaires d'internet à coopérer avec la société civile et avec des organisations de

[79] Recommandation CM/Rec(2018)2 sur les rôles et les responsabilités des intermédiaires d'internet.
[80] Recommandation CM/Rec(2016)1 sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau.
[81] Déclaration Decl(13/02/2019)1 sur les capacités de manipulation des processus algorithmiques, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4c
[82] Résolution 2254 (2019) sur la liberté des médias en tant que condition pour des élections démocratiques, http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-FR.asp?FileID=25409&lang=FR

toute tendance politique spécialisées dans la vérification des contenus pour s'assurer que toute information est confirmée par une source tierce qui fait autorité.

B. Droit à la vie privée et à la protection des données personnelles

73. L'article 8 CEDH protège le droit à la vie privée. Sur cette base, la Cour eur. DH a livré une abondante jurisprudence en matière de protection des données personnelles[83].

74. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108, 1981) énonce des principes et des règles concernant le traitement des données personnelles, ainsi que les droits des individus. Le Protocole additionnel à cette Convention, adopté en 2011, fixe les normes applicables à l'établissement d'autorités de contrôle chargées de veiller à la protection des données. Par rapport au Règlement général sur la protection des données de l'Union européenne, ce cadre juridique présente l'intérêt d'être ouvert à tous les pays du monde, permettant à différents ordres juridiques d'adhérer aux mêmes normes et favorisant par là leur harmonisation[84].

75. Le 10 octobre 2018, un nouveau Protocole modernisant la Convention (ci-après : « Convention 108 modernisée ») a été signé par 21 Parties à la Convention. L'article 5 de la Convention 108 modernisée renforce les principes de protection des données en prévoyant que les données sont traitées loyalement et de manière transparente, collectées pour des finalités explicites, déterminées et légitimes et non traitées de manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins de statistiques étant compatible avec ces fins, à condition que des garanties complémentaires s'appliquent. La Convention 108 modernisée prévoit en outre des principes et des exigences supplémentaires comme la prise en compte de la vie privée dès la phase de conception d'un service, l'examen de l'impact sur les données personnelles et le respect de la vie privée par défaut, ainsi que l'obligation de signaler toute atteinte aux données aux autorités de protection des données, au minimum. Elle instaure des garanties nouvelles, en particulier compte tenu de l'omniprésence des technologies de l'information dans le traitement des données, et distingue de nouvelles catégories de données sensibles. Ces garanties supplémentaires s'appliquent en particulier au traitement des données sensibles, telles que les opinions politiques. La Convention 108 modernisée comporte des dispositions plus détaillées sur les flux transfrontières de données, sur les compétences des autorités de contrôle – élargies par rapport à la version précédente – et sur le mécanisme de suivi.

76. En outre, un grand nombre d'instruments juridiques du Conseil de l'Europe traite de la protection des données personnelles dans le cadre du fonctionnement des réseaux sociaux.

77. Dès 1999, la Recommandation R(99)5 du Comité des Ministres, sur la protection de la vie privée sur internet, comportait des Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes ». La Recommandation CM/Rec(2010)13 de 2010, sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, énonce les conditions devant régir le profilage et livre une liste détaillée des informations à fournir aux personnes concernées. Elle note que le manque de transparence, voire l'« invisibilité » du profilage et le manque de précision qui peut découler de l'application automatique de règles d'inférence préétablies risquent de faire peser de graves menaces sur les droits et libertés de

[83] *Case law of the ECtHR concerning the protection of personal data*, disponible sur : https://rm.coe.int/case-law-on-data-protection/1680766992. Voir aussi Cour eur. DH, 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 sur : https://www.echr.coe.int/Documents/Guide_Art_8_FRA.pdf.

[84] Cela concerne à la fois des pays non européens (Cap Vert, Maurice, Mexique, Sénégal, Tunisie et Uruguay) et européens (comme l'Albanie, la Russie, la Serbie, la Turquie ou l'Ukraine).

l'individu. Bien qu'initialement considéré comme une technique commerciale et de marketing, le profilage s'applique aussi, comme les événements récents l'ont montré, aux processus électoraux.

78. La Résolution n° 3 des Ministres de la Justice sur la protection des données et la vie privée au troisième millénaire, adoptée en 2010 (MJU-30 (2010) RESOL), note que l'usage généralisé des technologies de l'information et de la communication (TIC), en permettant d'observer, de conserver et d'analyser la plupart des activités humaines du quotidien, pourrait générer le sentiment d'être en permanence observé et donc affaiblir le libre exercice des droits de l'homme et des libertés fondamentales, à moins que des normes efficaces en matière de protection des données ne soient mondialement appliquées de manière effective. La Résolution 1843 (2011) de l'Assemblée parlementaire sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne (2011) souligne que la protection de la vie privée est un élément nécessaire de la vie humaine et du fonctionnement humain d'une société démocratique, et que toute violation de la vie privée d'une personne met en jeu sa dignité, sa liberté et sa sécurité.

79. La Recommandation CM/Rec(2012)3 du Comité des Ministres sur la protection des droits de l'homme dans le contexte des moteurs de recherche (2012) note que l'historique des recherches d'un individu contient une empreinte qui peut révéler ses convictions, ses centres d'intérêt, ses relations ou ses intentions, et peut dévoiler entre autres ses opinions politiques ou ses convictions religieuses ou autres. Elle appelle à appliquer des principes de protection des données, dont notamment l'encadrement des finalités, une collecte de données minimisée et des limites à la conservation des données, et à veiller à ce que les intéressés soient informés du traitement et reçoivent toutes les informations pertinentes.

80. La Recommandation CM/Rec(2012)4 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux note l'importance croissante des services de réseaux sociaux et d'autres médias sociaux, qui offrent de grandes possibilités de renforcement de la participation des individus à la vie politique, sociale et culturelle. Elle préconise des actions visant à offrir aux utilisateurs de réseaux sociaux un environnement qui leur permette de continuer à exercer leurs droits et leurs libertés, à sensibiliser les utilisateurs aux éventuelles atteintes à leurs droits fondamentaux et aux moyens d'éviter d'avoir un impact négatif sur les droits d'autrui lorsqu'ils utilisent ces services, à renforcer la transparence quant au traitement des données et à interdire tout traitement illégitime des données à caractère personnel. Ces actions peuvent être menées en coopération avec les prestataires de réseaux sociaux. La Recommandation souligne également que les utilisateurs devraient être informés du réemploi de leurs données personnelles à des fins de profilage.

81. La Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux (2013) souligne que les États membres n'ont pas seulement des obligations négatives – s'abstenir de toute atteinte aux droits fondamentaux –, mais aussi des obligations positives, c'est-à-dire qu'ils doivent protéger activement ces droits, ce qui englobe la protection des personnes contre les faits commis par des acteurs non étatiques. L'omniprésence des différents appareils et les informations récoltées via ces appareils permettent de localiser et de surveiller leurs utilisateurs, jusqu'à révéler des informations personnelles délicates ou sensibles (dont les préférences politiques ou religieuses) qui peuvent être compilées pour établir un profil intime et détaillé de chaque utilisateur.

82. La Recommandation CM/Rec(2014)6 du Comité des Ministres (2014) comporte un Guide des droits de l'homme pour les utilisateurs d'internet, et en 2017, le Comité de la Convention STE 108 a adopté des Lignes directrices sur la protection des données à caractère personnel à l'ère des mégadonnées. Dans sa Déclaration Decl(13/02/2019)1 du 13 février 2019 sur les capacités de manipulation des processus algorithmiques, le Comité des Ministres encourage les États membres à étudier « la nécessité de cadres protecteurs supplémentaires relatifs aux

données, qui dépassent les principes actuels de la protection des données à caractère personnel et de la vie privée et visent à lutter contre les effets significatifs de l'utilisation ciblée des données sur les sociétés et, plus généralement, sur l'exercice des droits de l'homme ».

83. Enfin, le Conseil de l'Europe a produit ou commandé plusieurs rapports et études dans ce domaine, notamment *The use of the Internet & related services, private life & data protection : trends & technologies, threats & implications*[85]. Ce rapport appelle à affirmer et à protéger le droit à l'anonymat sur internet, à réglementer et à encadrer strictement le profilage et ses utilisations dans tous types de contextes, et invite le Conseil de l'Europe à adopter des lignes directrices sur les restrictions à appliquer aux technologies de surveillance, y compris au commerce international de ces technologies.

C. Protection contre la cybercriminalité

84. La Convention du Conseil de l'Europe sur la cybercriminalité, STE 185 (2001) (« Convention de Budapest ») couvre deux types de menaces contre la démocratie électorale[86]. Ce sont premièrement les attaques contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques relatifs aux élections, qui constituent des formes de cybercriminalité : accès illégal à des systèmes informatiques (article 2), interception illégale (article 3), atteinte à l'intégrité des données et des systèmes (articles 4 et 5), etc. Et deuxièmement, les opérations de désinformation, qui violent les règles concernant la protection des données personnelles, le financement de la vie politique, la couverture médiatique ou les communications relatives aux élections, c'est-à-dire les règles qui garantissent des élections libres, équitables et régulières.

85. Bien que ce deuxième type de menace ne relève pas en soi de la cybercriminalité, les preuves d'atteintes aux règles électorales prennent souvent la forme de preuves électroniques. Il est essentiel, par conséquent, que les États dotent leurs autorités de justice pénale des pouvoirs nécessaires pour recueillir de telles preuves. Les Parties à la Convention de Budapest sont tenues de le faire en vertu des articles 16 à 21, consacrés aux mesures procédurales comme la conservation rapide de données, la perquisition et la saisie de systèmes et de données informatiques, les injonctions de produire, etc.

86. Problème majeur, les données – et donc les preuves électroniques – sont évanescentes et souvent détenues par des prestataires de services étrangers, ou conservées sur des territoires multiples, changeants ou inconnus – « quelque part sur des serveurs dans le cloud[87] ». Trouver l'auteur d'une attaque, ou simplement identifier l'utilisateur d'une adresse IP (Internet Protocol), le propriétaire d'un réseau social ou celui d'un compte de courriel n'est souvent pas possible au moyen d'efforts raisonnables. C'est l'une des raisons pour lesquelles la cybercriminalité et les autres cybermenaces contre la démocratie électorale sont rarement poursuivies.

87. Il est indispensable de coopérer effectivement au niveau international et de travailler avec les prestataires de services. Sous sa forme actuelle, la Convention de Budapest comprend des dispositions détaillées en matière de coopération internationale, associant des mesures provisoires urgentes pour préserver les données (article 29, Conservation rapide de données

[85] « Utilisation d'internet et des services afférents, vie privée et protection des données : tendances et technologies, menaces et implications », Korff, 2013, disponible sur http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168067f7f4 (en anglais uniquement).

[86] Les informations qui suivent reposent sur une présentation d'Alexander Seger (Secrétaire exécutif du Comité de la Convention sur la cybercriminalité, Conseil de l'Europe) lors de la 15e Conférence européenne des administrations électorales (Oslo, Norvège, 19 et 20 avril 2018).

[87] Pour des informations détaillées, voir les rapports du Groupe de travail sur les preuves dans le cloud du Comité de la Convention sur la cybercriminalité, https://www.coe.int/fr/web/cybercrime/ceg (dernière consultation : 30 septembre 2018).

informatiques stockées ; article 35, Réseau 24/7) à des dispositions sur l'entraide judiciaire. Ces dispositions sont largement utilisées dans les enquêtes sur la cybercriminalité.

88. Cependant, elles ne couvrent suffisamment ni le cloud et les problèmes de compétence territoriale qu'il entraîne, ni le fait que des entreprises situées dans un État offrent leurs services dans de nombreux autres sans y être juridiquement ou physiquement présentes et sans devoir y rendre de comptes.

89. C'est pourquoi, les Parties à la Convention de Budapest ont ouvert des négociations sur un 2e Protocole additionnel, afin d'élargir les possibilités de coopération internationale et d'accès aux données dans le cloud. Les solutions envisagées comprennent la coopération directe avec des prestataires de services dans d'autres Parties, l'élargissement des perquisitions aux systèmes informatiques d'autres pays dans certaines circonstances limitées, ou l'entraide judiciaire urgente. Les négociations devraient se poursuivre jusqu'à fin 2019[88].

VI. Autres législations, jurisprudences et initiatives internationales et nationales[89]

A. Niveau international

90. Au niveau de l'ONU, la Déclaration commune du 1er juin 2011[90] sur la liberté d'expression et internet relève que les approches réglementaires mises au point pour d'autres moyens de communication – comme les services téléphoniques, la radio ou la télévision – sont très différentes de celles nécessaires sur internet, qui appelle des méthodes sur mesure. Dans sa version actualisée (3 mars 2017), cette déclaration évoque désormais les « fake news », la désinformation et la propagande et souligne la nécessité de donner la priorité à la liberté d'expression, affirmant que les interdictions de diffusion d'informations fondées sur des notions vagues et ambiguës comme les « fausses nouvelles » ou le « manque d'objectivité » sont incompatibles avec les normes internationales en matière de restrictions à la liberté d'expression, telles qu'énoncées au paragraphe 1 a), et devraient être supprimées[91].

91. La prise de conscience croissante de la nécessité d'éviter les fausses nouvelles et leur propagation, en particulier en période de campagne électorale, a suscité de multiples initiatives – recherche, éducation et coopération, solutions réglementaires et d'autorégulation, y compris au niveau international. L'OTAN a mis en place un Centre d'excellence en communication stratégique, laboratoire d'idées centré sur la maîtrise des informations en ligne et sur la cyberdéfense. En 2017 est né le Centre européen de lutte contre les menaces hybrides, fruit d'une coopération sur ce sujet entre l'UE et l'OTAN[92].

92. Il existe plusieurs réseaux de personnes œuvrant ensemble à vérifier la véracité des informations en ligne : par exemple l'International Fact-Checking Network (IFCN), unité du Poynter Institute réunissant des personnes du monde entier autour de la vérification des faits.

---

[88] Voir https://www.coe.int/fr/web/cybercrime/t-cy-drafting-group.
[89] Le présent rapport n'offre pas de description exhaustive des situations nationales. Voir aussi CDL-AD(2019)016.
[90] Déclaration signée le 1er juin 2011 par le Rapporteur spécial des Nations Unies sur le droit à la liberté d'opinion et d'expression, la Représentante de l'OSCE pour la liberté des médias, la Rapporteure spéciale de l'OEA sur la liberté d'expression et la Rapporteure spéciale de la CADHP sur la liberté d'expression et l'accès à l'information.
[91] Les États ne peuvent restreindre le droit à la liberté d'expression qu'en respectant les conditions de telles restrictions en droit international : elles doivent être prévues par la loi, servir l'un des intérêts légitimes reconnus en droit international et être nécessaires et proportionnées pour protéger cet intérêt.
[92] Voir aussi le guide pratique sur l'usage des réseaux sociaux en période électorale, élaboré par l'Institut international pour la démocratie et l'assistance électorale (International IDEA) à l'attention des administrations électorales : Seema Shah, *Guidelines for the Development of a Social Media Code of Conduct for Elections*, International IDEA, 2015. Guide disponible sur : https://www.idea.int/sites/default/files/publications/social-media-guide-for-electoral-management-bodies.pdf.

L'IFCN a été créé en 2015 pour soutenir et étudier les travaux de 64 organisations de vérification de faits réparties dans le monde entier.

B. Union européenne

93. En janvier 2018, la Commission européenne a mis en place un groupe d'experts à haut niveau (« GEHN ») chargé de préconiser des initiatives politiques pour lutter contre les « fake news » et la désinformation en ligne. Dans son rapport final[93], le GEHN plaide pour une approche pluridimensionnelle, poursuivant cinq grands objectifs :

1) renforcer la transparence des actualités en ligne ;
2) promouvoir la maîtrise des médias et de l'information afin de contrer la désinformation ;
3) élaborer des outils pour permettre aux utilisateurs et aux journalistes de dénoncer la désinformation ;
4) préserver la diversité et la pérennité de l'écosystème européen des médias d'actualité ;
5) promouvoir la poursuite des recherches sur l'impact de la désinformation en Europe.

94. Sur la base des constats du GEHN, la Commission européenne a publié en avril 2018 une Communication exposant sa stratégie de lutte contre le problème de la désinformation en ligne[94]. Cette stratégie ne prévoit pas d'intervention législative, mais plusieurs lignes d'action : 1) l'élaboration d'un Code de bonnes pratiques ambitieux par les acteurs clés du marché (dont les réseaux sociaux, les publicitaires et les autres membres du secteur publicitaire) ; 2) le renforcement des capacités en matière de vérification des faits et de suivi de la désinformation ; 3) le recours aux nouvelles technologies (comme l'intelligence artificielle) pour lutter contre la désinformation ; 4) le renforcement des processus électoraux, et 5) la promotion de l'éducation aux médias et de la maîtrise des médias.

95. En septembre 2018 a été adopté un Code de bonnes pratiques contre la désinformation[95], destiné à protéger les élections européennes de 2019. Ce Code poursuit les objectifs suivants :

- garantir la transparence au sujet des contenus sponsorisés, en particulier de la publicité à caractère politique ; restreindre les possibilités de ciblage de ces publicités et réduire les recettes des vecteurs de désinformation ;
- offrir plus de clarté sur le fonctionnement des algorithmes et permettre une vérification par des tiers ;
- faire en sorte que les utilisateurs puissent plus aisément découvrir et consulter des sources d'information différentes offrant des points de vue contrastés ;
- adopter des mesures visant à identifier et à fermer les faux comptes et à traiter le problème des bots automatiques ;
- fournir aux organismes de vérification des faits, aux chercheurs et aux pouvoirs publics les moyens de surveiller la désinformation en ligne.

96. La Commission européenne, à travers son programme-cadre pour la recherche et l'innovation Horizon 2020, a également soutenu plusieurs initiatives innovantes de développement de nouveaux outils et services destinés à aider les professionnels et les citoyens

[93] Voir https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
[94] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre la désinformation en ligne : une approche européenne, COM(2018) 236 final. Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018DC0236&from=FR.
[95] Disponible sur : https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

à vérifier les contenus en ligne (textes, images et vidéos). Elle compte en outre créer un réseau européen indépendant de vérificateurs de faits, qui seront sélectionnés parmi les membres européens de l'IFCN. Le réseau va mettre au point des méthodes de travail et repérer les bonnes pratiques afin d'assurer la plus grande couverture possible à ses corrections factuelles. Pour soutenir cet objectif, la Commission fournira au réseau les outils en ligne nécessaires, via une plateforme européenne sécurisée sur la désinformation. Par le biais du Mécanisme pour l'interconnexion en Europe (MIE), la Commission soutiendra également le déploiement d'une plateforme européenne sur la désinformation afin de renforcer les capacités de détection et d'analyse des campagnes de désinformation dans toute l'Europe.

97. En septembre 2018, la Commission européenne a formulé des recommandations spécifiques visant à défendre les processus démocratiques européens contre les manipulations exercées par des pays tiers ou des intérêts privés ; elle a proposé de nouvelles règles concernant les réseaux de coopération sur les élections, la transparence en ligne et la protection contre les incidents de cybersécurité, ainsi qu'une intensification de la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen[96]. En décembre 2018, un Plan d'action contre la désinformation[97] a été adopté, dans le but de renforcer les capacités et la coopération entre États membres et entre institutions de l'UE afin de prendre les devants face aux menaces associées à la désinformation. Notons aussi l'avis sur la manipulation en ligne et les données personnelles adopté en mars 2018 par le Contrôleur européen de la protection des données[98], qui recommande que les règles en matière de protection des données soient complétées et appliquées, que les régulateurs établissent ensemble un diagnostic du problème et coopèrent de façon transversale, que l'autorégulation et les codes de conduite soient encouragés et que les individus aient les moyens d'exercer leurs droits, y compris par des actions collectives.

98. Parmi les différents règlements de l'UE, ceux qui suivent sont particulièrement pertinents dans notre contexte :

- Le Règlement général sur la protection des données (RGPD[99]), directement applicable dans l'UE depuis le 25 mai 2018. Ses dispositions, à caractère obligatoire, offrent aux individus de nombreux droits, dont celui à une communication transparente, à l'effacement des données (« droit à l'oubli ») et à la portabilité des données (transfert d'un responsable du traitement des données à un autre). Le Règlement interdit généralement le traitement des données à caractère personnel « qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Il prévoit quelques exceptions, notamment lorsque « le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ». Les droits établis par le RGPD peuvent être exercés et appliqués non seulement par les individus, mais aussi par des organisations agissant en leur nom. Pour combler les

[96] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – « Garantir des élections européennes libres et équitables », COM(2018) 637 final. Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0637&from=FR.
[97] Voir https://eeas.europa.eu/sites/eeas/files/plan_daction_contre_la_desinformation.pdf
[98] Disponible sur : https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
[99] Disponible sur : https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_fr

lacunes liées à un traitement inapproprié des données hors de l'UE, le RGPD étend sa protection juridique au traitement des données personnelles de citoyens de l'UE indépendamment du lieu où se déroulent les activités de traitement. Cela le rend applicable aux entités établies hors de l'UE, si elles proposent des biens ou des services à des habitants de l'Union ou si elles surveillent leur comportement en ligne. Le Règlement encadre strictement les transferts de données hors de l'Union ; les responsables du traitement des données doivent tenir un registre de toutes leurs activités de traitement. Ils sont tenus d'adopter toutes les mesures nécessaires pour garantir que les données personnelles sont traitées de manière légale, équitable et transparente. Le RGPD a donc le potentiel voulu pour prévenir le traitement non autorisé de données personnelles à des fins électorales, comme celui qu'a pratiqué Cambridge Analytica[100].

- Le Règlement (UE) 2015/2120 établissant des mesures relatives à l'accès à un internet ouvert[101], en vigueur depuis le 30 avril 2016, crée pour les internautes de l'UE le droit individuel et opposable d'accéder à des contenus et services internet de leur choix et de les diffuser ; il affirme le principe de gestion non discriminatoire du trafic. La mise en œuvre des règles sur l'internet ouvert dans l'UE est assurée par les autorités nationales de régulation, qui devraient respecter les lignes directrices adoptées en 2016 par l'Organe des régulateurs européens des communications électroniques (ORECE). Par conséquent, il n'appartient pas aux prestataires de services internet d'arbitrer sur l'échec ou la réussite des services et des contenus diffusés. Les règles inscrivent le principe de la neutralité du réseau dans le droit de l'UE et cherchent à éviter que des contenus, applications et services en ligne ne soient bloqués, étouffés ou discriminés[102].

- La Directive 2000/31/CE du Parlement européen et du Conseil[103] prévoit des exonérations de responsabilité pour certains prestataires de services en ligne, dont les prestataires de services d'« hébergement », à condition qu'ils agissent promptement pour retirer les informations illégales qu'ils hébergent ou pour les rendre inaccessibles *dès le moment où ils en ont connaissance*. À cet égard, il faut noter que la Commission européenne, dans plusieurs communications récentes, a souligné la nécessité que les plateformes en ligne agissent de façon plus responsable et accentuent, dans toute l'UE, les efforts d'autorégulation visant à supprimer les contenus illégaux ; le 1er mars 2018, elle a adopté une Recommandation sur les mesures destinées à lutter contre les contenus illicites en ligne[104], qui s'adresse aux États membres et aux prestataires de services d'hébergement et vise à accroître la transparence et l'exactitude des mécanismes de notification et d'action.

C. Exemples au niveau national

99. Plusieurs États membres ont récemment adopté, ou prévoient de le faire, une législation conçue pour réglementer les contenus en ligne et lutter contre la désinformation à caractère politique en période électorale. L'Allemagne a ouvert la voie[105], en obligeant les intermédiaires d'internet (tels que Facebook, Instagram, Twitter ou YouTube) à retirer rapidement, sur réclamation, tout contenu illégal désigné comme tel dans le Code pénal ; les contenus manifestement illégaux doivent être bloqués ou supprimés dans les 24 heures. Les contenus concernés vont du discours de haine et de certaines infractions de diffamation à la menace contre

[100] Pour en savoir plus sur la mise en œuvre du RGPD dans les différents pays européens, voir : https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/.
[101] Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32015R2120.
[102] Voir https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.
[103] Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32000L0031.
[104] Disponible sur : https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.
[105] *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (*Netzwerkdurchsetzungsgesetz* – NetzDG) – Loi pour l'application du droit sur les réseaux, https://germanlawarchive.iuscomp.org/?p=1245.

l'ordre constitutionnel ou la sécurité nationale, etc. ; cette législation, bien que de nature générale et non spécifique aux campagnes électorales, peut avoir un impact direct sur l'opinion et le débat public, en particulier en période électorale. La loi allemande pour l'application du droit sur les réseaux, entrée en vigueur début 2018, prévoit des amendes pouvant atteindre 50 millions d'euros, applicables même si l'infraction n'a pas été commise en Allemagne.

100. En novembre 2018, le Parlement français a adopté une loi relative à la lutte contre la manipulation de l'information[106] en période électorale, destinée à identifier et à faire cesser les allégations délibérées d'un fait inexact ou trompeur par le biais d'un service en ligne pendant les trois mois précédant une élection. La nouvelle législation soumet les plateformes à une obligation de transparence : elles doivent fournir des informations loyales, claires et transparentes sur leur propre identité et qualité et sur celles du tiers pour lequel elles mettent en avant des contenus ; elles doivent aussi rendre public le montant des rémunérations reçues en contrepartie de la promotion de tels contenus. Le ministère public, toute personne ayant un intérêt urgent à porter l'affaire devant un juge, tout parti ou tout candidat peut porter plainte au sujet d'une information inexacte ou trompeuse diffusée en ligne de manière délibérée, artificielle ou automatisée et massive ; le caractère artificiel et la diffusion massive laissent soupçonner des informations fausses. Le juge est tenu de se prononcer dans un délai de 48 heures ; il est habilité à bloquer la publication et à contraindre la plateforme à faire cesser la campagne en question. Les intermédiaires techniques, c'est-à-dire les personnes offrant l'accès à des services de communication, doivent retirer rapidement tout contenu illicite porté à leur attention et mettre en place un dispositif facilement accessible et visible permettant à leurs utilisateurs de leur signaler de fausses informations. En outre, le Conseil supérieur de l'audiovisuel peut refuser de conclure une convention avec un pays étranger si les activités de ce dernier peuvent porter atteinte, en diffusant de fausses informations, aux intérêts fondamentaux de la nation ou au pluralisme des courants d'opinion[107].

101. La Russie[108], Singapour[109] et les Philippines ont cité la loi allemande comme un exemple positif en envisageant d'adopter, ou en adoptant, une législation destinée à lutter contre les contenus « illégaux » en ligne[110].

102. La Commission électorale britannique a appelé à rendre la pratique des campagnes électorales numériques plus transparente pour les électeurs. Elle a formulé des recommandations sur le caractère responsable des campagnes numériques, les dépenses

---

[106] Loi n° 2018 1202 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDB587F21F791D8941E5E11E82A0320A.tplgfr22s_1?cidTexte=JORFTEXT000037847559&categorieLien=id.

[107] La loi française a été vivement critiquée ; voir par exemple https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law. Au sujet de l'Allemagne, voir par exemple https://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590 et https://www.economist.com/europe/2018/01/13/germany-is-silencing-hate-speech-but-cannot-define-it.

[108] La loi fédérale « Sur l'information, les technologies de l'information et la sécurité de l'information » (27 juillet 2006, n° 149-FZ) a été adoptée le 18 mars 2019. Elle érige en infraction pénale la diffusion d'« informations non fiables d'importance sociale » pouvant nuire à la vie et à la santé publique, menacer massivement la sécurité publique, etc. La loi permet de bloquer les pages web comportant de telles informations. Le même jour a été adoptée la loi fédérale n° 30-FZ (« loi sur l'outrage »), qui ajoute un article 15.1.1 à la loi fédérale « Sur l'information, les technologies de l'information et la sécurité de l'information » (27 juillet 2006, n° 149-FZ). Elle érige en infractions pénales les messages constituant « un outrage à la société, à l'État, aux symboles officiels de l'État […] et aux organes exerçant le pouvoir de l'État » exprimés « sous une forme obscène ». Le Code des infractions administratives a été modifié pour prévoir des amendes en cas de publications contenant un « outrage obscène » et des « informations fausses ».

[109] https://techcrunch.com/2019/05/09/singapore-fake-news-law/?renderMode=ie11&guccounter=1&guce_referrer_us=aHR0cHM6Ly90ZWNoY3J1bmNoLmNvbS8yMDE5LzA1LzA5L3NpbmdhcG9yZS1mYWtlLW5ld3MtbGF3Lw&guce_referrer_cs=oKT9smcHtaNhdWGcU8VGvg ; https://mediawrites.law/fake-news-law-passed-in-singapore-protection-from-online-falsehoods-and-manipulation-act/

[110] Voir https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

afférentes, la transparence sur la rémunération des campagnes numériques et la mise en œuvre des règles en question[111].

103. Aux États-Unis, la loi bipartite sur la « publicité honnête » présentée au Congrès en octobre 2017[112] envisage des règles de divulgation et d'exclusion de responsabilité concernant la publicité politique en ligne. Les télévisions et radios sont tenues de longue date de divulguer l'identité de tous ceux qui leur achètent de l'espace publicitaire et la teneur de leurs messages ; ce n'est pas encore le cas pour les entreprises d'internet. La loi sur la publicité honnête obligerait les entreprises internet à révéler le contenu des publicités relatives à des élections ou à des campagnes et l'identité de leurs commanditaires. Plus précisément, il s'agirait de modifier une loi sur le financement des campagnes remontant à 1971 en ajoutant l'expression « communication payante sur internet ou communication numérique payante » à la liste des formes de médias soumises à la loi. La loi obligerait également tout site web dépassant les 50 millions de vues par mois – comprenant donc Facebook, Google et Twitter – à tenir une liste publique de toutes les organisations ou personnes dépensant au moins 500 $ en publicités relatives aux élections. Une exception serait prévue pour les « actualités, commentaires ou éditoriaux », pour veiller à ce que les exigences ne pèsent pas sur des expressions d'opinions ou couvertures d'actualités légitimes.

104. Dans certains pays, des unités spécialisées dans la lutte contre les désordres de l'information ont été créées ou sont en cours de création, par exemple :

a) Au Royaume-Uni, il est prévu de mettre en place une unité nationale sur la sécurité des communications pour lutter contre la désinformation par les « fake news ».
b) En République tchèque, le Centre de lutte contre le terrorisme et les menaces hybrides, placé sous l'égide du ministère de l'Intérieur, est une unité spécialisée dans l'analyse et les communications chargée de surveiller les menaces contre la sécurité nationale, ce qui recouvre un large éventail de dangers et d'incidents potentiels : terrorisme, attaques contre des cibles vulnérables, aspects sécuritaires des migrations, extrémisme, rassemblements publics, atteintes à l'ordre public et différentes infractions pénales, mais aussi campagnes de désinformation menaçant la sécurité intérieure. Le Centre formule également des propositions de solutions pratiques et législatives, qu'il met en œuvre chaque fois où c'est possible, et diffuse des informations et effectue des campagnes de sensibilisation auprès du grand public et des professionnels.

105. Au Brésil, le Conseil consultatif sur internet et les élections, qui conseille le Tribunal électoral, a encouragé la coopération entre autorités électorales, universitaires et praticiens en vue d'estimer l'efficacité et l'impact réel des mesures adoptées. Au Panama et au Mexique[113] par exemple, les opérateurs et les plateformes coopèrent avec les autorités électorales pour détecter les menaces et diffuser les informations officielles.

106. La vérification des faits[114] s'est développée dans de nombreux pays[115]. Dans certains d'entre eux, des réseaux de vérificateurs sont apparus ; citons par exemple #Verificado2018, groupe de journalistes, de citoyens et de partenaires universitaires qui se sont efforcés de démystifier la désinformation virale, de vérifier la véracité des affirmations des politiques et de

---

111 Voir https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf

112 https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22Honest%20Ads%20act%22%7D&searchResultViewType=expanded.

113 Au Mexique, pendant les préparatifs des élections de 2018, l'INE (Instituto Nacional Electoral) a conclu des accords de coopération avec Facebook, Twitter et Google ; voir INE, *Democracia en riesgo, Elecciones en tiempos de desinformación, Estrategia y acciones implementadas para enfrentar la desinformación deliberada en las elecciones mexicanas de 2018*.

114 Cf. Lazer et al., 2018.

115 Voir par exemple l'annexe du rapport CdE 2017 : Les désordres de l'information, qui recense les initiatives de vérification des faits et de démystification en Europe. Voir aussi https://reporterslab.org/fact-checking/.

lutter contre les fake news à l'occasion des élections fédérales mexicaines de 2018. L'Espagne a également mis en place une unité spéciale de vérification des faits lors des dernières élections[116].

VII. Défis du numérique pour la démocratie et les droits de l'homme

107. 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, ce qui englobe 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 œuvre à travers les dispositifs électoraux et la justice ordinaire.

108. Le recours aux technologies numériques affecte plusieurs aspects spécifiques de la démocratie. Premièrement, les nouvelles technologies de l'information – vote électronique ou mise en place et actualisation de listes électorales centralisées, par exemple – ont un impact sur la *démocratie électorale*, c'est-à-dire sur les activités et infrastructures institutionnelles qui rendent les élections possibles, souvent désignées dans le contexte d'internet par le terme d'« administration en ligne ». Deuxièmement, internet et les nouvelles technologies de l'information ont le potentiel d'autoriser davantage de transparence et de comptes rendus, ainsi que des formes plus larges et plus efficaces de participation politique, élargissant le champ de la « sphère publique » ; en ce sens, ils ont un impact sur la démocratie délibérative, c'est-à-dire sur la participation des individus à un débat ouvert avec la conviction qu'il aboutira à de meilleures décisions sur les sujets de préoccupation communs[117]. Enfin, dans la mesure où ces technologies aident de nombreuses personnes dispersées à s'organiser et à agir sur une question sociale, économique ou politique précise, on peut considérer qu'elles ont une influence sur la « *démocratie du suivi* », à savoir « les comptes à rendre au public et le contrôle par le public des décisionnaires, qu'ils œuvrent dans le domaine de l'État, des institutions interétatiques ou des organisations dites non gouvernementales ou de la société civile comme les entreprises, les syndicats, les associations sportives ou caritatives» [118]. Dans la mesure où la capacité des citoyens à exercer un suivi et à s'auto-organiser à des fins politiques dépend à la fois des informations auxquelles ils ont accès et de leurs possibilités de délibérer et de s'entendre sur un ordre du jour commun, on peut considérer que les variables de cette démocratie du suivi entrent dans la catégorie de la démocratie délibérative.

A. Défis pour la démocratie électorale

109. Comme évoqué plus haut, le concept de « *démocratie électorale* » désigne les activités et les infrastructures institutionnelles qui rendent les élections possibles. De l'organisation du scrutin lui-même à la création et à l'administration des listes électorales ou au recours à des urnes électroniques ou au vote par internet, l'aspect électoral de la démocratie fixe les conditions matérielles et institutionnelles requises pour traduire le suffrage populaire en désignation de représentants ou en adoption de lois et de politiques publiques. La bonne tenue des listes électorales, par exemple, est cruciale pour l'application du principe du suffrage universel, tout comme l'est le strict respect des procédures de vote et de dépouillement pour celle du principe du suffrage libre.

---

[116] https://elpais.com/politica/2019/03/10/actualidad/1552243571_703630.html.
[117] Laidlaw 2015, pp. 10-11.
[118] John Keane, *The Life and Death of Democracy*, 2009. Pour une définition de la « démocratie du suivi » (*monitory democracy*), voir http://thelifeanddeathofdemocracy.org/glossary/monitorydemocracy/.

110. Si, d'une part, l'usage des technologies numériques peut rendre les processus démocratiques plus accessibles pour tous les citoyens, il peut aussi entraver l'exercice et le développement de la démocratie électorale, en suscitant de nouvelles formes d'ingérences indues dans le droit de voter et de se présenter à une élection (Protocole n° 1 à la CEDH, article 3), le droit à la liberté d'expression (article 10 CEDH) et le droit au respect de la vie privée (article 8 CEDH).

111. D'après le Centre de la sécurité des télécommunications (CST) du gouvernement canadien, « dans le monde entier, des parties adverses mobilisent des moyens cybernétiques […] contre les élections, […] pour faire baisser la participation, truquer les résultats et voler les données des électeurs [...], contre des partis et des personnalités politiques, [...] pour se livrer au cyberespionnage à des fins de contrainte et de manipulation, pour discréditer publiquement des individus [...] [et] contre les médias, à la fois traditionnels et sociaux […] pour répandre la désinformation et la propagande et orienter les opinions des électeurs» [119]. D'après le CST en outre, il est « hautement probable que les activités de cybermenaces contre les processus démocratiques dans le monde gagnent en volume et en sophistication » dans les années à venir, pour les raisons suivantes[120] :

- *De nombreux moyens cybernétiques efficaces, peu coûteux et faciles à utiliser se trouvent à la disposition du public.*
- *L'essor rapide des réseaux sociaux, associé au déclin des sources d'information qui ont longtemps fait autorité, facilite l'usage de moyens cybernétiques et d'autres méthodes pour injecter désinformation et propagande dans les médias et influencer les électeurs.*
- *Les administrations électorales utilisent de plus en plus internet pour améliorer leurs services aux électeurs. Or, plus ces services basculent en ligne, plus ils sont exposés aux cyberattaques.*
- *La prévention des menaces cybernétiques est délicate, car il est souvent difficile de les détecter, d'en trouver les auteurs et d'y réagir dans de brefs délais. Par conséquent, le*

[119] CST 2017. On connaît plusieurs exemples de telles interventions dans le monde entier :

- « En juin 2016, l'État étasunien d'Arizona a fermé son système d'enregistrement des électeurs pendant près d'une semaine après des tentatives frauduleuses d'accès au système. Le mois suivant, l'agence électorale de l'État de l'Illinois a fermé son site internet pendant deux semaines : elle avait découvert que des dizaines de milliers de fiches d'électeurs (noms, adresses, numéros de permis de conduire…) étaient susceptibles d'avoir été consultées par les parties adverses » (Nakashima, cité par le CST).
- « Face aux faiblesses perçues de ses systèmes de dépouillement des suffrages et aux avertissements quant aux risques de ciblage des élections par la Russie, les Pays-Bas ont modifié les procédures de vote lors de leur scrutin le plus récent. Pour éviter que des parties adverses ne puissent s'ingérer dans l'élection, tous les suffrages ont été comptés manuellement » (Escritt, cité par le CST).
- « En décembre 2016, des parties adverses sont parvenues à accéder au site internet de la Commission électorale centrale du Ghana pendant les élections générales au moment du dépouillement. Un inconnu a twitté de faux résultats, annonçant la défaite du candidat sortant. La Commission électorale a répliqué par d'autres tweets affirmant que ces résultats étaient faux. Bien que l'issue de l'élection n'ait pas été altérée, l'incident a semé la confusion dans l'esprit de nombreux électeurs » (BBC News, cité par le CST).
- « Lors de la dernière élection présidentielle aux États-Unis, les deux principaux partis politiques ont fait l'objet de tentatives de cyberespionnage par la Russie. Des agents russes ont utilisé les possibilités cybernétiques pour accéder aux courriels de personnel politique clé, travaillant à la campagne du Parti démocrate. Ils ont ensuite fait fuiter ces courriels de manière à gêner la candidate du Parti démocrate » (ODNI, cité par le CST).
- « D'après certains médias, les services de renseignement français pensent que des réseaux zombies ont été utilisés pour influencer l'élection présidentielle. Des comptes de réseaux sociaux, les mêmes que ceux qui étaient actifs lors de l'élection étasunienne de l'année précédente, ont mis en avant des informations fausses et diffamatoires contre un candidat bien placé. Quelques jours avant le scrutin, un parti a aussi subi la publication non autorisée de milliers de courriels relatifs à sa campagne » (Auchard, cité par le CST).
- « La cyberguerre, autrefois très hypothétique, est devenue une réalité établie, et les attaques de la part d'États étrangers contre un système national de vote en ligne constituent désormais une menace crédible. En mai 2014, des pirates affiliés à la Russie ont pris pour cible les infrastructures électorales ukrainiennes et brièvement retardé le dépouillement des suffrages » (Springall *et al.* 2014).

[120] CST 2017.

rapport coût/bénéfices penche en faveur de ceux qui utilisent les moyens cybernétiques plutôt que de ceux qui se défendent contre leur utilisation.

- *Enfin, il existe une « dynamique du succès » qui pousse les auteurs d'attaques à recommencer et inspire, par mimétisme, des comportements similaires.*

112. La Convention sur la cybercriminalité du Conseil de l'Europe, STE 185 (« Convention de Budapest », 2001) et les travaux actuellement menés sur un deuxième Protocole additionnel à ce traité montrent que de nombreux États ont pris la mesure des risques[121].

113. Sous l'angle de la cybercriminalité, deux types d'ingérence au moins peuvent menacer la démocratie électorale. Le premier consiste à attaquer la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques électoraux, et notamment à :

- compromettre les listes électorales ou les systèmes d'enregistrement des électeurs, par exemple en piratant des systèmes informatiques ou en supprimant, modifiant ou ajoutant des données ;
- altérer les machines à voter afin de manipuler les résultats ;
- s'ingérer dans le fonctionnement des systèmes (en lançant par exemple une attaque par déni de service distribué le jour du scrutin) ;
- accéder illégalement à des systèmes informatiques pour subtiliser, modifier ou diffuser des données sensibles : par exemple, voler des données sur des ordinateurs servant à une campagne électorale pour les utiliser dans des opérations de communication.

114. De telles attaques entrent clairement dans des catégories de cybercriminalité prévues par la Convention de Budapest, comme l'accès illégal à des systèmes informatiques (article 2), l'interception illégale (article 3), l'atteinte à l'intégrité des données et des systèmes (articles 4 et 5), etc. Les Parties à ce traité, qui sont aujourd'hui plus d'une soixantaine, ont transposé ces dispositions dans leur droit interne.

115. Comme mentionné précédemment, ces attaques constituent une ingérence dans plusieurs droits fondamentaux garantis par la CEDH et par d'autres instruments internationaux de droits de l'homme. Elles peuvent être menées par des pouvoirs publics, des partis politiques/ des candidats, des puissances étrangères ou des acteurs privés. À cet égard, il faut souligner qu'en vertu de la CEDH, les États ont l'obligation positive d'assurer des élections libres et sûres et de garantir des droits tels que le droit à la vie privée et la liberté d'expression.

116. Second type d'attaques : les campagnes d'information (ou plutôt de désinformation), qui ne constituent pas un cybercrime mais violent les règles concernant la protection des données personnelles, le financement de la vie politique, la couverture médiatique ou les reportages relatifs aux élections, c'est-à-dire les règles destinées à garantir des élections libres, équitables et loyales. Les preuves des atteintes à ces règles sont souvent des preuves électroniques, c'est-à-dire situées dans des systèmes informatiques. Il est essentiel, par conséquent, que les États dotent leurs autorités de justice pénale des pouvoirs nécessaires pour recueillir de telles preuves. Les Parties à la Convention de Budapest sont tenues de le faire en vertu des articles 16 à 21.

117. Les normes internationales indiquent en effet qu'il appartient aux États de prévenir les inégalités dans la couverture médiatique des campagnes électorales et de s'assurer que les citoyens sont informés sur les partis politiques, afin de pouvoir choisir leurs représentants de façon libre et éclairée. Les États doivent s'abstenir de s'ingérer indûment dans l'exercice des droits fondamentaux, mais ont aussi des obligations positives, consistant à prévenir les violations commises par des tiers. Un juste équilibre est à ménager entre les droits qui entrent en conflit. L'abus de données tirées des listes électorales à des fins partisanes, ou le « déballage » d'informations personnelles sur un candidat en pleine campagne politique, constituent des

[121] « Cybercrime in the election process : the role of the Budapest Convention », http://www.venice.coe.int/files/15EMB/Alexander_Seger.pptx.

exemples fréquents de tels conflits. La plupart des démocraties considéreraient le premier de ces scénarios comme une atteinte claire au droit à la vie privée et à l'équité électorale, même si les partis ont le droit d'accéder à ces informations. On peut avancer, en revanche, que la nature du débat démocratique autorise à faire passer le droit politique à l'expression sur un candidat avant son droit à la vie privée, à condition que l'expression en question ne soit pas clairement diffamatoire ou calomnieuse. Les démocraties contemporaines, rompues à de tels scénarios, ont produit un vaste ensemble de décisions de justice et de législations nationales sur ce dilemme.

118. Depuis deux décennies au moins, plusieurs pays expérimentent le vote par internet, dans le but de renforcer les droits politiques. Dès 2000 par exemple, la Suisse a lancé le projet « Vote électronique » afin d'en tester la fiabilité. Depuis, le pays a mené plus de 150 essais au niveau fédéral et certains cantons ont permis à leurs citoyens de voter en ligne. En 2008, la Norvège a également entrepris de tester le vote par internet, avec plusieurs essais pendant les élections municipales de 2011 et les élections législatives de 2013. Au Canada, le vote par internet est possible dans certaines provinces (Ontario et Nouvelle-Écosse) depuis 2003. L'expérimentation la plus réussie à ce jour est peut-être celle menée en Estonie, où les discussions sur le vote par internet ont commencé en 2001 et où ce vote est considéré depuis 2005 comme une forme de suffrage supplémentaire et juridiquement contraignante[122].

119. Malgré le succès de certaines de ces expériences, le vote par internet pose plusieurs problèmes de sécurité. « L'Estonie a été le premier pays au monde à recourir au vote par internet au niveau national, et aujourd'hui plus de 30 % des suffrages s'y expriment en ligne », mais des chercheurs de l'Université du Michigan et de l'Open Rights Group constatent que « le système [estonien] de vote en ligne connaît des limites structurelles et des lacunes procédurales sérieuses susceptibles de compromettre l'intégrité des élections », à tel point que « des agresseurs pourraient cibler les serveurs électoraux ou les comptes d'électeurs pour modifier l'issue d'un scrutin ou saper la légitimité du système ». Les chercheurs vont jusqu'à conclure qu'« un jour, si des progrès fondamentaux sont accomplis en matière de sécurité informatique, le profil de risque pourrait devenir plus favorable au vote par internet ; mais nous n'estimons pas possible, aujourd'hui, de sécuriser un système de vote par internet» [123].

120. Dans ce contexte, il faut souligner que la désinformation et les ingérences numériques généralisées dans le discours politique ne visent peut-être pas à subvertir le mécanisme des élections en lui-même, mais plutôt à saper la confiance du public envers ce processus et envers le système politique. L'ouverture des démocraties libérales fait à la fois leur force et leur faiblesse. On ne saurait tolérer que les technologies numériques sapent la confiance des citoyens envers le processus électoral – d'où la nécessité de les rassurer quant à la sécurisation de ces technologies. À cette fin, elles devraient être introduites progressivement et peuvent être combinées avec les méthodes traditionnelles. L'innovation ne peut se faire aux dépens des exigences légales, dont la sécurité.

121. Face à ces difficultés, plusieurs approches interdépendantes s'imposent, consistant à reconnaître 1) la nature transnationale du problème, et 2) le rôle essentiel joué par les gardiens des autoroutes de l'information (les prestataires de services internet) dans les enquêtes sur les cas de cybercriminalité et la poursuite de leurs auteurs. Le cadre international doit être renforcé en vue d'établir des mécanismes plus efficaces de coopération transnationale entre les pays et les acteurs privés, et, si possible, d'apporter plus d'uniformité dans les législations nationales. À terme, la solution semble consister à « adapter le cadre constitutionnel des démocraties modernes » au nouvel environnement électronique, cet environnement où la cybercriminalité prospère, mais aussi où pouvoirs publics, entreprises et citoyens interagissent et rendent la démocratie possible[124].

[122] ACE Project 2018.
[123] Springall et al. 2014.
[124] Mecinas Montiel 2016, p. 427.

B. Défis pour la démocratie délibérative

122. Le principe du suffrage libre repose sur la libre formation de la volonté de l'électeur. Cette liberté, qui recoupe en partie l'égalité des chances en matière électorale, implique que les États – et les pouvoirs publics en général – respectent leur devoir de neutralité, notamment en ce qui concerne l'usage des médias de masse, l'affichage, le droit de manifester sur la voie publique ou le financement des partis et des candidats[125]. La liberté de se forger sa propre opinion comprend le droit d'être correctement informé avant de prendre une décision, celui de naviguer en ligne en privé et celui de communiquer de manière confidentielle sur internet. Le suivi des activités d'internautes sans leur consentement et en vue de comprendre et d'exploiter leurs comportements en ligne est contraire à ces droits.

123. La technologie est en train de modifier les manières de faire campagne. Pour les partis, internet constitue un puissant moyen de présenter leur programme à l'électorat et d'élargir les soutiens à leurs causes. Les coûts de communication avec les électeurs peuvent s'y avérer beaucoup plus faibles qu'à la radio ou la télévision, vu la possibilité d'accéder gratuitement aux réseaux sociaux et à des plateformes de blogs et de partage de vidéos. Ce type de communication peut bénéficier en particulier aux petits partis politiques ayant des ressources limitées et aux candidats indépendants.

124. Cependant, les changements dans la production et la consommation de contenus relatifs aux élections posent un défi aux institutions et principes établis de régulation des communications électorales, comme la liberté d'association, les plafonds de dépenses et l'encadrement de la publicité politique. Ils empêchent les règles existantes d'assurer un terrain égal, en matière de communication électorale, aux acteurs anciens et nouveaux, aux riches et aux pauvres, aux entreprises et à la société civile. Les nouveaux intermédiaires et plateformes assurent aujourd'hui l'important rôle de gardiens autrefois dévolu aux journalistes, mais n'ont pas encore adopté les engagements éthiques des médias. Cela représente une menace pour les élections et ouvre la voie à d'éventuelles pratiques de corruption. L'étude du Conseil de l'Europe *Internet et campagnes électorales* (2017) identifie plusieurs sources d'inquiétude pour l'équité et la légitimité des processus électoraux, comme le manque de transparence sur les campagnes, les dépenses, les messages et les algorithmes employés pour la publicité en ligne, des atteintes à grande échelle à la vie privée, le manque de filtre journalistique pour vérifier la véracité des messages politiques, la montée de la désinformation et les failles dans la réglementation des campagnes électorales (comme l'impossibilité de faire appliquer les périodes de silence), et constate « l'incapacité de la réglementation à garantir l'équité des règles du jeu politique et à limiter le rôle de l'argent dans les élections» [126].

125. De nouvelles formes de communication viennent bousculer les campagnes électorales traditionnelles non seulement en aidant à diffuser des messages à moindre coût, mais aussi en utilisant des techniques de marketing spécifiques adaptées aux différents segments de l'électorat. Ainsi, les annonces et messages personnalisés, possibles dans tous les domaines du marketing numérique, ont été récemment appliqués au champ électoral et ont offert un avantage non transparent à ceux qui avaient accès à un tel mécanisme. Les messages électoraux sont devenus de plus en plus personnalisés. Les concepteurs des campagnes ne s'intéressent

[125] Commission de Venise, Code de bonne conduite en matière électorale, rapport explicatif : Le suffrage libre.

[126] CdE 2017 : Internet et campagnes électorales. Voir aussi le rapport de 2018 *L'impact des nouvelles technologies de l'information sur les processus électoraux* (Doublet 2018, CDDG(2018)11), qui suggère la mise en place par le Conseil de l'Europe d'un large programme d'action dans ce domaine. Il recommande par exemple de définir la durée des campagnes électorales pour éviter le risque que des campagnes numériques massives aient lieu durant les périodes préélectorales ; d'exiger l'identification du matériel numérique pour savoir qui se trouve derrière les plateformes en ligne ; d'imposer aux plateformes en ligne de déclarer les dépenses qu'elles ont consacrées aux campagnes électorales numériques, ou encore d'interdire à une personne physique ou morale étrangère d'engager des dépenses dans des campagnes numériques à des fins électorales.

guère à la partie de l'électorat ayant déjà arrêté son choix : ils se concentrent sur la minorité des électeurs indécis. Les nouvelles techniques de campagne permettent d'ajuster sur mesure les messages électoraux, parfois sous couvert de messages généraux et politiquement neutres. Cette influence souterraine est facilitée par l'utilisation des réseaux sociaux, non seulement parce que les données y sont traitées par des algorithmes, mais aussi et surtout parce qu'ils permettent d'adresser des annonces et messages personnalisés directement à des groupes de profils spécifiques sans que les destinataires ne détectent cette personnalisation. Avec l'aide de la technologie, les techniques de campagne ont basculé vers une approche évolutive, d'un à un ou de groupe à groupe : c'est ce que Joseph Pine appelle le « sur-mesure de masse» [127]. Contrairement aux médias traditionnels, qui ont en principe une couleur politique affirmée et connue des lecteurs, les prestataires d'internet n'ont pas de ligne politique déclarée. S'il n'est pas clairement précisé que les informations fournies sont en fait une annonce partisane, les utilisateurs peuvent avoir l'impression de se trouver en présence d'une information politiquement neutre.

126. La manipulation des intentions de vote a été étudiée par Rob Epstein, qui s'est notamment intéressé à l'influence des classements des résultats de recherche (en particulier sur Google, le moteur prédominant) sur les intentions de vote (l'auteur parle d'effet manipulateur des moteurs de recherche – SEME, pour *Search Engine Manipulation Effect)*[128]. D'après une étude de 2015, les résultats arrivant en tête et liés à des sites internet qui favorisent un candidat ont un impact sur les opinions des électeurs indécis[129]. Cinq expériences menées dans deux pays différents suggèrent que « 1) les classements biaisés de résultats de recherche peuvent faire varier de 20 % ou plus les intentions de vote des électeurs indécis ; 2) cette variation peut être beaucoup plus importante dans certains groupes démographiques, et 3) le classement peut être masqué de façon à ce que les internautes n'aient pas conscience de la manipulation ». Les auteurs de l'étude concluent que « si Google favorise un candidat, son impact sur les électeurs indécis peut facilement décider de l'issue des élections ». Certes, ces résultats demanderaient à être corroborés par des recherches supplémentaires, mais on peut conclure avec les auteurs qu'ils sont « d'autant plus troublants » que « l'activité de classement des résultats de recherches en ligne est entièrement déréglementée ».

127. Dans ce contexte, il faut garder à l'esprit que les classements opérés par les moteurs de recherche sont le produit d'algorithmes complexes et ne visent pas nécessairement à manipuler, mais à proposer les résultats les plus récents et les plus pertinents ; cependant, ces algorithmes eux-mêmes peuvent être manipulés par différents sites internet cherchant à monter en tête des classements. Chacun peut constater ce phénomène, et Google travaille constamment à améliorer son algorithme de recherche pour prévenir de telles intrusions. Dans tous les cas, que la manipulation soit intentionnelle ou non, l'effet « SEME » a deux conséquences de poids pour la démocratie : le pouvoir de manipuler les préférences peut être utilisé par des acteurs privés ou publics pour nuire à l'équité électorale, et les utilisateurs de moteurs de recherche n'ont pas conscience que les critères des mécanismes de classement les empêchent de prendre des décisions pleinement éclairées, et donc d'exercer leur liberté d'expression.

128. L'effet SEME n'est pas l'apanage des moteurs de recherche. Les réseaux sociaux s'appuient eux aussi sur une architecture de code qui n'est pas sans parti pris. Les entreprises comme Facebook, Twitter ou Instagram, contrairement aux médias traditionnels, ne sont pas politiquement orientées ; elles sont avant tout mues par des intérêts commerciaux et conçoivent leur structure de codage en fonction de ces intérêts. En ce sens, les algorithmes qui régissent les réseaux sociaux favorisent une vision partielle, voire illusoire de la politique et de la

[127] B.J. Pine, II. (1993), *Mass Customization : The New Frontier in Business Competition*, Harvard Business School Press, Boston.
[128] Epstein 2016.
[129] Epstein et Robertson 2015.

démocratie, car ils offrent des informations biaisées ne reflétant que les intérêts et le comportement de chaque utilisateur[130].

129. Les entreprises de réseaux sociaux et de moteurs de recherche peuvent façonner les interactions sociales en ligne parce qu'elles ont le pouvoir non seulement d'encoder l'environnement de ces interactions, mais aussi de profiler leurs utilisateurs et de prédire leurs comportements. Ces entreprises peuvent facilement accéder « aux archives de nos comportements numériques : « j'aime » sur Facebook, historiques de navigation, termes que nous avons recherchés ou historiques d'achat, qui peuvent être utilisées pour prédire automatiquement et avec précision une série de traits personnels très sensibles dont l'orientation sexuelle, l'appartenance ethnique, les opinions politiques et religieuses, la personnalité, l'intelligence, le niveau de bonheur, la consommation de substances addictives, la séparation d'avec le conjoint, l'âge ou le genre» [131]. En outre, les architectes des sites peuvent traiter ces informations de façon à créer des profils d'utilisateurs très précis, à prédire leurs préférences et même à leur réserver des données et des annonces ciblées afin de promouvoir ou de décourager certains comportements[132].

130. D'un côté, les entreprises comme Facebook ou Google vendent les données de leurs utilisateurs. De l'autre, ceux qui les achètent utilisent ces données, en n'ayant pas ou presque pas à rendre des comptes, pour influencer les consommateurs et parfois les électeurs au moyen de « publicités sur mesure fondées sur des informations personnelles» [133]. C'est exactement ce qu'a fait Cambridge Analytica. Le modèle commercial actuel de nombreux sites web consiste à offrir des contenus en échange de données personnelles. Le fait que nous soyons prêts à livrer de telles informations en échange de services gratuits permet une collecte généralisée de données par les sites web, et donc de potentiels usages et abus par différents acteurs.

131. Certes, les utilisateurs de réseaux sociaux doivent accepter expressément les conditions générales en matière de vie privée imposées par leurs propriétaires, mais ils n'ont aucun ou pratiquement aucun contrôle sur les personnes autorisées à « acheter » leurs données personnelles ou sur les usages qui peuvent en être faits. Une telle situation sape le droit fondamental à la protection de la vie privée et des données personnelles, puisque l'utilisateur ne peut quasiment pas imposer de limites aux utilisations de ces données[134]. Dans son arrêt n° 292/2000, le Tribunal constitutionnel espagnol affirme : « Le droit fondamental à la protection des données personnelles […] confère à son titulaire une série de facultés, consistant principalement à imposer à des tiers d'accomplir certaines actions ou de s'en abstenir […]. Le droit à la protection des données garantit aux individus le pouvoir de disposer de ces données. […] Mais [ce pouvoir] se vide de sa substance si l'intéressé ignore quelles données se trouvent en possession de tiers, qui les possède, et à quelles fins» [135].

132. Ceux qui usent et abusent ainsi des données personnelles à des fins électorales, sous couvert de liberté du commerce, peuvent menacer sérieusement la nature libre et équitable des

---

[130] Van Dijck 2013 ; McChesney 2013.
[131] Graepel et al. 2013.
[132] Par exemple, comme le raconte Robert Epstein (2016) :
« […] Une étude réalisée entre autres par Robert M. Bond, aujourd'hui professeur de sciences politiques à l'Ohio State University, parue dans Nature *en 2012, décrit une expérience à l'éthique discutable pour laquelle, un jour d'élection en 2010, Facebook a adressé à plus de 60 millions de ses utilisateurs un rappel : « Allez voter ! ». Ce message a fait se rendre aux urnes quelque 340 000 personnes qui, autrement, ne se seraient pas déplacées. En 2014, dans le magazine New Republic, Jonathan Zittrain, professeur de droit international à l'Université Harvard, souligne que vu la masse des informations qu'il a collectées sur ses utilisateurs, Facebook pourrait très bien n'adresser un tel rappel qu'aux partisans de tel ou tel parti ou candidat, et faire facilement basculer l'issue d'un scrutin serré – sans que personne ne le sache. Et comme les publicités, ainsi que les classements des résultats de recherche, sont éphémères, ce type de manipulation d'un scrutin ne laisserait aucune trace sur le papier ».*
[133] Christopher Wylie, cité par Guimón 2018.
[134] Davara 2003, pp. 43-44.
[135] Cité par Davara 2003.

élections, d'au moins trois manières : premièrement, des acteurs privés peuvent utiliser de telles informations pour exercer directement des pressions indues sur la compétition électorale ; deuxièmement, les entreprises d'internet et de réseaux sociaux, sous prétexte de liberté commerciale, peuvent restreindre l'accès à ces informations en fonction de leurs orientations politiques, offrant ainsi un avantage peu détectable à certains partis ou candidats ; troisièmement, la marchandisation des données personnelles complique la surveillance des sommes dépensées pour les campagnes.

133. Les menaces qui pèsent sur les droits au respect de la vie privée, à des élections libres et équitables et à la liberté d'expression et d'opinion – certains experts y ajoutent même la liberté de pensée – pointent la nécessité de réglementer les droits commerciaux des entreprises d'internet et des réseaux sociaux. Cela étant, interdire totalement la « marchandisation des informations » entraverait aussi le développement d'internet et, par conséquent, l'accès à une source apparemment inépuisable d'information politique et d'action démocratique. Tant que les entreprises n'auront pas trouvé de nouvelles formes de financement d'internet, imposer des limites excessives à la marchandisation des données personnelles pourrait faire obstacle à des droits politiques fondamentaux tels que la liberté d'expression et la liberté d'organiser des actions politiques. Paradoxalement, les technologies qui ont accru les possibilités d'expression sont aussi celles qui nuisent à ces possibilités[136].

134. D'une part, le droit d'accéder à internet est une condition nécessaire au plein exercice de la liberté d'expression, elle-même indispensable à l'existence d'une société démocratique[137]. D'autre part, internet lui-même fait peser sur la démocratie plusieurs types de menaces. Ni les réseaux sociaux, ni internet ne sont (et ne devraient devenir) un espace hors-la-loi[138]; il est donc urgent de trouver des solutions à ces conflits de droits de manière à protéger raisonnablement la vie privée et les droits politiques et commerciaux.

135. L'absence de réglementation d'internet et des réseaux sociaux ou son insuffisance prive les utilisateurs de tout recours juridique pour préserver leurs données et, surtout, leur liberté

---

[136] Pour citer Laidlaw (2015, p. xi-xii) : *« Les technologies de communication qui favorisent ou entravent la participation au discours en ligne sont entre les mains d'acteurs privés […]. Inévitablement, nous dépendons de ces entreprises pour exercer notre droit à la liberté d'expression en ligne, et elles deviennent les gardiennes de notre expérience en ligne […].*
Le pouvoir qu'ont ces gardiens sur notre exercice du droit à la liberté de parole a eu deux effets. Premièrement, les entreprises concernées sont de plus en plus visées par des mesures juridiques visant à mettre à profit leur capacité à réguler les comportements de tiers […]. Deuxièmement, […], l'encadrement de la parole dans le cyberespace a largement été abandonné à l'autorégulation, à l'image de l'encadrement très léger d'internet en général […]. Il en résulte un système de gouvernance privée parallèle à la loi et dépourvu de toutes les garanties de droits de l'homme qu'on attend habituellement des systèmes gérés par l'État, comme les principes de responsabilisation, de prévisibilité, d'accessibilité, de transparence et de proportionnalité ».

[137] *Lingens c. Autriche*, requête n° 9815/82 (Cour eur. DH, 8 juillet 1986) : « La liberté d'expression, consacrée par le paragraphe 1 de l'article 10 (art. 10-1), constitue l'un des fondements essentiels d'une société démocratique ». De plus, dans l'affaire *Ahmet Yıldırım c. Turquie* (requête n° 3111/10, 18 décembre 2012), la Cour conclut que le blocage d'internet « semble heurter de front le libellé même du paragraphe 1 de l'article 10 de la Convention, en vertu duquel les droits reconnus dans cet article valent "sans considération de frontière" ».
Voir aussi Laidlaw (2015, pp. 19-21) :
« La démocratie s'est toujours incarnée dans des pratiques de communication, et la liberté d'expression est constamment considérée par les tribunaux comme centrale pour la démocratie. Pour citer un passage fameux de l'arrêt Lingens c. Autriche *de la Cour européenne des droits de l'homme, la liberté d'expression « constitue l'un des fondements essentiels d'une société démocratique ». […]*
De nombreux pays, comme l'Estonie, la Finlande, la France, la Grèce et l'Espagne, ont légiféré pour reconnaître l'accès à internet comme un droit fondamental. En 2003, le Comité des Ministres du Conseil de l'Europe a adopté une Déclaration affirmant l'importance de la liberté d'expression sur internet. Depuis 2010, on observe un changement de paradigme au niveau international autour de la reconnaissance des droits de l'homme dans le cyberespace. L'accès à internet comme droit fondamental a reçu le blanc-seing de l'ONU à travers un rapport de Frank La Rue, Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression […]. Puis, en 2012, le Conseil des droits de l'homme des Nations Unies a adopté une résolution affirmant la liberté d'internet comme relevant des droits fondamentaux, dont notamment le droit à la liberté d'expression ».

[138] Tribunal électoral du Mexique, g.

d'expression et leurs droits démocratiques. D'une part, il est problématique que des entreprises privées censurent les contenus qu'elles jugent « nuisibles » sans rendre de comptes et sans transparence sur leurs actions.

136. D'autre part, la responsabilité positive qu'a l'État de prévenir les ingérences indues de tierces parties ne doit pas entraîner d'ingérence indue de la part de l'État lui-même, à travers une réglementation excessive ou injustifiée pouvant porter atteinte aux droits qu'elle est censée protéger. La surveillance injustifiée par l'État de communications privées, et les différentes manières dont les plateformes en lignes peuvent être utilisées pour affecter – intentionnellement ou accidentellement – le flux des informations, nuisent directement à la liberté d'expression, au dialogue démocratique et aux principes de neutralité institutionnelle et d'équité des élections. Bien qu'on puisse comprendre, dans le contexte décrit plus haut, que de nombreux États entreprennent actuellement de légiférer contre les « fake news », une telle législation peut mettre en danger le droit fondamental à la liberté d'expression et d'information – n'oublions pas que les propos exagérés sont eux aussi protégés par les normes internationales des droits de l'homme, comme l'article 10 CEDH. Habilitées à s'ingérer dans des propos publics, les autorités pourraient abuser de ce pouvoir pour réduire les dissidents au silence, empêcher les discussions remettant en cause la pensée dominante et limiter les critiques envers la marche de la société. Comme l'a souligné la Commission de Venise, « les moyens de communication de masse ne sont pas la seule catégorie qui devrait se voir reconnaître un degré élevé de liberté d'expression. Ainsi, les personnes qui communiquent des informations ou des idées sur des questions d'intérêt public et contribuent au débat ouvert sur ces sujets, y compris les membres de groupes de campagne et les représentants élus, devraient se voir reconnaître un degré élevé de liberté d'expression, dont le droit à une certaine exagération voire à la provocation, dès lors qu'elles agissent de bonne foi et prennent les précautions requises pour fournir des informations précises et fiables» [139].

137. Le filtrage, le blocage et le retrait de contenus illégaux sur internet, notamment pour lutter contre les crimes de haine et la diffamation ou encore préserver la sécurité nationale, la propriété intellectuelle et la vie privée, représentent un exercice nécessaire mais délicat, qui peut cependant aller trop loin et aboutir à la censure et au bâillonnement illégitime des opposants politiques. De telles mesures doivent être prévues par la loi, ce qui suppose une définition précise et étroite des infractions visées[140], et poursuivre l'un des buts légitimes énumérés à l'article 10 CEDH. Les critères de nécessité dans une société démocratique et de proportionnalité doivent toujours être observés[141]. Enfin, il doit exister un recours judiciaire effectif devant un tribunal indépendant et impartial.

138. S'agissant des « fake news », dont la plupart n'entrent dans aucune des catégories autorisant des poursuites, il faut recourir à des moyens alternatifs, comme la vérification des faits (qui devient de plus en plus efficace et organisée, bien qu'elle ne constitue pas la panacée), des programmes d'éducation aux médias visant à souligner le problème et à permettre de reconnaître les contenus faux, et des investissements dans un journalisme de qualité[142]. Pour cela, les pouvoirs publics auront besoin de coopérer à la fois avec les citoyens et avec l'industrie d'internet.

139. Parallèlement, il faut souligner que toutes les mesures contre les désordres de l'information doivent être conçues avec le plus grand soin, de manière à préserver la « neutralité

[139] CDL-AD(2013)024, Avis sur la législation relative à la protection contre la diffamation de la République d'Azerbaïdjan, par. 37.
[140] Voir par exemple Commission de Venise, Avis sur la loi fédérale relative à la lutte contre les activités extrémistes de la Fédération de Russie, CDL-AD(2012)016.
[141] Voir par exemple Commission de Venise, Turquie : avis sur la loi n° 5651 de réglementation des publications sur internet et de lutte contre les infractions pénales commises par le biais de ces publications (« loi sur internet »), CDL-AD(2016)011.
[142] Voir le rapport CdE 2017 : Les désordres de l'information, qui formule plus de 30 recommandations à l'attention de différents acteurs.

du réseau ». C'est le principe fondateur de la Toile : les prestataires de services internet sont censés traiter toutes les données en ligne à égalité et assurer les conditions nécessaires à un accès sans barrières ni discrimination fondée sur les sources ou sur les contenus. Pour que le rôle démocratique d'internet ne soit pas monopolisé par des puissances privées, il est nécessaire que toutes les données envoyées et reçues soient traitées à égalité, sans écarts dans les prix et la qualité de service[143]. Abolir la politique de « neutralité du réseau », comme a accepté de le faire la Commission fédérale des communications des États-Unis en décembre 2017[144], permet aux prestataires de services internet de bloquer ou de ralentir des sites et de facturer des vitesses de téléchargement plus rapides. En pareilles circonstances, des services, applications et sites en ligne peuvent bénéficier d'un traitement préférentiel pour diverses raisons, commerciales ou idéologiques – y compris dans des pays moins démocratiques, où les prestataires d'internet sont propriétés de l'État et soumis à la censure et où les autorités peuvent être tentées de favoriser l'accès aux médias pro-gouvernement.

140. Pour conclure, bien qu'une réglementation excessive ou inadéquate d'internet puisse s'avérer contre-productive en gênant l'accessibilité et le développement d'internet et, par conséquent, la liberté d'expression et le dialogue démocratique lui-même, le problème des désordres de l'information ne saurait rester sans solution. Il est urgent d'agir contre le risque d'atteintes à la vie privée par l'abus d'informations personnelles, contre les dommages infligés à la liberté d'expression et à l'équité électorale par l'architecture même d'internet (effet manipulateur des moteurs de recherche, bulles épistémiques, chambres d'écho, fake news) et contre le manque de réglementation qui prive les citoyens de recours juridique efficace pour protéger leurs droits individuels et politiques.

141. Cette action doit passer par les puissants acteurs privés qui, quoiqu'avant tout mus par des intérêts commerciaux, sont à la fois en position d'entraver les droits de l'homme et d'assurer un forum essentiel à la démocratie, et doivent reconnaître cette responsabilité.

VIII. Conclusions

142. 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 œuvre à travers les dispositifs électoraux et la justice ordinaire.

143. 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

[143] Du point de vue du droit constitutionnel comme du droit international des droits de l'homme, il est crucial de tenir compte de l'existence d'acteurs influents, hors autorités élues, qui entravent l'exercice de droits fondamentaux. Voir Herdis Thorgeirsdóttir (2005), *Journalism Worthy of the Name : the Affirmative Side of Article 10 of the ECHR*, Kluwer Law International.

[144] La réglementation sur la neutralité du réseau, adoptée en 2015 et qui cherchait à empêcher les prestataires d'internet d'accorder un traitement préférentiel aux sites et aux services qui les payaient pour accélérer leur trafic, a officiellement expiré en juin 2018.

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.

144. Les services en ligne ont enrichi et diversifié les sources d'actualités ; ils aident les citoyens à accéder aux informations et à prendre des décisions sur des thèmes essentiels en démocratie, dont le choix de leurs représentants. Au même moment toutefois, une nouvelle ère de désordres de l'information – mésinformation, désinformation, information malveillante – a déformé l'écosystème des communications au point de grever sérieusement les décisions des électeurs, trompés, manipulés et abreuvés de fausses nouvelles destinées à peser sur leur vote. Un tel environnement pourrait saper l'exercice du droit à des élections libres et menace gravement le fonctionnement des régimes démocratiques.

145. Peu 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. Elles affirment leur responsabilité sociale, forme d'autorégulation visant avant tout à « ne pas nuire » et à respecter les principes de l'État de droit et des droits de l'homme, dont le droit des utilisateurs à un recours ou la responsabilité de l'entreprise à l'égard des produits (en vertu du droit commercial, de la concurrence, de l'environnement, etc.)[145]. Cependant, de telles initiatives sont volontaires et sporadiques et ne s'appuient pas sur un cadre juridique reconnu.

146. Bien qu'il appartienne aux États de prévenir activement les ingérences de tierces parties dans les droits civils et politiques, une intervention étatique indue, à travers une réglementation excessive ou injustifiée, peut aboutir à saper les droits qu'elle était censée protéger. La surveillance injustifiée par l'État de communications privées, et les différentes manières dont les plateformes en lignes peuvent être utilisées pour affecter – intentionnellement ou accidentellement – le flux des informations, nuisent directement à la liberté d'expression, au dialogue démocratique et aux principes de neutralité institutionnelle et d'équité des élections. Habilitées à s'ingérer dans des propos publics, les autorités pourraient abuser de ce pouvoir pour réduire les dissidents au silence, empêcher les discussions remettant en cause la pensée dominante et limiter les critiques envers la marche de la société. En particulier, le filtrage, le blocage et le retrait de contenus illégaux sur internet, notamment pour lutter contre les crimes de haine et la diffamation ou préserver la sécurité nationale, la propriété intellectuelle ou la vie privée, doivent être conformes à la loi, ce qui suppose une définition étroite et précise des infractions visées et la poursuite d'un des buts légitimes énumérés à l'article 10 CEDH. Les critères de nécessité dans une société démocratique et de proportionnalité doivent toujours être observés. Enfin, il doit exister un recours judiciaire effectif devant un tribunal indépendant et impartial.

[145] Facebook, Google et Twitter ont signé le Code de bonnes pratiques contre la désinformation et se sont engagés à présenter, tous les mois, les mesures prises en vue des élections européennes de mai 2019. Voir les rapports d'avril sur la mise en œuvre du Code de bonnes pratiques, https://ec.europa.eu/digital-single-market/news-redirect/651264.

147. S'agissant des « fake news », il faut recourir à des moyens alternatifs, comme la vérification des faits, des programmes d'éducation aux médias visant à souligner le problème et à permettre de reconnaître les contenus faux, et des investissements dans un journalisme de qualité.

148. Parallèlement, il faut souligner que toutes les mesures contre les désordres de l'information doivent être conçues avec le plus grand soin, de manière à préserver le principe de la « neutralité du réseau ». Internet devrait rester un lieu ouvert.

149. Pour relever tous ces défis interdépendants et mondiaux, plusieurs mesures sont nécessaires.

Concernant la démocratie électorale :

A. ériger 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 ;
B. 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 ;
C. préparer les administrations électorales 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.

Concernant la démocratie délibérative :

D. reconnaître 1) la nature transnationale du problème et 2) le rôle essentiel joué par les intermédiaires d'internet (prestataires de services internet et entreprises de moteurs de recherche et de réseaux sociaux) ;
E. renforcer le cadre international 1) pour établir des mécanismes plus efficaces de coopération transnationale entre les pays et les acteurs privés, et, si possible, 2) pour apporter plus d'uniformité dans les législations nationales ;
F. travailler à un modèle de réglementation et de traitement des litiges fondé sur la coresponsabilité des acteurs privés et publics, ainsi que sur de multiples approches réglementaires et de résolution des conflits. Un tel modèle pourrait englober au moins quatre stratégies, toutes capables de s'adapter en continu à l'environnement mouvant d'internet et des technologies de la communication :

- promouvoir la poursuite des recherches et de la coopération entre administrations électorales, universitaires et praticiens afin d'évaluer l'impact réel des technologies numériques sur les processus électoraux et l'efficacité des mesures adoptées ;
- favoriser une éducation destinée à renforcer la culture juridique et démocratique chez les citoyens ;
- promouvoir 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 ;
- prévoir des mécanismes de recours au niveau juridique et politique et sous forme de règlement alternatif des conflits.

150. 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.

151. 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 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.

152. Compte tenu des principaux constats issus de ces documents et de la présente étude, la montée récente de l'influence des canaux de communication électorale sur internet appelle des actions sur les points suivants :

A. réviser les 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) ;

B. amener les intermédiaires d'internet à rendre des comptes en faisant la transparence sur les dépenses et en rendant accessibles des données permettant d'assurer cette transparence, plus spécifiquement concernant la publicité politique. En particulier, les intermédiaires d'internet devraient donner accès aux données concernant les publicités politiques payantes, pour éviter de favoriser les ingérences illicites (étrangères) dans les élections et permettre d'identifier les catégories de publics visés ;

C. journalisme de qualité : renforcer l'exactitude et la fiabilité des actualités et des échanges avec le public, renforcer les médias de service public et les médias locaux, promouvoir l'autorégulation en mettant l'accent sur la transparence des actualités en ligne et de leur diffusion ;

D. 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 (avec la réflexion qui s'impose sur les limites des initiatives de vérification des faits) ; renforcer la maîtrise des médias (réseaux sociaux compris) à travers des initiatives d'éducation et de promotion;

E. internet ouvert : assurer la neutralité du réseau, envisager de renforcer juridiquement le droit des utilisateurs à un internet ouvert, 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 assurer une surveillance judiciaire pour prévenir les éventuels abus ;

F. protection des données : affirmer et protéger le droit à l'anonymat sur internet, réglementer et limiter strictement la mise en place et l'utilisation du profilage dans tous types de contextes ; en outre, le Conseil de l'Europe pourrait envisager d'adopter des

lignes directrices sur les restrictions à appliquer aux technologies de surveillance, y compris le commerce international de telles technologies ; de promouvoir la Convention 108 comme « étalon d'or » au niveau international ; et, si possible, d'élaborer un instrument juridique spécifique contre le risque élevé que l'usage des technologies numériques dans les campagnes et les publicités politiques fait peser sur la protection des données personnelles.

153. Comme nous l'avons déjà souligné, 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.