# DÉSINFORMATION ET CAMPAGNES ÉLECTORALES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# Désinformation et campagnes électorales

Yves-Marie Doublet

Direction générale de la démocratie
Gouvernance démocratique
Division de l'assistance électorale

Conseil de l'Europe

Édition anglaise :
*Disinformation and electoral campaigns*
ISBN 978-92-871-8911-0

*Les vues exprimées dans cet ouvrage sont de la responsabilité de l'auteur et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.*



Couverture et mise en page : Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Photo couverture : © Depositphotos

Éditions du Conseil de l'Europe
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-8910-3


Imprimé dans les ateliers
du Conseil de l'Europe

# Sommaire


**INTRODUCTION** 5

**1. APERÇU GÉNÉRAL DE LA SITUATION** 9

1.1. Données techniques 9

1.2. Données politiques 12

1.3. Intensification du processus 14

1.4. Réponses possibles 17

**2. RECOMMANDATIONS** 29

2.1. Définition des termes 29

2.2. Transparence 30

2.3. Durée des campagnes électorales 32

2.4. Dépenses consacrées aux campagnes électorales numériques 32

2.5. Protection des citoyens à l'égard du traitement des données à caractère personnel régi par le Règlement général européen sur la protection des données (RGPD) 33

2.6. Principes fondamentaux relatifs aux algorithmes et à l'intelligence artificielle 36

2.7. Procédure sommaire en cas d'urgence 37

2.8. Coopération avec les différents intervenants 37

2.9. Conformité avec le droit européen 39

2.10. Mise en application 39

2.11. Synthèse des propositions 39

**3. PROGRAMME D'ACTION** 41

**CONCLUSION** 45

# Introduction

1. Pour le *Cambridge Dictionary*, les *fake news* sont des « histoires fausses qui ont l'apparence d'un traitement de l'actualité, qui sont diffusées sur internet ou d'autres médias, et qui sont généralement créées pour influencer les opinions politiques ou faire une blague ».

2. Depuis l'été 2016, les *fakes news* désignent la diffusion virale délibérée de fausses nouvelles sur internet et les médias sociaux[1]. Ces mots, qui désignent un contenu fabriqué, un contenu manipulé, une imposture et un contenu trompeur, ou encore un contexte ou une connexion erronés, voire une satire et une parodie, ont donc pris des sens divers. Le *Guardian* a été le premier journal à mentionner que la petite ville de Veles, en Macédoine, est à l'origine de ce phénomène. Veles est le lieu où des sites politiques ont utilisé le piège à clics, qui pousse les visiteurs à cliquer sur un lien vers une page web particulière, aux fins de gagner de l'argent en surfant sur la Trumpmania pendant la campagne électorale américaine en 2016. Plus de 100 sites affichant des fausses nouvelles ont été animés par des adolescents de cette ville. Une enquête menée par le site américain Buzzfeed le 3 novembre 2016, quelques jours avant l'élection présidentielle américaine, explique le succès du phénomène : « La meilleure façon de créer de la rumeur médiatique est d'associer des publications politiques sur Facebook à des contenus à caractère sensationnel et souvent faux, ce qui peut plaire aux partisans de Trump[2]. »

3. Cette approche impose de faire la distinction entre la fausse information, la désinformation et la propagande, ce que décrit très précisément la chercheuse américaine Renee DiResta, directrice de l'analyse des politiques à Data for Democracy[3]. La fausse information fait référence à des informations incorrectes ou erronées relayées par des journalistes sans intention de nuire. La désinformation est une tentative délibérée d'amener le public à croire des choses fausses. Elle consiste à fabriquer des informations qui sont mélangées à des faits et des pratiques qui dépassent le cadre du traitement de l'actualité. Il s'agit notamment de comptes automatisés utilisés pour

1. « Fake News Definition und Rechtslage », Wissenschaftlicher Dienste, Deutscher Bundestag, 2017.
2. « L'histoire vraie des *fake news* », *L'Opinion*, 1315, 7 août 2018.
3. « How do we know what's true anymore ? », YouTube, 13 avril 2018.

des réseaux de faux abonnés, de vidéos manipulées ou de publicités ciblées[4]. Cette technique est diffusée par un groupe qui vise un autre groupe et trompe les lecteurs.

4. Dans cette hiérarchie des différents modes de communication, la propagande désigne des informations qui ont un contenu programmatique spécifique et qui sont diffusées par un gouvernement, des organisations ou des individus. En novembre 2017, le Premier ministre britannique a déclaré que la diffusion de fausses nouvelles était un moyen de « transformer l'information en arme »[5]. Ces différents contenus sont souvent considérés comme des fausses nouvelles mais les moyens et les intentions diffèrent d'un type d'information à l'autre. D'un point de vue social, les fausses nouvelles contribuent à former des communautés qui ont accès aux mêmes opinions, partagent la même idéologie et les mêmes théories conspirationnistes[6].

5. Les fausses nouvelles peuvent prendre plusieurs formes : déclarations, expression d'opinions infondées ou discours haineux contre des groupes sociaux ou des minorités. L'initiative de cette manipulation de l'opinion publique peut être d'origine privée, mais certains gouvernements tentent de contrôler les médias sociaux pour façonner l'opinion publique, contrer l'opposition et désamorcer les critiques.

6. Au cours des dernières années, cette pratique, qui empêche les citoyens de prendre des décisions éclairées, s'est beaucoup répandue. L'impact de ce phénomène est d'autant plus important que sa diffusion est extrêmement rapide et que l'identification des auteurs de telles campagnes et du matériel numérique est très difficile.

7. Plusieurs facteurs expliquent le développement du phénomène des fausses nouvelles :

*L'impact des médias sociaux :* en 2016, le nombre d'utilisateurs actifs de Facebook s'élevait à 2 milliards par mois et Twitter comptait 400 millions d'utilisateurs. On compte environ 1,8 milliard d'utilisateurs mensuels de YouTube. Dans son *Digital News Report 2018*, Reuters Institute for the Study of Journalism considère que Facebook est de loin le réseau le plus important pour trouver, lire, regarder et partager des informations d'actualité, même si son utilisation est tombée de 42 % en 2016 à 36 % en 2018. Rien qu'aux États-Unis, 62 % des adultes reçoivent des informations d'actualité sur les médias sociaux[7]. Pour chaque groupe d'âge de moins de 45 ans, les actualités en ligne sont plus importantes que les actualités télévisées.

*Les méthodes et leur vitesse :* Facebook a créé un modèle de ciblage qui permet à des partis politiques d'accéder à plus de 162 millions d'utilisateurs américains pendant une campagne électorale et de les cibler individuellement par âge, sexe, district du Congrès et intérêts[8]. Il a été souligné que les médias numériques utilisent un

4. « Une approche pluridimensionnelle de la désinformation » : rapport du Groupe d'experts de haut niveau sur les fausses informations et la désinformation en ligne, Commission européenne, 12 mars 2018 (en anglais uniquement).
5. Buchan L. "Theresa May warns Russia over election meddling and vows to protect the UK", *The Independent*, 13 novembre 2017.
6. Zizek, S., « Fake News, Wohin das Auge reicht », *Neue Zürcher Zeitung*, 6 août 2018.
7. Allcott, H., Genztkow, M., « Social Media and Fake News in the 2016 Election », *Journal of Economic Perspectives*, Volume 31, 2, 2017, pp. 211-236.
8. Chester, J., "The role of digital marketing in political campaigns", Internet Policy Review, Center for digital democracy, Washington, D. C., 31 décembre 2017.

processus d'algorithme pour viser à la fois les clients et les électeurs. Des comptes robots sont créés pour influencer le discours politique. Ces comptes tweetent et retweetent en utilisant souvent des faux *likes* (j'aime) et *followers* (abonnés) pour atteindre un large public. En outre, une étude récente du Massachusetts Institute of Technology a montré que les fausses nouvelles se propagent plus rapidement que les vraies, qu'elles sont beaucoup plus susceptibles d'être retweetées que les vraies (dans une proportion de 70 %) et que les nouvelles vraies mettent environ six fois plus de temps à atteindre 1 500 personnes (par exemple) que les fausses[9].

*Les coûts :* on constate qu'ils ont baissé et qu'ils reposent sur une stratégie à court terme qui n'a pas pour objet de promouvoir la qualité. En effet, il suffit de disposer de 40 000 euros pour financer une opération de propagande sur les réseaux sociaux, de 5 000 euros pour lancer une initiative de discours haineux et de 2 600 euros pour acheter 300 000 abonnés sur Twitter[10]. Des informations fausses et préjudiciables sont produites à des fins lucratives. On a donc assisté pendant plusieurs années à un mariage entre des entreprises numériques et des entreprises de médias, et des responsables de campagnes politiques ont combiné des profils d'électeurs à des informations commerciales provenant de revendeurs de données *(data brokers)*. Cette évolution, qui a favorisé l'essor du marketing politique fondé sur l'analyse de données, peut avoir une incidence considérable sur la société, l'équité électorale et la démocratie.

8. Cette évolution soulève un certain nombre de questions. En quoi les fausses nouvelles sont-elles différentes des fausses informations qui ont été utilisées dans le passé, par exemple par les deux superpuissances pendant la guerre froide ? Les médias sociaux modifient-ils les pratiques qui sont généralement utilisées lors des campagnes électorales ? Les fausses nouvelles ont-elles eu une incidence réelle sur le résultat des élections ? Devrions-nous considérer que ces pratiques sont les effets secondaires d'une mutation technologique et qu'elles sont d'autant plus inévitables qu'elles sont difficiles à réglementer ? Devrions-nous répondre à ce phénomène en s'appuyant sur une approche fondée sur l'autorégulation ou sur la réglementation ? Quelle option choisir si l'autorégulation se révèle inefficace, en particulier lorsque les pratiques en question sont menées en dehors du territoire où se déroulent les élections ? Une approche réglementaire est-elle conforme au principe de la liberté d'expression ? Quels types d'instruments juridiques ont été introduits jusqu'à présent dans différents États membres du Conseil de l'Europe ou dans d'autres pays pour lutter contre les fausses nouvelles ? Quels enseignements tirer de ces expériences ? Comment la protection de la vie privée des citoyens est-elle garantie ? Faut-il prendre des mesures juridiques au niveau international, compte tenu des nombreux cas de déstabilisation des campagnes électorales récemment enregistrés dans divers pays ? Outre un éventuel cadre réglementaire, comment sensibiliser davantage le public à la nécessité de vérifier l'authenticité des informations et les faits, et comment l'aider à porter un jugement plus éclairé sur les contenus éditoriaux publiés dans les médias ?

9. Le présent rapport s'efforce de répondre à ces questions et de faire des propositions pour mettre en place un cadre juridique au niveau du Conseil de l'Europe.

9. http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.
10. www.assemblee-nationale.fr/15/pdf/rapports/r0990.pdf.

# 1. Aperçu général de la situation

10. La question des fausses nouvelles peut être examinée à la fois du point de vue technique et du point de vue politique.

## 1.1. Données techniques

11. Il est utile de passer en revue les diverses techniques qui peuvent être utilisées dans les médias sociaux pour mieux comprendre leur importance dans ce contexte.

12. Des études montrent que les personnes qui prennent connaissance des informations d'actualités par des algorithmes (de recherche, de détection d'agrégats sociaux et d'autres)[11] et non par des éditeurs sont plus nombreuses et que les algorithmes présentent une plus grande variété de sources en ligne à la plupart des utilisateurs. Or, les algorithmes ne sont pas neutres. Ils ont été conçus avec une précision maximale pour choisir, trier, classer, hiérarchiser, filtrer et cibler les informations disponibles ou les actualités de dernière minute. Ils constituent un moyen d'organiser les informations à grande échelle en améliorant certains aspects de celles-ci. Les algorithmes de calcul ont recours à l'apprentissage automatique pour produire un résultat. Les algorithmes d'apprentissage automatique sont utilisés comme des « généralisateurs » alimentés par des données à partir desquelles ils peuvent apprendre. L'algorithme prend ses propres décisions concernant les opérations à effectuer pour accomplir la tâche en question. Cette technique permet d'effectuer des tâches beaucoup plus complexes qu'un algorithme classique. Andrew Ng, de l'université Stanford, définit l'apprentissage automatique comme suit : « la science qui permet aux ordinateurs d'agir sans qu'ils aient à être explicitement programmés ». Il s'agit en particulier de la conception, de l'analyse, du développement et de la mise en œuvre de méthodes qui permettent à une machine de fonctionner via un processus systématique et d'accomplir des tâches difficiles.

Un véritable modèle commercial reposant sur la collecte de données monétisées et la supervision du comportement individuel en ligne a été développé[12]. Samantha Bradshaw, de l'Institut Internet d'Oxford, a expliqué aux membres de la commission chargée du numérique, de la culture, des médias et des sports de la Chambre des communes que Facebook avait le pouvoir de manipuler les émotions des individus

11. Newmann, N., "Executive Summary and Key Findings", *Reuters Institute Digital News Report, 2017*.
12. *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Commission nationale informatique et libertés, décembre 2017, https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.

en leur présentant différents types d'histoires : « Si vous leur présentez des histoires plus négatives, [les gens] seront plus négatifs. Si vous leur présentez des histoires positives, ils seront plus positifs. »[13] N'oublions pas non plus à cet égard que le terme « postvérité » a été désigné comme le mot de l'année 2016 par l'*Oxford Dictionary*. Ce terme fait référence à des circonstances dans lesquelles les faits objectifs ont moins d'influence dans la formation de l'opinion publique que les appels à l'émotion et aux opinions personnelles. L'utilisation de l'analyse de données fondée sur le profil psychologique de millions de personnes a été, par exemple, au cœur des travaux de Cambridge Analytica, une société née en 2012 et issue de SCL Group. Son objectif est de « présenter un fait qui est étayé par une émotion ».

13. L'ancien président-directeur général (PDG) de Cambridge Analytica a témoigné devant la commission susmentionnée : « Afin que le message soit adapté aux électeurs, Cambridge Analytica avait besoin d'informations sur leur comportement, par exemple les produits qu'ils achètent, les médias qu'ils lisent, les voitures qu'ils conduisent. » Au terme d'enquêtes qui ont duré environ un an, le *Guardian* a écrit ce qui suit : « [Cambridge Analytica] […] a rémunéré des chercheurs de l'université de Cambridge pour recueillir des profils psychologiques détaillés sur l'électorat américain à partir d'un groupe d'utilisateurs américains de Facebook créé principalement à leur insu au moyen d'un sondage en ligne. »[14] Les candidats qui veulent cibler les électeurs et diffuser des messages à leur intention utilisent des outils adaptés qui permettent de faire un « microciblage » de groupes spécifiques. L'expression « publicités occultes » a également été utilisée pour décrire cette technique.

14. Les experts utilisent l'expression « chambre d'écho politique » comme métaphore pour désigner les « clics » en ligne qui finissent par créer une « bulle » politique dans laquelle les gens peuvent s'installer tout en utilisant les services en ligne. Voici un exemple de la façon dont les flux d'algorithmes encouragent les partis pris : « Si vous lisez des sources d'information libérales, ou si vous avez des amis de tendance libérale, Facebook vous présentera des informations d'actualités plus libérales. Même chose pour les conservateurs, voire les membres les plus marginaux du spectre politique. Bref, cette orientation confirmée par un algorithme signifie que plus vous lisez d'informations qui vous conviennent, plus Facebook vous présentera des informations qui vous conviennent… Plus vous entendez les mêmes points de vue issus des mêmes sources, plus vous confortez vos idées sans jamais les remettre en question. »[15]

15. Cependant, les données et les algorithmes « sont opaques ; en effet, celui qui est destinataire des données de sortie (résultat) de l'algorithme ne sait pas concrètement comment ou pourquoi il a été classé comme tel à partir des données d'entrée. En outre, les données d'entrée elles-mêmes peuvent être totalement inconnues ou connues seulement partiellement[16] ». Stirista, une société de marketing numérique, propose une modélisation de ce type pour détecter les personnes qui sont des partisans et électeurs potentiels. La société affirme qu'elle a mis en correspondance 155 millions d'électeurs avec leurs « adresses électroniques, cookies en ligne et pseudonymes »,

13. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.
14. *Ibid*.
15. https://lifehacker.com/how-sites-like-google-and-facebook-put-you-in-political-1787659102.
16. Burrell, J., « "How the machine thinks": Understanding opacity in machine learning algorithms », *Big Data and Society*, janvier 2016, pp. 1-12.

mais aussi avec « leur culture, leur religion, leurs intérêts, leurs opinions politiques et des centaines de points de données qui lui ont permis de créer des profils d'électeurs riches et détaillés »[17]. Les convictions politiques d'un électeur ne peuvent pas toujours être façonnées par des algorithmes mais ceux-ci peuvent être utilisés pour déterminer son profil. Cette pratique fait désormais partie intégrante d'un modèle commercial parce que c'est un moyen de gagner de l'argent.

16. L'opacité des algorithmes soulève deux questions : le résultat est-il dû à la volonté du concepteur de la plateforme ? Est-il observable par un utilisateur ? Certains effets indésirables des algorithmes ont été délibérément programmés sans que les utilisateurs le sachent. Dans ces cas de figure, l'opacité est une stratégie délibérée consistant à manipuler des consommateurs ou des électeurs à leur insu. Il appartient aux programmeurs, aux autorités publiques, aux organisations non gouvernementales (ONG) et aux journalistes de vérifier ces algorithmes et de détecter leurs cibles cachées. Dans d'autres cas, les effets n'ont peut-être pas été programmés par les opérateurs et ils peuvent avoir été détectés, ou non, par les utilisateurs[18].

17. Un « bot » (robot social) est un autre mécanisme de pression sophistiqué permettant d'influencer les électeurs. Il s'agit d'un logiciel automatisé qui imite le comportement humain sur les médias sociaux en publiant des informations, en affichant son approbation *(like)* et en s'adressant à des personnes réelles[19]. Selon un expert allemand, « [l]es robots sociaux sont des faux comptes qui sont créés dans les médias sociaux et veulent se faire passer pour des personnes réelles »[20]. Une personne qui contrôle un seul « bot » peut donc exercer une influence sur un million de personnes. Les « bots », par exemple, peuvent polariser l'opinion publique en diffusant des discours haineux. Lors de la même audition devant la commission de la stratégie numérique du Bundestag, l'expert a considéré que les « bots » étaient des techniques caractérisées par les critères suivants : « qualité faible, fréquence élevée, manipulation », tandis que certaines fausses nouvelles sont associées aux critères « grande qualité, fréquence faible, manipulation »[21]. D'après les estimations du fournisseur de services « cloud » Imperva Incapsula, les « bots » représentaient 51,2 % de l'ensemble du trafic internet en 2016. Beaucoup d'entre eux ont une finalité commerciale, mais les « bots » malveillants ne sont pas identifiables et peuvent être utilisés pour le piratage, l'envoi massif de messages commerciaux *(spamming)* et le vol de contenus[22].

18. Dans le cadre de la loi électorale britannique, les candidats peuvent acheter des « bots » et payer des personnes qui diffuseront leurs messages de campagne, ce qui est d'autant plus trompeur que cela se produit à l'insu des électeurs[23].

---

17. Chester, J., *op. cit*.
18. Cardon, D., « Le pouvoir des algorithmes », *Pouvoirs,* 164, *La Datacratie*, 2018.
19. *Digital campaigning*: *Increasing transparency for voters*, The Electoral Commission, juin 2018.
20. Hegelich, S., *Ausschuss Digitale Agenda*, Hochschule für Politik München, Deutscher Bundestag Auschussdrucksache, 18, 24, p. 125.
21. « Fake News, Social Bots, Hacks und Co-Manipulationsversuch demokratischer Willensbildungsprozesse im Netz », Wortprotokoll der 81 Sitzung, 25 janvier 2017, Deutscher Bundestag.
22. Freedom on the Net 2017, « Manipulating social media to undermine democracy ».
23. *Digital campaigning, Increasing transparency for voters*, *op. cit.*

19. Un « troll » est une personne réelle qui consacre du temps sur l'internet et les médias sociaux à diffuser des messages et des commentaires clivants ou non pertinents pour agacer ou irriter d'autres personnes[24].

20. Les hashtags sont des codes courts insérés dans les messages afin de faciliter leur consultation. Leur utilisation pendant les campagnes électorales a été signalée. Les hashtags les plus répandus contiennent des « sujets tendance » qui sont l'objet de conversations. Ils sont manipulés par des « bots ». Les hashtags reproduits reflètent l'avis d'un très petit nombre de personnes qui ont un grand nombre de comptes, ce qui donne ainsi l'impression qu'ils sont très nombreux. Des codes courts et simples laissent croire qu'une opinion est largement répandue[25].

21. En 2011, les dépenses des candidats en publicité numérique se sont élevées à 0,3 % du total des dépenses publicitaires au Royaume-Uni. En 2017, ces dépenses ont atteint 42,8 % du total des dépenses publicitaires[26].

## 1.2. Données politiques

22. Les médias sociaux ont été félicités pour avoir mis à disposition des informations démocratiques et pour avoir favorisé la discussion en ligne. Les informations de nature politique sont ainsi plus accessibles et aident les électeurs à faire des choix plus éclairés. Dans son arrêt du 10 mars 2009, dans l'affaire *Times Newspaper LTD c. Royaume-Uni*, la Cour européenne des droits de l'homme a déclaré que « [grâce] à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information[27] ». Cependant, les médias sociaux peuvent également être utilisés à mauvais escient et avoir une incidence sur les convictions politiques.

23. Afin d'évaluer l'influence des réseaux de faux comptes et de « bots » sur les votes, des recherches ont été menées sur les campagnes électorales américaines, le référendum sur le maintien du Royaume-Uni dans l'Union européenne en 2016, les élections présidentielles en France, les élections générales britanniques et allemandes en 2017, et l'élection présidentielle tchèque en 2018.

24. Lors des élections présidentielles de 2008 et de 2012, les équipes de campagne de Barack Obama ont disposé de dizaines de séries de données sur quasiment tous les électeurs. Il est généralement admis que les fausses nouvelles ont peut-être contribué au succès de l'élection de Donald Trump à l'élection présidentielle américaine de 2016. Les médias sociaux représentaient 13,8 % des sources d'information sur les élections de 2016. Les fausses nouvelles ont été partagées et penchaient fortement en faveur de Donald Trump. Une base de données analysée par une source contient 115 fausses informations pro-Trump qui ont été partagées 30 millions de fois sur Facebook et 41 fausses informations pro-Clinton partagées 7,6 millions de

24. *Ibid.*
25. « L'histoire vraie des *fake news* », *op. cit.*
26. *Digital campaigning: Increasing transparency for voters*, *op. cit.*
27. Paragraphe 27 de l'arrêt.

fois[28]. Une de ces fausses informations indiquait que le pape soutenait le candidat Donald Trump. Plus généralement, les publicités de Facebook ont été déterminantes dans la victoire de Donald Trump. Lors de sa campagne présidentielle, le candidat républicain a dépensé la plus grande partie de son budget publicitaire numérique sur Facebook. Il a envoyé 5,9 millions de messages à des électeurs ciblés, tandis que Hillary Clinton n'a envoyé que 66 000 messages[29]. Si cette stratégie n'a pas vraiment compté dans quelques États indécis, on peut néanmoins penser qu'elle a eu un impact décisif sur l'élection présidentielle américaine.

25. Selon le rapport intérimaire susmentionné de la commission chargée du numérique, de la culture, des médias et des sports de la Chambre des communes sur la désinformation et les fausses nouvelles publiées le 29 juillet 2018 : « Lors des élections présidentielles, les Russes ont diffusé plus de 3 000 annonces publicitaires sur Facebook et Instagram pour promouvoir 120 pages Facebook dans une campagne qui a atteint 126 millions d'Américains. »[30] Lors des auditions du mois d'avril 2018 devant le Congrès américain, Mark Zuckerberg, PDG de Facebook, a expliqué que les comptes russes utilisaient des publicités plutôt pour influencer l'opinion sur des questions précises que pour défendre des candidats spécifiques ou faire passer des messages politiques.

26. Concernant le référendum de 2016 sur le maintien du Royaume-Uni dans l'Union, les chercheurs qui participaient à un projet de recherche conjoint des universités de Swansea (Royaume-Uni) et de l'université de Californie à Berkeley (États-Unis) ont repéré 156 252 comptes russes qui tweetaient sur le Brexit et constaté qu'ils avaient publié plus de 45 000 messages sur le Brexit durant les dernières 48 heures de la campagne[31]. Selon un rapport du groupe 89up, entre le 1er janvier et le 23 juin 2016, l'agence de communication Russia Today (RT) et Sputnik ont publié 261 articles anti-Union sur le référendum du maintien dans l'Union. Le rapport a également montré que RT et Sputnik avaient plus de contacts pro-Brexit sur Twitter que pour les mouvements Vote Leave ou Leave[32].

27. Dans le cas des élections présidentielles en France en 2017, une étude a révélé des modes d'utilisation anormaux de comptes, ce qui laisse entendre qu'il existe un marché noir de « bots » de désinformation politique réutilisables[33]. Sur la base de 17 millions de messages recueillis, il est apparu que les utilisateurs qui avaient participé aux Macron Leaks (fuites de courriers concernant Emmanuel Macron) étaient plutôt des étrangers ayant un intérêt préexistant pour les sujets de la droite alternative et des médias alternatifs que des utilisateurs français ayant des opinions politiques diverses.

28. S'agissant des élections générales britanniques de 2017, un rapport publié dans le cadre du projet de l'Oxford Internet Institute sur la propagande informatique

28. Allcott, H., Genztkow, M., *op. cit.*, pp. 211-236.
29. « L'histoire vraie des *fake news* », *op. cit.*
30. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm.
31. « Putin's Brexit? The influence of Kremlin media and bots during the 2016 UK EU referendum », 89up, février 2018.
32. « Russian Twitter accounts promoted Brexit ahead of EU referendum », Reuters, 15 novembre 2017.
33. Ferrara, E., "Disinformation and social bot, operations in the run-up to the 2017 French Presidential Election", *First Monday*, 22, 8, 2017.

a considéré que les *junk news* sont des « informations trompeuses, mensongères ou incorrectes qui ont l'apparence d'informations authentiques sur la politique, l'économie et la culture » et qu'elles constituaient 11,4 % des contenus partagés[34].

29. Si l'on examine les effets des fausses nouvelles sur les élections générales en Allemagne en 2017, on note que celles qui sont d'origine étrangère ont joué un rôle limité. La plupart d'entre elles ont été diffusées par l'extrême droite. La priorité n'a pas été systématiquement accordée aux médias sociaux, mais les médias classiques ont également été utilisés. Les fausses nouvelles étaient axées principalement sur deux thèmes : les réfugiés et la criminalité. Par rapport aux États-Unis, le rôle limité des médias sociaux dans les canaux d'information en Allemagne peut expliquer le faible impact des fausses nouvelles. Pour l'essentiel, les fausses nouvelles ont visé des batailles rangées au cours desquelles un millier de migrants se seraient affrontés dans une petite ville de Bade-Wurtemberg. Ces fausses nouvelles ont été partagées par 500 000 personnes[35].

30. D'après les éléments de preuve fournis par de nombreux articles « tendance » publiés sur des pages Facebook, le rôle de l'influence étrangère et de la désinformation lors de la dernière élection présidentielle tchèque en 2018 a été souligné[36].

31. Certains observateurs estiment que cette expression de la désinformation mérite d'être mise en perspective. En effet, il s'agit d'une pratique qui a toujours existé parce qu'elle fait partie intégrante du débat politique. Au XIX$^{e}$ siècle, le chancelier Otto von Bismarck a déclaré que les gens ne mentaient jamais autant qu'après une chasse, pendant une guerre ou avant une élection. Il existe par ailleurs des exemples historiques patents de mensonges politiques à presque toutes les époques. On peut citer par exemple la Roumanie du V$^{e}$ siècle, la France du XVII$^{e}$ siècle et l'Allemagne du XIX$^{e}$ siècle, ainsi que dans le monde entier au XX$^{e}$ siècle[37].

## 1.3. Intensification du processus

32. Les effets de la désinformation varient d'un pays à l'autre, mais la propagation rapide du phénomène, sa sophistication technique en termes de rapidité, d'échelle et d'extraterritorialité, le fait qu'il soit considéré comme inoffensif par la société et ses besoins de financement relativement limités sont autant de changements de grande ampleur et de menaces non seulement pour le processus électoral, mais aussi pour nos démocraties en général. Le groupe de consultation et de recherche Gartner

34. www.niemanlab.org/2017/06/brits-and-europeans-seem-to-be-better-than-americans-at-not-sharing-fake-news/.
35. Sängerlaub, A., Meier, M., Dieter-Rühl, W., « Fakten statt Fakes », Stiftung für Neue Verantwortung, mars 2018.
36. www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-Czech-presidential-elections.pdf.
37. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/85595.html. Voir aussi Huyghe, F.-B., « Désinformation : armes du faux, lutte et chaos dans la société de l'information », *Sécurité globale*, 6, 2016, p. 64.

estime que, d'ici à 2020, l'intelligence artificielle sera un outil de désinformation qui dépassera l'intelligence artificielle utilisée pour la détecter[38].

33. Beaucoup d'eau a coulé sous les ponts depuis l'adoption en 2016 d'une résolution du Parlement européen sur la communication stratégique de l'Union pour contrecarrer la propagande dirigée contre elle par des tiers[39].

34. De plus en plus de pays sont concernés. Dans son rapport pour 2017, Freedom on the Net a réalisé une étude complète de la liberté d'internet dans 65 pays, soit 87 % des utilisateurs du réseau dans le monde. L'ONG a pris note de la prédominance des « bots politiques » dans 20 pays, de la pratique consistant à diffuser des fausses nouvelles durant les périodes électorales dans 16 pays et de l'utilisation de comptes détournés dans 10 pays. Dans les 20 pays cités, l'examen des schémas caractéristiques des activités en ligne semblait indiquer que des « bots » avaient été utilisés de façon coordonnée pour influencer le discours politique[40].

35. Il paraît évident que les cas susmentionnés d'influence des médias sociaux sur les campagnes électorales dans les démocraties occidentales ne sont pas isolés. Ainsi, le projet de recherche sur la propagande informatique de l'université d'Oxford[41] a permis d'apporter des preuves que des campagnes formelles de manipulation avaient été orchestrées par des médias sociaux dans 48 pays en 2018 (contre 28 l'année précédente). Dans chaque pays, il existe au moins un parti politique ou un organisme gouvernemental qui utilise les médias sociaux pour manipuler l'opinion publique à l'échelle nationale. Les petits pays où les électeurs sont moins éduqués peuvent être plus vulnérables aux *junk news* et à la désinformation que les grands pays où la population est plus instruite et où le journalisme est de qualité.

36. Les opérations de désinformation numérique ont une incidence plus grande sur les électeurs que les techniques classiques. On peut s'attendre à une augmentation de ces pratiques, car elles permettent, par rapport aux techniques classiques, d'atteindre un public plus large. Les partisans des hommes politiques contribuent à cette tendance. Avant l'avènement du numérique, les militants politiques qui partageaient les mêmes convictions auraient passé beaucoup plus de temps à entrer en contact avec les électeurs : ils auraient fait du porte-à-porte pour recueillir des informations et convaincre les gens de voter.

37. Les techniques conçues par les revendeurs de données pour comprendre le profil psychologique des électeurs (voir ci-dessus) sont beaucoup plus invasives que par le passé, en raison de l'utilisation des algorithmes et des moteurs de recherche.

38. Il semblerait que les algorithmes renforcent la tendance des individus à ne s'intéresser qu'aux objets, personnes, opinions et cultures qui correspondent à leurs intérêts. Le rapport de l'Autorité nationale française de protection des données

38. « Gartner reveals Top Predictions for IT Organisations and Users in 2018 and Beyond », press release, 3 octobre 2017.
39. 23 novembre 2016 (2016/2030(INI)), paragraphe 52 : « Le Parlement européen estime qu'il convient d'accorder une attention particulière aux nouvelles technologies – y compris la diffusion numérique, les communications mobiles, les médias en ligne et les réseaux sociaux, notamment à caractère régional – qui facilitent la diffusion des informations […]. »
40. Freedom on the Net 2017, *Manipulating social media to undermine democracy, 2018*, Freedom House.
41. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

personnelles publié en décembre 2017 sur les questions éthiques soulevées par les algorithmes et l'intelligence artificielle concluait, notamment, que la personnalisation de l'information pouvait conduire à une fragmentation extrême de l'espace public, à la disparition d'un ensemble minimal d'informations de base partagées par les personnes et à une atomisation de la communauté politique.

39. Il soulève également la question du droit à la vie privée. Dans des pays comme les États-Unis, en raison du premier amendement qui garantit la liberté d'expression, l'utilisation des données politiques n'est pas protégée. À cet égard, contrairement aux États-Unis, les pays européens ont élaboré des règles générales de confidentialité qui pourraient être utilisées pour intensifier les efforts de lutte contre la désinformation.

40. Les techniques numériques changent très rapidement et continuent d'évoluer. Les dégâts causés par les fausses nouvelles sont mineurs par rapport à ceux qui pourraient découler des *deep fakes*. Il s'agit d'une technique qui permet d'utiliser l'intelligence artificielle pour imiter des voix et des images afin de créer des réalités alternatives. Une personne, par exemple, peut sembler dire ou faire des choses qu'elle n'a jamais dites ou faites. Pour créer des formes élémentaires de *deep fakes*, il suffit de fournir des images et des sons d'une personne à un ordinateur et de lui donner des instructions pour qu'il apprenne à imiter sa voix[42].

41. Il faut entre douze et quarorze heures pour nier une rumeur qui continue de circuler sur Twitter[43]. L'impact des *junk news* à la veille d'un jour de scrutin peut donc être dévastateur.

42. Le relativisme augmente dans nos sociétés. Cela signifie que le vrai et le faux, le bien et le mal, les logiques de raisonnement et les procédures de justification sont considérés comme des produits issus de conventions et de cadres d'évaluation divergents. Leur autorité se limite au contexte qui les suscite[44]. Ce point a été souligné par le philosophe Slavoj Zizek pour expliquer l'évolution du phénomène des fausses nouvelles, qui est lié au travail de déconstruction postmoderne et qui ne permet pas à l'individu de faire la différence entre des vraies et des fausses nouvelles[45]. Lorsque Donald Trump a été interrogé par la journaliste Lesley Stahl (il s'agissait du premier entretien télévisé de Donald Trump après son élection à la présidence en 2016), le président américain a déclaré qu'il agressait la presse pour « dévaloriser » et « discréditer » les journalistes afin que personne ne croie aux informations négatives véhiculées à son sujet[46]. Cette stratégie délibérée, dans un contexte de méfiance envers les journalistes, crée un climat qui joue sur les peurs et les préjugés des individus afin d'influencer leur comportement et contribue à déstabiliser les électeurs qui perdent leurs points de repère.

43. L'utilisation croissante d'outils numériques dans les campagnes politiques a un impact financier important qui doit être pris en compte.

---

42. https:// whatis.techtarget.com/ definition/deepfake.
43. Rapport n° 677 (2017-2018) de Catherine Morin-Desailly, fait au nom de la commission de la culture, de l'éducation et de la communication du Sénat français, déposé le 18 juillet 2018.
44. https://plato.stanford.edu/entries/relativism/.
45. Zizek, S., *op. cit.*
46. https://www.cnbc.com/2018/05/22/trump-told-lesley-stahl-he-bashes-press-to-discredit-negative-stories.html.

Tous les États membres du Conseil de l'Europe ont adopté des règlements sur le financement politique conformément à la Recommandation Rec(2003)4 du Comité des Ministres aux États membres sur les règles communes contre la corruption dans le financement des partis politiques et des campagnes électorales. Les règles portent sur les limites des dépenses, la transparence des ressources, le contrôle et les sanctions. Ce cadre juridique a été mis en œuvre progressivement sous l'impulsion du Groupe d'États contre la corruption (GRECO).

Dans la plupart des États membres, les règles juridiques actuelles en matière de financement des campagnes n'exigent pas l'inclusion de matériel numérique et, si les dons étrangers faits à des partis politiques ou à des candidats sont interdits, aucune règle n'interdit explicitement les dépenses à l'étranger.

Au Royaume-Uni, des préoccupations ont été exprimées quant au financement des outils numériques largement utilisés au cours de la campagne référendaire sur la sortie du pays de l'Union (groupe « Vote Leave »). Le plafond des dépenses autorisées pendant cette campagne était de 7 millions de livres sterling. Arron Banks, qui est considéré comme proche des groupes d'intérêts russes, aurait donné 8,4 millions de livres sterling à la campagne en faveur du « Leave », le don le plus important jamais accordé à un parti politique au Royaume-Uni. L'origine de cet argent reste incertaine. Les dons de sources clandestines[47] faits pour influencer une campagne électorale ainsi que les campagnes électorales numériques menées de l'étranger pour influencer les électeurs fragilisent encore davantage les règles du financement des partis politiques fondées sur la transparence et peuvent même les rendre totalement inefficaces.

## 1.4. Réponses possibles

44. Le statut juridique d'un fournisseur de services internet doit être précis au regard du droit de l'Union. À cet égard, l'article 14 de la Directive 2000/31/CE[48] donne des informations détaillées sur les responsabilités d'un fournisseur de services. Il doit être interprété comme signifiant que la règle énoncée s'applique à un fournisseur de services internet qui n'a pas joué un rôle actif, c'est-à-dire qui n'a pas cherché à prendre connaissance des données stockées ou à les contrôler. S'il n'a pas joué ce rôle, le fournisseur ne peut pas être tenu responsable des données qu'il a stockées à la demande d'un annonceur. En revanche, sa responsabilité est engagée s'il a eu connaissance du caractère illicite de ces données ou des activités de cet annonceur

47. Paragraphe 191 de l'Interim Report : https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

48. « 1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :
   a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ; ou
   b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.
   2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire. »

et s'il a omis de prendre rapidement des mesures pour supprimer ou désactiver l'accès aux données concernées[49]. En conséquence, un fournisseur d'accès comme Facebook ne doit supprimer un message illégal que s'il connaît son contenu. Dans une communication du 28 septembre 2017 sur la lutte contre le contenu illégal en ligne en vue de renforcer la responsabilité des plateformes en ligne, l'Union européenne a esquissé une approche européenne qui essaie de combiner la nécessité de supprimer rapidement et efficacement un contenu illégal, et celle de prévenir et de poursuivre des infractions avec l'obligation de sauvegarder le droit à la liberté d'expression en ligne[50]. Le 1er mars 2018, la Commission a publié une recommandation sur les mesures visant à lutter efficacement contre les contenus illicites en ligne, que nous examinerons en détail au point 97[51].

45. Dans le cadre de la lutte contre la pratique de la diffusion de fausses informations, deux options sont possibles : l'une est fondée sur l'autorégulation, l'autre sur la réglementation légale.

### 1.4.1. Autorégulation

46. Les praticiens plaident pour l'autorégulation : Facebook et Twitter ont annoncé le lancement d'initiatives internes visant à fournir aux citoyens davantage de moyens et d'informations leur permettant de déterminer quelles organisations ou personnes ont payé pour des publicités politiques et qui sont les cibles prévues.

47. En janvier 2018, la Commission européenne a mis en place le Groupe d'experts de haut niveau sur les fausses informations et la désinformation en ligne chargé de donner des avis sur les initiatives politiques pour lutter contre les fausses nouvelles et les fausses informations diffusées en ligne. La principale réalisation du groupe d'experts est un rapport dont le but était d'examiner les meilleures pratiques à la lumière des principes fondamentaux et des réponses appropriées découlant de ces principes[52]. Ce rapport a été présenté dans les termes suivants, censés donner un aperçu de son contenu : « une bonne dose d'éthique, un soupçon de responsabilité »[53].

48. L'approche multidimensionnelle recommandée par le groupe d'experts repose sur un certain nombre de réponses qui sont interdépendantes, se renforcent mutuellement et reposent sur cinq « piliers » conçus pour :

1. améliorer la transparence des actualités en ligne, notamment en garantissant un partage adéquat et conforme à la vie privée des données relatives aux systèmes qui permettent leur diffusion en ligne ;

49. Arrêt de la Cour de justice des Communautés européennes (Grande Chambre) du 23 mars 2010, *Google France SARL et Google Inc. c. Louis Vuitton Malletier SA* (C-236/08), *Google France SARL c. Viaticum SA et Luteciel SARL* (C-237/08), et *Google France SARL c. Centre national de recherche en relations humaines (CNRRH) SARL et autres* (C-238/08).

50. https://ec.europa.eu/digital-single-market/fr/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.

51. https://ec.europa.eu/digital-single-market/fr/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

52. https://ec.europa.eu/digital-single-market/fr/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

53. Bensamoun, A., « Stratégie européenne sur l'intelligence artificielle : toujours à la mode éthique », *Recueil Dalloz*, 2018, n° 19, p. 1022.

2. promouvoir l'éducation aux médias et à l'information pour lutter contre la désinformation et aider les utilisateurs à naviguer dans l'écosystème des médias numériques ;
3. mettre au point des outils permettant aux utilisateurs et aux journalistes de lutter contre la désinformation et de s'engager de façon positive en faveur des technologies de l'information qui évoluent rapidement ;
4. préserver la diversité et la pérennité de l'écosystème européen des médias d'information ; et
5. encourager les chercheurs à poursuivre leurs travaux sur l'incidence de la désinformation en Europe afin d'évaluer les mesures prises par les différents acteurs et d'adapter constamment les réponses nécessaires.

49. Dans la perspective des prochaines élections européennes de mai 2019, l'Union européenne s'est déclarée préoccupée par les risques éventuels de désinformation avant le jour du scrutin. Le 26 avril 2018, elle a proposé un code de bonnes pratiques sur la désinformation à l'échelle de l'Union. La Commission devait évaluer sa mise en œuvre dans le cadre d'une large consultation avec les parties prenantes et sur la base d'indicateurs de performance clés fondés sur ses objectifs. Si les résultats ne sont pas satisfaisants, la Commission pourrait présenter d'autres mesures, y compris des mesures de nature réglementaire. Elle prévoit de soutenir la création d'un réseau européen indépendant de vérificateurs de faits afin d'établir des méthodes de travail communes, d'échanger les meilleures pratiques, d'assurer une couverture géographique aussi large que possible dans l'ensemble de l'Union et de participer à des activités conjointes de vérification de faits et à des activités connexes. Elle vise également à améliorer l'obligation, pour les fournisseurs d'accès, de rendre compte, et la transparence des activités en ligne, et à tirer profit des nouvelles technologies pour lutter contre la désinformation à long terme. La Commission attire l'attention sur la nécessité de renforcer la capacité des sociétés à résister à la désinformation. Son rapport sur les progrès accomplis dans ce domaine devrait être publié d'ici au mois de décembre 2018.

50. En ce qui concerne ces initiatives, deux propositions méritent d'être étudiées : les activités des plateformes en ligne et la vérification des faits.

51. Concernant les activités des plateformes en ligne, le groupe d'experts nous rappelle que les réseaux publicitaires exploités par les plateformes elles-mêmes ou par d'autres parties jouent un rôle important dans leur stratégie et qu'il poursuit les trois objectifs suivants :

- les réseaux publicitaires refusent d'afficher des publicités sur des sites internet considérés comme des fournisseurs de désinformation, ce qui réduit directement les revenus de ces derniers ;
- les fournisseurs de publicités excluent les publicités provenant de sources de désinformation et indiquent clairement que les publicités politiques sont du contenu parrainé afin de créer de la transparence ; et
- les réseaux publicitaires ne distribuent de revenus aux sites et aux partenaires que s'ils sont en mesure de confirmer qu'ils respectent des conditions pertinentes.

52. En août 2018, Facebook a investi dans des publicités à l'échelle mondiale proclamant que « les faux comptes ne sont pas nos amis ». Cependant, le rapport de la commission de la Chambre des communes (voir *supra*) indique que les graves défaillances des activités de l'entreprise qui ont débouché sur une manipulation de données, la production d'informations erronées et un niveau élevé de désinformation se sont de nouveau produites[54]. Devant les commissions des affaires juridiques et de la culture du Sénat français, un responsable de Google France a fait savoir que son organisation avait lancé de nombreuses initiatives contre la désinformation en ligne, en particulier la suppression de la publicité utilisée pour diffuser de fausses nouvelles, la mise en œuvre du principe consistant à « suivre l'argent » dans la lutte contre la désinformation, et la modification des références des algorithmes liés à des événements[55]. Facebook et Twitter ont promis de créer des archives que le public pourra utiliser pour consulter des publicités politiques[56]. Pour les élections américaines de mi-mandat de 2018, les sociétés Facebook, Google et Twitter ont déclaré qu'elles vérifieront que les candidats résident bien aux États-Unis et qu'elles publieront des bases de données sur les publicités politiques qu'elles ont diffusées moyennant paiement[57]. Facebook a retiré 32 comptes et pages sur sa plateforme concernant les prochaines élections de mi-mandat au Congrès américain[58]. Elle a créé des réseaux de faux comptes et d'événements, et a utilisé des réseaux pour détecter et neutraliser les « mauvais acteurs ». Enfin, 652 pages créées en Iran et diffusant des messages pro-iraniens ont été bloquées[59].

53. La vérification des informations par des entités internet de vérification des faits (telles que Snopes.com) devrait être renforcée. Par exemple, le directeur de Pagella Politica[60], une organisation italienne indépendante de vérification des faits, souligne les efforts de sa structure : « Lorsque nous trouvons un article qui est manifestement faux, nous écrivons un texte vérifiant les faits qui est publié dans une section spécifique ou sur notre site internet et nous fournissons son lien vers Facebook[61]. » Le code de principes du Réseau international de vérification des faits (IFCN – International Fact-Checking Network) doit également être cité. Le Centre allemand de recherche sur l'intelligence artificielle (Deutsche Forschungszentrum für künstliche Intelligenz GmbH-DFKI) développe, par exemple, une application pour détecter les fausses images qui sont utilisées pour fournir de fausses informations et qui ont été initialement publiées dans un contexte tout à fait différent[62].

Il faut cependant garder à l'esprit que, chaque jour, des centaines de millions d'informations circulent sur l'internet. Il paraît évident que les vérificateurs de faits ne parviendront à en traiter qu'une fraction, car leurs capacités de traitement ne correspondent pas aux besoins, même si ces vérificateurs ne travaillent pas que pour

54. Paragraphe 133 : https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.
55. Rapport n° 677 (2017-2018) de Catherine Morin-Desailly, *op. cit.*
56. Chester, J., *op. cit*.
57. « Digital campaigning, Increasing transparency for voters », *op. cit.*
58. « Facebook deckt neue gefälschte Konten auf », *Neue Zürcher Zeitung*, 2 août 2018.
59. « "Fake News": la tech américaine orchestre sa réplique », *Les Échos*, 23 août 2018.
60. https://pagellapolitica.it.
61. https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/.
62. *DFKI Newsletter*, 40, 2017.

un opérateur comme Facebook et proposent leurs services à d'autres plateformes en ligne. Il existe manifestement un fort déséquilibre entre ceux qui supervisent les algorithmes et les données, et les personnes qui en sont l'objet. Il existe également un déséquilibre entre les ressources humaines qui « pilotent » la désinformation et le nombre de personnes qui la détectent. Par exemple, une équipe spéciale East StratCom a été créée en septembre 2015 dans le cadre du Service européen pour l'action extérieure[63]. Cette équipe, qui s'appuie sur des bénévoles pour recueillir des exemples de désinformation, manque notoirement d'effectifs. Un rapport de mars 2018 du Conseil de l'Atlantique Nord recommandait que l'Union demande à tous les États membres de détacher un expert national pour la renforcer[64].

54. En conclusion, force est de constater que l'autorégulation n'est pas une solution totalement satisfaisante.

### 1.4.2. Réglementations

55. Les dispositions réglementaires ne peuvent pas, d'un point de vue juridique, nuire à la libre prestation de services et à la liberté d'expression.

#### 1.4.2.1. Libre prestation de services

56. En ce qui concerne les règles de l'Union, des restrictions d'intérêt général peuvent être apportées pour garantir la libre prestation de services destinés à protéger les consommateurs[65].

#### 1.4.2.2. Liberté d'expression

57. Plusieurs pays ont adopté des propositions de loi qui permettront aux gouvernements de poursuivre les personnes soupçonnées de diffuser de « fausses » informations sur internet. C'est le cas, notamment, de la Malaisie en avril 2018 et du Bélarus en juin 2018[66]. Cependant, le contexte dans lequel s'inscrit le principe de la liberté d'expression rend irréaliste un recours éventuel à la censure en Europe. Toute proposition en ce sens serait rapidement assimilée à l'instauration d'un « ministère de l'information » ou d'un « ministère de la vérité »[67]. Cet argument a été avancé lors d'un débat parlementaire contre une proposition de loi déposée par le Parti populaire au Congrès des députés de l'Espagne le 17 juillet 2018. Le Congrès a rejeté cette proposition qui visait à renforcer les capacités de surveillance des services de renseignement en matière de désinformation.

63. https://euvsdisinfo.eu/news.
64. www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation.
65. *Commission c. France*, 22 octobre 1998, C-184/96.
66. « Lukaschenkos Schlag gegen den Journalismus », *Neue Zürcher Zeitung*, 10 août 2018.
67. Reuter, M., « Stellungsnahme Auschuss Digitale Agenda », Deutscher Bundestag, Netzpolitik.org.

58. En Europe, la liberté d'expression est consacrée par l'article 10 de la Convention européenne des droits de l'homme[68] et par l'article 11 de la Charte des droits fondamentaux de l'Union européenne[69]. Dans l'affaire *Handyside c. Royaume-Uni* du 7 décembre 1976, la Cour européenne des droits de l'homme a considéré que la liberté d'expression s'appliquait non seulement aux « informations » et aux « idées » qui sont reçues de manière favorable ou considérées comme inoffensives ou indifférentes, mais également à celles qui offensent, choquent ou dérangent l'État ou tout groupe social. À ce titre, elle s'inscrit dans le cadre du pluralisme, de la tolérance et de l'esprit d'ouverture sans lesquels il n'existe pas de « société démocratique ». Cela signifie, entre autres, que toute « formalité », « condition », « restriction » ou « sanction » imposée dans ce domaine doit être proportionnée à l'objectif légitime poursuivi. Dans un autre arrêt[70], la Cour de Strasbourg a estimé que, dans les campagnes électorales, la diffusion d'informations devait avoir lieu même si ces informations peuvent être considérées comme fausses. L'article 10 de la Convention en tant que tel n'interdit pas la discussion ou la diffusion d'informations reçues, même s'il existe une forte probabilité que ces informations ne soient pas véridiques. Suggérer le contraire priverait les personnes du droit d'exprimer leurs vues et opinions sur les déclarations faites dans les médias et limiterait ainsi de manière déraisonnable la liberté d'expression garantie à l'article 10 de la Convention.

59. La Cour européenne des droits de l'homme veille à ne pas apporter son soutien à des mesures qui pourraient entraîner des abus, par exemple en ce qui concerne les ordres de blocage : en effet, bloquer l'accès à des sites d'hébergement, des sites de tierces parties et des sites internet qui font l'objet de poursuites rend l'information inaccessible et limite de ce fait les droits des internautes. Cette ingérence n'avait pas été considérée comme prévisible et n'avait pas accordé au requérant le degré de protection qui lui était garanti par l'État de droit dans une société démocratique[71]. De même, bloquer l'accès d'un utilisateur à YouTube sans base légale porte atteinte au droit de recevoir et de communiquer des informations[72].

60. Les États membres du Conseil de l'Europe ont l'obligation positive d'assurer l'efficacité de la liberté d'expression : ils sont tenus de créer un environnement favorable à la participation de toutes les personnes concernées au débat public et de

---

68. « Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.
L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »
69. « Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières. »
70. *Salov c. Ukraine*, 6 septembre 2005, 655118/01.
71. *Ahmet Yildirim c. Turquie*, 18 décembre 2012, 3111/10.
72. *Cengiz et autres c. Turquie*, 1er décembre 2015, 48226/10 et 14027/11.

leur permettre d'exprimer leurs opinions et leurs idées sans crainte. L'État ne doit pas uniquement s'abstenir de toute ingérence dans la liberté d'expression de l'individu, il a également l'« obligation positive » de protéger son droit à la liberté d'expression contre toute attaque, y compris de la part de particuliers[73].

61. L'existence de faits peut être démontrée tandis que la véracité d'un jugement de valeur ne peut pas être prouvée. L'obligation de prouver la véracité d'un jugement de valeur est impossible à satisfaire et porte atteinte à la liberté d'opinion elle-même, qui est un élément fondamental du droit garanti par l'article 10[74].

62. Dans ce domaine, il convient de se référer non seulement à la jurisprudence de la Cour mais aussi aux normes adoptées par le Conseil de l'Europe : la Recommandation CM/Rec(2016)5 du Comité des Ministres aux États membres sur la liberté d'internet (13 avril 2015) appelle les États membres à créer un environnement propice à la liberté de l'internet, notamment la fourniture de programmes d'éducation aux médias et au numérique. Il convient également de rappeler que le « discours de haine » a été défini par le Comité des Ministres en 1997. Le Conseil de l'Europe a adopté une Convention sur la cybercriminalité à Budapest le 23 novembre 2001 et on peut estimer qu'une cyberattaque est effectivement une forme de désinformation. On savait, jusqu'à une époque récente, que les cybermenaces avaient des conséquences physiques ou économiques. On sait désormais que la désinformation peut nuire au processus démocratique.

63. La Déclaration conjointe sur les « fausses nouvelles », la désinformation et la propagande adoptée en 2017 par des rapporteurs spéciaux[75] permet d'obtenir une vue d'ensemble compréhensible des normes internationales dans ce domaine. La déclaration exprime la préoccupation des organisations internationales quant à la désinformation en ligne, souligne que les États ont l'obligation positive de créer un environnement propice à la liberté d'expression et définit des normes générales de politique publique pour atteindre cet objectif[76].

64. Il existe donc un besoin impératif et une demande importante de réglementations qui dépassent le cadre d'un simple régime d'autorégulation. Cependant, pour élaborer des propositions de cadre réglementaire s'appliquant à la désinformation, il faut d'abord dresser un inventaire des règles qui existent dans ce domaine dans un certain nombre d'États membres et d'autres pays.

---

73. *Dink c. Turquie*, 14 septembre 2010, 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09.
74. *Jérusalem c. Autriche*, 27 mai 2001, 26958/95.
75. Désignés par les Nations Unies, l'Organisation pour la sécurité et la coopération en Europe, l'Organisation des États américains et le rapporteur spécial sur la liberté d'expression et l'accès à l'information en Afrique (ACPHR) pour promouvoir la coopération internationale et formuler des normes relatives à la liberté d'expression, à la liberté des médias et aux médias.
76. Point 3 de la déclaration conjointe :
« *a.* Les États ont l'obligation positive de promouvoir un environnement de communication libre, indépendant et pluraliste, en ce compris la diversité des médias, qui est un moyen essentiel de combattre la désinformation et la propagande.
*b.* Les États doivent établir un cadre réglementaire précis pour les radiodiffuseurs et le placer sous la supervision d'un organe protégé contre toute ingérence ou pression commerciale et politique, et dont la mission est de promouvoir un secteur de la radiodiffusion libre, indépendant et pluraliste. »

### 1.4.2.3 Exemples de cadres juridiques

**France**

65. Les règles régissant la protection des données à caractère personnel limitent la mesure dans laquelle les logiciels qui ciblent les individus peuvent se développer dans la pratique, étant donné que le consentement est une condition préalable à la collecte de données. Le système juridique français établit une distinction entre les contacts politiques réguliers et les contacts occasionnels entretenus avec les partis politiques et les candidats. Pour les contacts réguliers, la personne concernée doit recevoir des informations sur le traitement des données (nature des données, objet du traitement, conditions dans lesquelles elle peut exprimer son opposition à ce traitement). Pour les contacts occasionnels, le consentement de la personne pour le traitement est requis[77]. Ces règles sont semblables aux normes de l'Union.

66. Les fausses nouvelles sont déjà régies par un article de la loi du 29 juillet 1881 qui s'appliquait à l'origine à la presse. Il s'agit de nouvelles qui pourraient être considérées comme susceptibles de perturber l'ordre public[78]. Trois conditions sont requises : les nouvelles publiées, reproduites ou diffusées sont fausses, la publication risque de troubler l'ordre public et l'auteur a agi de mauvaise foi. Les faits doivent être précis et détaillés. Les poursuites judiciaires peuvent être engagées par le parquet. Si l'ordre public n'est pas perturbé, il n'y a pas de fondement juridique pour une action en justice. Dans la pratique, très peu d'affaires sont portées devant les tribunaux. La diffusion de fausses nouvelles est punie d'une amende de 45 000 euros. Ces règles ont été étendues à l'information en ligne en 2004.

67. L'article 411-10 du Code pénal traite des intérêts fondamentaux de la nation : « Le fait de fournir, en vue de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, aux autorités civiles ou militaires de la France des informations fausses de nature à les induire en erreur et à porter atteinte aux intérêts fondamentaux de la nation est puni de sept ans d'emprisonnement et de 100 000 euros d'amende. »

68. Ceux qui, à l'aide de fausses nouvelles, auront influencé le vote ou déterminé des électeurs à s'abstenir seront punis d'un emprisonnement d'un an et d'une amende de 15 000 euros (article L.97 du Code électoral).

69. La diffusion de fausses nouvelles peut nuire à la légalité du vote et rendre l'élection nulle et non avenue. Cela s'est produit lorsqu'il a été annoncé qu'un candidat avait retiré sa candidature en faveur d'un autre candidat. Le Conseil d'État, en sa qualité de juge électoral, a estimé que cela pouvait nuire à l'équité des résultats, ce qui a entraîné l'annulation de l'élection[79].

70. En 2018, après l'affaire de la diffusion de fausses nouvelles concernant Emmanuel Macron lors de la campagne électorale présidentielle de 2017, une proposition de loi a été déposée par des députés visant à empêcher la propagation de fausses

77. https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.
78. Auvret P., « Fausses nouvelles », *Jurisclasseur Communication*, fascicule 3210.
79. Conseil d'État, France, 14 avril 1999, 196924. Jurisdata 1999-050242.

nouvelles lors des campagnes électorales lorsque l'acte a été commis sur le territoire d'un État membre de l'Union. Cette proposition a été critiquée par la presse et les avocats. Après une première lecture par l'Assemblée nationale, le Sénat l'a rejetée au motif qu'elle n'était pas en mesure de répondre à la question soulevée par la désinformation et qu'elle était contraire à la liberté d'expression lors des campagnes électorales. Le Sénat craignait également que le processus puisse être détourné à des fins politiques. Toutefois, la proposition est à nouveau à l'ordre du jour de l'Assemblée nationale, qui aura le « dernier mot ».

71. La proposition de loi vise à signaler et à faire cesser les allégations délibérément fausses ou mensongères diffusées sur une plateforme en ligne au cours des trois mois précédant une élection.

72. Les plateformes sont soumises à une obligation de transparence. Elles doivent fournir des informations claires, correctes et transparentes sur leurs propres identité et qualité ou sur celles du tiers dont elles parrainent le contenu. Elles doivent également rendre public le montant reçu en échange du parrainage du contenu.

73. Un procureur, toute personne ayant un intérêt juridique à porter l'affaire en urgence devant un juge, ainsi que des parties ou des candidats peuvent se plaindre d'une information prétendument fausse ou involontaire et diffusée délibérément, artificiellement et massivement en ligne. Cette notion de diffusion artificielle et généralisée sera un indice caractérisant une fausse information. Un juge est tenu de statuer sur une affaire de cette nature dans un délai de 48 heures et a le droit de bloquer la publication et de contraindre la plateforme à cesser cette campagne.

74. Les intermédiaires techniques, qui sont des personnes facilitant l'accès aux services de communication, seront soumis à une exigence de coopération renforcée. Ils devront donc rapidement retirer tout contenu illicite porté à leur attention et mettre en place un mécanisme facilement accessible et visible permettant aux personnes de leur signaler d'éventuelles fausses nouvelles.

75. Pendant les trois mois précédant l'élection, le Conseil supérieur de l'audiovisuel (CSA), qui est l'autorité française de régulation de la communication audiovisuelle, peut ordonner la suspension de la diffusion d'un service de radiotélévision contrôlé par un État étranger ou placé sous son influence si ce service diffuse de fausses informations de nature à altérer la sincérité du scrutin.

### Allemagne

76. La liberté d'expression est prévue à l'article 5, paragraphe 1, de la Loi fondamentale, qui couvre la liberté d'expression et la liberté de diffusion[80]. Les poursuites engagées par le chef de l'État turc, Recep Tayip Erdogan, contre un journaliste allemand qui l'avait attaqué ont été rejetées. Le procureur a estimé que cet acte ne pouvait pas être considéré comme une infraction[81].

80. BVerfGE, 54, 208 57, Heinrich Böll, 3 juin 1980.
81. Brauer, J., « Ermittlungsverfahren gegen Jan Böhmermann wegen Beleidigung von Organen und Vertretern ausländischen Staaten usw. Vermerk zur rechtlichen Bewertung », Generalstaatsanwalt, Coblence, 13 octobre 2016.

77. Selon le droit pénal, il convient de faire une distinction entre les déclarations concernant des individus précis et les déclarations générales. La diffusion de fausses nouvelles générales sans aucune référence à des personnes ou groupes de personnes déterminés n'est pas passible de sanctions pénales. Les insultes et la diffamation peuvent être sanctionnées lorsqu'elles visent des personnes. Dans un arrêt du 22 juin 2018, la Cour constitutionnelle a confirmé la condamnation pénale d'une négationniste pour incitation à la haine et à la violence contre des segments de la population. La requérante avait publié de nombreux articles niant les crimes commis sous le régime nazi, et plus précisément les meurtres commis au camp d'extermination d'Auschwitz-Birkenau. La diffusion d'allégations factuelles qui sont manifestement fausses et délibérément trompeuses ne contribue pas au processus de formation de l'opinion. Elle n'est donc pas couverte par la liberté d'expression[82]. Les insultes sont sanctionnées par une amende ou une peine d'emprisonnement de deux ans. Les mêmes sanctions s'appliquent aux insultes délibérées contre des individus. Les demandes de suppression d'informations d'actualité ne sont pas expressément réglementées, mais elles sont examinées par le pouvoir judiciaire qui statue en conséquence.

78. La personne qui propose une plateforme de diffusion d'informations, de commentaires, de blogs et de forums internet – conformément au droit de l'Union (voir *supra*, paragraphe 44) – est considérée comme un fournisseur d'hébergement au regard du paragraphe 10 de la *Telemediengesetz* (loi sur les médias de télécommunications) et n'est pas censée surveiller activement le contenu des messages sous l'angle des exigences du droit et du droit pénal. Si elle a connaissance de ces messages ou contenus, elle doit les supprimer immédiatement.

79. Depuis le 1er octobre 2017, la *Netzwerkdurchsetzungsgesetz*[83] (loi sur les réseaux sociaux – NetzDG) est entrée en vigueur. Baptisée « loi Facebook », la NetzDG vise clairement les plateformes de partage social qui sont conçues pour faciliter la communication interpersonnelle. Son objectif est de lutter contre les discours haineux et le partage de contenu criminel (anticonstitutionnel, terroriste, pédopornographique, etc., mais aussi diffamatoire)[84]. Les fournisseurs de réseaux sociaux qui reçoivent plus de 100 plaintes par année civile concernant des contenus illicites sont tenus de produire des rapports semestriels en langue allemande sur le traitement de ces plaintes et de publier ces rapports au *Journal officiel fédéral* et sur leur propre site web au plus tard un mois après la fin du semestre concerné. Les rapports publiés sur leur site web doivent être aisément reconnaissables, directement accessibles et constamment disponibles.

---

82. 1 BvR 673/18, « Bundesverfassungsgericht stärkt Meinungsfreiheit », *Frankfurter Allgemeine Zeitung*, 4 août 2018.
83. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.
84. https://www.technologylawdispatch.com/2017/10/social-mobile-analytics-cloud-smac/germanys-new-hate-speech-act-in-force-what-social-network-providers-need-to-do-now.

80. Le rapport doit contenir les éléments suivants :

- des observations générales décrivant les efforts déployés par le fournisseur du réseau social pour éliminer les activités qui font l'objet de sanctions pénales sur la plateforme ;
- la description des mécanismes de dépôt de plaintes concernant des contenus illicites et des critères appliqués pour décider s'il convient de supprimer ou de bloquer ces contenus ;
- le nombre de plaintes reçues concernant des contenus illicites au cours de la période considérée, ventilées par type de plaignants (organismes ou utilisateurs) et par type de motifs ;
- l'organisation, les ressources en personnel, les compétences spécialisées et linguistiques dans les services chargés du traitement des plaintes, ainsi que la formation et le soutien des personnes chargées de ce traitement ;
- l'affiliation à des associations professionnelles ainsi que des informations sur l'existence ou non d'un service de traitement des plaintes dans ces associations ;
- le nombre de plaintes pour lesquelles un organe externe a été consulté en vue de la prise de la décision ;
- le nombre de plaintes qui ont été déposées au cours de la période considérée et qui ont entraîné la suppression ou le blocage des contenus en cause, ventilées par type de plaignants (organismes ou utilisateurs).

81. Les plateformes qui ne sont pas établies en Allemagne « doivent immédiatement désigner une personne qui est habilitée à recevoir un service en République fédérale d'Allemagne et attirer l'attention sur ce fait sur leur plateforme d'une manière aisément reconnaissable et directement accessible ». Le contenu doit être supprimé ou bloqué dans les 24 heures s'il est manifestement illicite. Les autres contenus illicites doivent être supprimés ou bloqués « immédiatement », c'est-à-dire dans un délai de sept jours au cours duquel le contenu est « évalué ». Cette obligation ne s'applique pas aux plaintes déposées par d'autres moyens que la procédure de traitement des plaintes. Il est très probable que le géoblocage (blocage géographique) ne suffise pas.

82. Les infractions à la réglementation peuvent entraîner des amendes pouvant aller jusqu'à 5 millions d'euros pour les particuliers et jusqu'à 50 millions d'euros pour le fournisseur de plateforme lui-même. L'infraction à la réglementation peut être sanctionnée même si elle n'est pas commise en République fédérale d'Allemagne.

83. Un certain nombre d'avocats estiment que la loi est incompatible avec le principe de la liberté d'expression. Même le Wissenschaftlicher Dienst du Bundestag, le service de recherche de l'Assemblée allemande qui contribue au travail des députés sur les politiques au parlement et dans les circonscriptions, en fournissant des informations spécialisées, des analyses et des avis d'experts, a exprimé sa préoccupation quant à la conformité de cette loi avec la Loi fondamentale sur plusieurs points : les très courtes périodes pendant lesquelles la compatibilité des messages avec la liberté d'expression doit être évaluée ; la légitimité de l'objectif de la loi (lutte contre la déstabilisation de l'opinion publique, *Vergiftung der Stimmung im Land*) ; les dispositions ambiguës de la loi concernant la nécessité, ou non, de produire des faits détaillés ; la proportionnalité des amendes concernant la liberté d'expression ; la conformité de

la loi avec la loi relative à la vie privée. La jurisprudence de la Cour constitutionnelle allemande, de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme devrait clarifier ces différents points.

**Royaume-Uni**

84. La Commission électorale britannique a appelé à renforcer la transparence à l'égard des électeurs en ce qui concerne la pratique des campagnes électorales numériques. Elle a formulé des recommandations sur les responsabilités en matière de campagnes numériques, les dépenses qui sont consacrées à ces campagnes, la transparence des paiements et l'application de ces règles[85].

**États-Unis d'Amérique**

85. Le Honest Ads Act (loi sur les publicités honnêtes) présenté au Congrès américain en octobre 2017 introduit des règles de divulgation et d'exonération de responsabilités concernant la publicité politique en ligne. Les entreprises technologiques doivent conserver des copies des annonces électorales et les mettre à la disposition du public. Les annonces publicitaires doivent également contenir des clauses de non-responsabilité semblables à celles qui sont incluses dans les publicités diffusées à la télévision ou dans la presse. Elles doivent indiquer aux électeurs les noms de ceux qui ont acheté la publicité diffusée, le montant payé et les cibles visées. La date et l'heure auxquelles la première publicité a été diffusée pour la première fois doivent également être fournies[86]. Twitter s'est engagé à soutenir la proposition de loi bipartite déposée par le sénateur Amy Klobuchar (D-MN), le sénateur Mark Warner (D-VA) et l'ancien sénateur John McCain (R-AZ).

86. Il est clair que de nombreux pays sont conscients des dangers que représente la manipulation de l'opinion publique durant les campagnes électorales et que des efforts considérables sont déployés pour mettre en œuvre de nouvelles réglementations visant à lutter contre la désinformation. Cependant, de nombreux obstacles entravent l'élaboration de règles efficaces compatibles avec les normes constitutionnelles et internationales, et rendront l'exercice difficile[87].

87. Les recommandations ci-après pourraient apporter des éléments de réflexion nécessaires pour un débat sur d'éventuelles normes internationales au sein du Conseil de l'Europe. Ces normes combinent l'autorégulation et la réglementation officielle parce qu'il s'agit d'une question globale qui concerne le renforcement de la vie privée, la transparence, la dissuasion, la réactivité du suivi, l'éthique, l'éducation et les bonnes pratiques des plateformes.

85. « Digital campaigning, Increasing transparency for voters », *op. cit*.
86. https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act.
87. C'est la raison pour laquelle le Conseil d'État français a rendu son avis juridique sur la proposition de loi parlementaire sur les fausses nouvelles.

# 2. Recommandations

88. Pour relever ces défis juridiques et techniques, le Conseil de l'Europe pourrait envisager d'aborder les questions suivantes.

## 2.1. Définition des termes

89. Les termes « désinformation » ou « fausses informations » devraient être utilisés au lieu et place de « fausses nouvelles ».

90. Le groupe d'experts est d'avis que l'expression « fausses nouvelles » ne « permet pas de saisir la complexité de la notion de désinformation, qui porte sur des contenus qui ne sont pas vraiment ou complètement "faux" mais qui sont composés d'informations inventées, mélangés à des faits et des pratiques qui dépassent le cadre de ce que l'on entend généralement par "nouvelles" »[88]. Le même groupe de travail estime que l'expression « fausses nouvelles » est non seulement inappropriée mais aussi trompeuse parce qu'elle a été adoptée par certaines personnalités politiques et leurs partisans qui l'utilisent pour désigner une couverture médiatique qui ne leur plaît pas. Ces termes sont donc devenus une arme avec laquelle des acteurs puissants peuvent s'immiscer dans la circulation de l'information pour attaquer et fragiliser les médias indépendants.

91. En droit français, le champ d'application des « fausses informations » est plus large que celui des « fausses nouvelles » car il ne fait référence à aucune diffusion antérieure des informations en question, qui peuvent avoir été liées à des faits précis et détaillés. Il est donc nécessaire, pour éviter aux autorités publiques d'avoir à traiter des questions juridiques relatives à la protection de la liberté de l'information, d'établir l'intention malveillante de la diffusion de ces fausses informations.

92. Dans ce contexte, nous devons garder à l'esprit la jurisprudence de la Cour européenne des droits de l'homme : « La matérialité des déclarations de fait peut se prouver ; en revanche, les jugements de valeur ne se prêtant pas à une démonstration de leur exactitude, l'obligation de preuve est donc impossible à remplir et porte

88. « A multi-dimensional approach to disinformation, Report of the Independent High level Group on fake news and online disinformation », Commission européenne, 2018, p. 10 (en anglais uniquement).

atteinte à la liberté d'opinion elle-même, élément fondamental du droit garanti par l'article 10 [de la Convention] »[89].

## 2.2. Transparence

93. La question de la transparence devrait principalement viser les opérateurs et le financement de leurs activités.

94. Les obligations de transparence s'appliquent déjà dans le domaine de la communication. L'article 6 de la Directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, en particulier le commerce électronique dans le marché intérieur (« Directive sur le commerce électronique ») prévoit que les États membres veillent à ce que les communications commerciales qui font partie d'un service de la société de l'information ou qui le constituent remplissent au moins les conditions suivantes :

a. la communication commerciale doit être clairement identifiable comme telle ;

b. la personne physique ou morale pour le compte de laquelle la communication commerciale est faite doit être clairement identifiable.

95. Le Règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur peut également être mentionné. En effet, il crée un environnement réglementaire prévisible pour l'utilisation transfrontière en ligne, la reconnaissance et l'application des services d'identification, d'authentification et de confiance électroniques, services qui pourraient être utilisés pour favoriser le développement et l'utilisation volontaire de systèmes d'identification sécurisée des fournisseurs d'informations sur la base des normes de sécurité et de confidentialité les plus élevées, y compris l'utilisation éventuelle de pseudonymes vérifiés.

96. L'article 5 de la Directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union fixe les modalités d'identification des opérateurs de services essentiels.

97. La Recommandation (UE) 2018/334 de la Commission européenne, du 1er mars 2018, sur les mesures destinées à lutter, de manière efficace, contre les contenus en ligne illicites[90], améliore la transparence et l'exactitude des mécanismes de notification et d'action :

« 16) Les prestataires de services d'hébergement devraient être encouragés à publier des explications claires, aisément compréhensibles et suffisamment détaillées au sujet de leur politique en matière de retrait de contenus ou de blocage de l'accès à des contenus qu'ils stockent, notamment les contenus considérés comme illicites.

17) Les prestataires de services d'hébergement devraient être encouragés à publier, à intervalles réguliers, et de préférence au moins une fois par an, des rapports sur leurs activités relatives au retrait de contenus considérés comme illicites ou au blocage de

89. *Morice c. France*, 23 avril 2015, 293969/10.

90. https://ec.europa.eu/digital-single-market/fr/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

l'accès à ces derniers. Ces rapports devraient comporter, en particulier, des informations sur le volume et le type de contenus retirés, sur le nombre de notifications et de contre-notifications reçues, ainsi que sur le délai de réaction. »

Il existe donc une tendance générale à renforcer la transparence en ce qui concerne les prestataires de services opérant dans l'Union.

98. Les propositions de loi américaine et française et la Commission électorale britannique relèvent de la même façon la nécessité d'identifier qui se trouve derrière ces plateformes en ligne. Pour y parvenir, la Commission électorale britannique recommande que le matériel numérique utilisé pour les campagnes électorales soit identifiable. Cette exigence serait utile pour faire respecter les plafonds de dépenses des partis politiques, des candidats et des tiers parce que les sources de publicité politique sont diverses et difficiles à identifier. Pour accroître la transparence, la Commission électorale britannique recommande que « les candidats soient tenus de fournir des factures de leurs fournisseurs contenant des informations plus détaillées sur les activités menées au cours de leurs campagnes ».

99. La réglementation doit-elle aller plus loin avec des plateformes de médias sociaux « labellisés » ? Reporters sans frontières, l'une des principales ONG de défense et de promotion de la liberté de l'information, souhaite créer un référentiel ISO européen sur la transparence des médias, l'éthique et l'indépendance. Un tel système, qui indique clairement les sources, peut néanmoins s'avérer contre-productif. Les « listes blanches » d'articles ou de sources d'information d'actualité établies à partir de la notation d'un utilisateur ou d'une institution indépendante deviennent souvent un substitut des informations approuvées par le gouvernement. Elles peuvent donner l'impression que seuls les médias sociaux qui portent un tel label sont fiables. Dans leur communication sur la désinformation du 26 avril 2018[91], les institutions de l'Union ont recommandé la mise en place d'indicateurs de fiabilité des sources de contenu, fondés sur des critères objectifs et approuvés par les associations de médias d'information. Qui sera néanmoins habilité à délivrer ce label et que se passera-t-il si une plateforme labellisée diffuse de fausses nouvelles ?

100. Le *Honest Ads Act* (loi sur les publicités honnêtes) des États-Unis soutient que la transparence du financement des publicités politiques est essentielle pour faire respecter d'autres lois sur le financement des campagnes, notamment l'interdiction du financement des dépenses de campagne par des ressortissants étrangers. La loi étend aux plateformes numériques les exigences actuelles en matière d'accès du public aux ventes de publicités politiques sur des réseaux radiodiffusés, câblés et satellites. Elle renforce la transparence et l'obligation de rendre compte des achats de publicités payantes. En effet, elle exige que les plateformes numériques comptant au moins 50 millions de visiteurs mensuels uniques tiennent, pendant les douze mois (surtout les mois critiques) qui précèdent la campagne électorale, un registre complet des demandes soumises par les annonceurs dont le montant total des demandes d'achat de publicités politiques autorisées sur ces plateformes au cours des douze mois précédents dépasse 500 dollars des États-Unis.

91. European Commission Brussels. 26.04.2018 COM (2018) 236 final.

101. Dans le même ordre d'idées, la Commission électorale britannique invite les candidats à indiquer combien ils ont dépensé pour produire et envoyer des messages ciblés aux électeurs en utilisant les canaux numériques.

## 2.3. Durée des campagnes électorales

102. Les restrictions à la publicité, limitées à la durée des campagnes électorales, ne portent pas atteinte à la liberté de prestation des services et à la liberté d'expression au regard des normes de l'Union européenne, compte tenu en particulier de l'intérêt général en jeu.

103. Pour couvrir les activités liées à une campagne numérique, la période électorale doit être déterminée avec précision par la loi et ne pas être trop courte. Il existe des pays où cette période est très courte (Azerbaïdjan, Grèce, Lituanie, Macédoine du Nord). Dans ce contexte, les partis et les candidats ne sont pas tenus d'enregistrer les revenus perçus et les dépenses engagées avant cette période, même s'ils sont liés à une campagne électorale. Il faut donc remettre en question les périodes de campagne qui sont courtes et les prolonger afin d'éviter le risque de concurrence déloyale et d'ingérence des campagnes numériques importantes avant le début de la campagne électorale officielle.

104. Par exemple, pendant les six mois précédant une élection générale en France, l'utilisation à des fins de propagande électorale de tout procédé de publicité commerciale par la voie de la presse ou par tout moyen de communication audiovisuelle est interdite (article L.52-1 du Code électoral). Une telle règle pourrait être transposée, assortie d'un délai plus court, pour réglementer ou interdire toute diffusion d'éléments de désinformation à grande échelle et artificielle.

## 2.4. Dépenses consacrées aux campagnes électorales numériques

105. Il serait logique de considérer que les dépenses consacrées aux campagnes numériques font partie des dépenses électorales s'il n'y a pas d'autre disposition sur ces questions et qu'elles sont donc incluses dans les plafonds de dépenses des partis, des candidats et des tiers concernés, le cas échéant.

106. Les dépenses consacrées aux campagnes numériques par un pays étranger devraient-elles être interdites ? Une telle décision serait-elle contraire au droit à la liberté d'expression ?

107. Il existe, dans différents États membres du Conseil de l'Europe, des députés qui représentent des électeurs à l'étranger (France, Portugal et Roumanie, par exemple). Il s'agit d'électeurs d'États membres qui vivent à l'étranger mais qui votent dans le pays où ils sont inscrits comme électeurs et dans l'Union. Les citoyens européens peuvent voter aux élections locales dans le pays européen où ils vivent. Cependant, en tant qu'électeurs, ils peuvent être préoccupés par le problème de la désinformation.

108. L'interdiction des dépenses électorales à l'étranger est-elle différente de l'interdiction des dons à l'étranger, qui est une règle largement répandue au sein du Conseil de

l'Europe (France, Allemagne sous certaines conditions, Lettonie, Moldova, Roumanie, Turquie et Ukraine, par exemple) ? Pourquoi les dons à l'étranger devraient-ils être interdits et les dépenses électorales à l'étranger autorisées ? Quelle serait l'incidence d'une interdiction des dons à l'étranger si, en même temps, les dépenses électorales à l'étranger étaient admises ? Les dépenses numériques engagées à l'étranger à des fins électorales pourraient être considérées comme des dons en nature de tiers. En outre, tous les pays n'imposent pas un plafond des dépenses électorales. En conséquence, l'absence de réglementation dans ce domaine pourrait être un moyen de créer une inégalité des chances entre les partis politiques et les candidats, et de contourner la règle limitant les dépenses électorales lorsque celle-ci s'applique.

109. La liberté d'expression n'a pas été prise en compte lorsque les législateurs de différents États membres ont décidé d'interdire les dons de sociétés étrangères. Comme celles-ci ne votent pas, l'interdiction de toute dépense de campagne engagée par ces sociétés pourrait être conforme au principe de la liberté d'expression.

110. En ce qui concerne le droit d'une ONG de diffuser des publicités politiques à la radio et à la télévision, la Cour européenne des droits de l'homme a estimé nécessaire d'équilibrer, d'une part, le droit de l'ONG requérante de communiquer des informations et des idées d'intérêt général que le public a le droit de recevoir, et, d'autre part, la volonté des autorités de protéger le débat et le processus démocratiques contre les distorsions de puissants groupes financiers ayant un accès avantageux aux médias influents. La Cour a reconnu que ces groupes pouvaient bénéficier d'avantages concurrentiels dans le domaine de la publicité payante et ainsi limiter le débat libre et pluraliste dont l'État reste le garant ultime[92]. En conséquence, le risque d'un déséquilibre entre des forces politiques en concurrence doit être pris en compte pour maintenir un débat libre et pluraliste. Ce risque, qui a été souligné par la Cour de Strasbourg en son temps avec des médias classiques, peut se présenter avec les médias sociaux, qui n'étaient pas aussi répandus qu'aujourd'hui. Des candidats et des partis politiques peuvent bénéficier de l'aide de plateformes en ligne puissantes et anonymes tandis que d'autres en sont privés. L'ingérence non régulée des médias sociaux dans les campagnes électorales risque donc de créer des campagnes électorales déloyales.

## 2.5. Protection des citoyens à l'égard du traitement des données à caractère personnel régi par le Règlement général européen sur la protection des données (RGPD)

111. Les États-Unis d'Amérique et l'Union européenne ont une approche différente de la protection de la vie privée. Le premier amendement aux États-Unis autorise l'utilisation de données politiques qui sont considérées comme une forme protégée de discours.

112. Dans l'Union européenne, le Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à

92. *Animal Defenders International c. Royaume-Uni*, 22 avril 2013, 48876/08. Doublet, Y.-M., « L'interdiction des campagnes politiques publicitaires à la télévision et à la radio n'est pas contraire à l'article 10 de la CEDH », *Revue trimestrielle des droits de l'homme*, 2014, 98, p. 483.

l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données, ou « RGPD »), et abrogeant la Directive 95/46/CE, s'applique dans tout l'espace de l'Union depuis le 25 mai 2018, et tous les États membres ont dû l'incorporer dans leur droit interne avant le 6 mai 2018. Le règlement énonce que la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne (TFUE) prévoient que toute personne a droit à la protection des données à caractère personnel.

113. Selon ce règlement, le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être équilibré par rapport aux autres droits fondamentaux, conformément au principe de proportionnalité. Le règlement respecte tous les droits fondamentaux et observe les principes reconnus par la charte, consacrés par les traités, et notamment le droit au respect de la vie privée et familiale, du domicile et des communications, le droit à la protection des données à caractère personnel, le droit à la liberté de pensée, de conscience et de religion, le droit à la liberté d'expression et d'information, le droit à la liberté d'entreprise, le droit à un recours juridictionnel effectif et à un procès équitable, ainsi que le respect de la diversité culturelle, religieuse et linguistique.

114. Le règlement ne s'applique pas à des questions de protection des libertés et droits fondamentaux ou de libres flux des données à caractère personnel liées à des activités qui n'entrent pas dans le champ d'application du droit de l'Union, notamment les activités relatives à la sécurité nationale. À cet égard, on peut considérer que les questions électorales relèvent de la souveraineté de chaque État membre et sont couvertes par le principe de subsidiarité. Mais les partis politiques peuvent recueillir des données personnelles sur les opinions politiques de la population. Le traitement de ces données peut être autorisé pour des raisons d'intérêt public, à condition que des garanties appropriées soient établies.

115. En mars 2018, le Conseil européen a déclaré que « les réseaux sociaux et les plateformes numériques [devaient] garantir des pratiques transparentes ainsi qu'une protection totale de la vie privée et des données à caractère personnel des citoyens[93] ». Malgré le champ d'application de ce règlement, le Conseil de l'Europe pourrait s'inspirer de plusieurs de ses dispositions pour élaborer un cadre juridique contre la désinformation car, dans une certaine mesure, les finalités du règlement et celles du cadre juridique fourni par le Conseil de l'Europe sont les mêmes. Les définitions, le consentement obligatoire des personnes et la transparence des moyens de traitement pourraient présenter un certain intérêt pour le Conseil de l'Europe afin de garantir l'intégrité des campagnes électorales et des élections.

93. www.consilium.europa.eu/en/press/press-releases/2018/03/23european-council-conclusions-22-march-2018/.

116. Dans la perspective des élections de 2019 au Parlement européen, l'Union européenne cherche à imposer des amendes aux partis politiques européens qui utilisent abusivement les données personnelles d'un électeur pour influencer les élections. Les sanctions pourraient représenter 5 % du budget annuel d'un parti politique qui est financé par le budget général de l'Union européenne, par des dons et des contributions. Ce projet a été signalé par le *Financial Times* le 26 août 2018. Il suppose l'approbation des gouvernements des États membres de l'Union et du Parlement européen, et nécessite de modifier le Règlement (UE, Euratom) n° 1141/2014 du 22 octobre 2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes en vigueur depuis le 1er janvier 2017[94]. L'article 27, paragraphe 4, point *a*, sur les sanctions prévoit qu'en cas d'infractions non quantifiables, le pourcentage du budget annuel du parti politique européen ou de la fondation politique européenne concernée est de 5 %. Le champ d'application de cette règle est limité aux partis politiques européens. Elle vise à assurer la fiabilité du contenu des messages.

## 2.5.1. Définitions

117. La définition des données à caractère personnel et du traitement fournie par le RGPD peut être utile en ce qui concerne l'exploitation autorisée des données pour définir les profils électoraux.

118. La définition des données à caractère personnel est plus large dans le RGPD que dans la précédente législation de l'Union et comprend des identificateurs en ligne, tels qu'une adresse IP. Par « données personnelles », on entend toute information relative à une personne physique identifiée ou identifiable (« personne concernée »). Une personne physique identifiable est une personne qui peut être identifiée, de manière directe ou indirecte, en particulier à partir d'un identifiant tel que le nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à partir d'un ou de plusieurs facteurs spécifiques à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale. « Traitement » désigne, aux fins du règlement, toute opération ou ensemble d'opérations portant sur des données ou séries de données personnelles, que ce soit par un moyen automatisé ou non, comme la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction. Les individus ont le droit de ne pas être soumis à des décisions fondées sur un traitement automatisé sans aucune intervention humaine, si une telle décision peut leur causer un préjudice.

119. Les algorithmes ne devraient être réglementés par ces règles que s'ils reposent sur des données personnelles. Cependant, si tel n'est pas le cas, il s'agit d'un angle mort du point de vue juridique[95]. Il convient donc de le souligner.

94. Koch, T., « Das neue Recht der europäischen politischen Parteien », PRUF, MIP 2018, 24. Jahrgang, p. 71.
95. Villani, C., *et al.*, *Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne*, La Documentation française, Paris, 2018, p. 148.

### 2.5.2. Transparence du traitement

120. Conformément au règlement, tout traitement de données à caractère personnel doit être licite et équitable. Il doit apparaître clairement aux personnes physiques que les données à caractère personnel les concernant sont collectées, utilisées, consultées ou traitées et dans quelle mesure elles sont ou seront traitées. Le principe de transparence exige que toutes les informations et communications relatives au traitement de ces données à caractère personnel soient facilement accessibles et faciles à comprendre, et qu'un langage clair et intelligible soit utilisé.

### 2.5.3. Nécessité d'obtenir le consentement de la personne

121. Pour être licite, le traitement doit être fondé sur le consentement de la personne concernée ou sur tout autre fondement légitime prévu par la législation, soit dans le règlement, soit dans un autre acte législatif de l'Union ou d'un État membre qui y est mentionné. Au moins une des conditions suivantes doit être remplie : le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci. Il n'y a aucune certitude que le consentement soit donné. Le consentement doit pouvoir être retiré à tout moment, aussi facilement qu'il a été donné.

122. Si ce règlement sur la protection des données n'est pas la seule réponse au problème, il s'agit d'un élément clé qui donne une plus grande marge d'action aux individus et accroît la responsabilité des opérateurs numériques.

## 2.6. Principes fondamentaux relatifs aux algorithmes et à l'intelligence artificielle

123. L'article premier du RGPD dispose que la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. C'est pourquoi l'autorité française de protection des données, la Commission nationale de l'informatique et des libertés (CNIL), considère que l'intelligence artificielle doit respecter deux principes fondamentaux : la loyauté[96] ainsi que la vigilance et la vigilance/réflexivité. La loyauté s'applique aux plateformes et consiste à « assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs ». La loyauté impose une obligation aux contrôleurs.

Étant donné que le développement des algorithmes entraîne une diminution de la vigilance individuelle, le principe de vigilance et de réflexivité à l'égard des algorithmes devrait être consacré dans le cadre juridique de la désinformation[97].

96. Conseil d'État, « Le numérique et les droits fondamentaux », 2014, pp. 273, 278-281.
97. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf, p. 50.

## 2.7. Procédure sommaire en cas d'urgence

124. Dans les procédures judiciaires accélérées en cas d'urgence, l'action judiciaire telle qu'elle est proposée dans l'actuelle proposition de loi française déposée par des députés peut être dissuasive mais elle soulève trois questions :

- la Cour européenne des droits de l'homme considère que les propos peuvent être plus exagérés lors des campagnes électorales qu'en temps normal. Lors des campagnes électorales, des excès verbaux sont admis[98]. De ce fait, la question de l'applicabilité de cette ingérence peut se poser ;
- en France comme en Allemagne, le juge n'a pas beaucoup de temps pour apprécier si la désinformation est une menace pour l'ordre public et si elle est en mesure de déstabiliser la campagne électorale (48 heures et 24 heures après réception de la plainte). Or, compte tenu de la rapidité de diffusion des fausses nouvelles, une décision judiciaire rapide permettrait à un candidat visé par des attaques et des fausses nouvelles de répondre ;
- si cette option était choisie par le Conseil de l'Europe, il conviendrait de veiller à la proportionnalité de la sanction. Un fournisseur d'accès à internet peut se voir ordonner de bloquer, au détriment de ses clients, l'accès à un site web qui porte atteinte au droit d'auteur. Une telle injonction et son exécution doivent toutefois assurer un juste équilibre entre les droits fondamentaux concernés. Les mesures adoptées par le fournisseur d'accès à internet doivent être strictement ciblées, en ce sens qu'elles doivent servir à mettre fin à la violation par un tiers du droit d'auteur ou d'un droit connexe, sans pour autant affecter les internautes qui utilisent les services du fournisseur pour accéder légalement à l'information. Sans cela, l'ingérence du fournisseur dans la liberté d'information de ces internautes serait injustifiée au regard de l'objectif poursuivi[99].

## 2.8. Coopération avec les différents intervenants

125. Le Groupe d'experts de haut niveau sur les fausses informations et la désinformation en ligne a souligné qu'il faudrait s'efforcer d'accroître la sensibilisation des médias et du système éducatif aux dangers que peuvent poser les divers mécanismes numériques de désinformation. À cet égard, il appelle à des actions de soutien aux programmes d'éducation à l'information et aux médias destinés aux citoyens de tous âges.

126**.** Les intervenants sont des plateformes, des vérificateurs de faits, des journalistes, des médias et des organismes de recherche.

La vérification des faits est aujourd'hui une activité dispersée dans les États membres qui devraient prendre des initiatives pour développer des plateformes consacrées à cette activité.

127. Le groupe d'experts recommande que l'utilisateur puisse contrôler ce qu'il souhaite afficher en fonction de critères de qualité et que les journalistes puissent

98. Cour européenne des droits de l'homme, *Brasilier c. France*, 11 avril 2006, Requête n° 71343/01.
99. Cour de justice de l'Union européenne, UPC Telekabel, 27 mars 2014, C-314/12.

bénéficier d'outils professionnels de vérification automatique de contenu, de formations et de projets d'innovation médiatique.

128. La défense de la liberté d'expression, de la liberté de la presse et du pluralisme, le soutien au journalisme de qualité sont des points clés du programme d'action du groupe d'experts. À cet égard, la confiance dans le traitement de l'actualité dépend du pays concerné. Cette confiance dans les organes d'information et les journalistes s'élève à 62 % en Finlande et à 23 % en Grèce. Seuls sept États membres du Conseil de l'Europe ont un taux supérieur à 50 % parmi les 21 États membres analysés par Reuters dans son rapport publié à la fin de 2017[100] : la Finlande, le Portugal, la Pologne, les Pays-Bas, l'Espagne, l'Allemagne et le Danemark. Les organes de presse et les journalistes souffrent également d'une perte de confiance dans ce contexte. Il convient enfin d'accorder une attention particulière aux formes d'aide publique aux organisations de médias.

129. Ces étapes devraient être complétées par un cadre d'exécution. Nous avons vu précédemment que le groupe d'experts avait invité la Commission européenne à promouvoir un code de pratiques à l'échelle européenne qui reflète les rôles et responsabilités des différentes parties prenantes. La transparence, en particulier la transparence financière, l'obligation de rendre compte, la protection de la vie privée, l'accès protégé, la distinction entre la publicité politique et d'autres contenus et la coopération entre les plateformes sont les principaux points soulevés.

130. Il s'agit d'une approche consensuelle dans laquelle les plateformes en ligne ont un rôle clé. Cependant, l'expérience américaine montre qu'il ne faut pas que les marchés numériques soient uniquement entre les mains des opérateurs et qu'un rôle plus important devrait être confié aux pouvoirs publics.

131. Quatre autres points méritent une attention particulière[101] :

- la nécessité pour les représentants de la société civile de contrôler les opérateurs. Les actions menées aux États-Unis par Upturn[102], Propublica[103], Electronic Frontier Foundation[104] peuvent être mentionnées dans ce contexte ;
- la promotion de l'éthique dans la formation des ingénieurs, techniciens, gestionnaires de plateformes en ligne ;
- l'introduction d'un recours collectif non seulement pour mettre fin à une infraction, mais aussi pour remédier à tout préjudice pouvant être subi à titre personnel ;
- la création d'une commission chargée de l'éthique des technologies numériques, qui pourrait diffuser des guides de bonnes pratiques, élaborer des codes de conduite et donner des conseils aux gouvernements.

100. https://reutersinstitute.politics.ox.ac.uk.
101. Villani, C., *op. cit.*
102. upturn.org.
103. https://www.propublica.org/.
104. https://www.eff.org/.

## 2.9. Conformité avec le droit européen

132. Le cadre juridique proposé est conforme aux exonérations de responsabilité des prestataires de services prévues à l'article 14 de la Directive 2000/31/CE. Mais les prestataires de services sont également soumis à d'autres obligations, en particulier celles de la transparence, conformément aux outils s'appliquant aux plateformes en ligne (voir *supra*) et aux lignes directrices prévues par la Recommandation de la Commission européenne sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne, même si la portée de la présente recommandation est différente de la question examinée. Elle serait également conforme au droit à la protection des données à caractère personnel accordé par le RGPD.

Cette approche peut évoluer dans le sens des initiatives antérieures de l'Union européenne sans remettre en cause le principe de l'exonération de responsabilité prévu à l'article 14 de la Directive 2000/31/CE.

## 2.10. Mise en application

133. Si les parties prenantes gouvernementales ou non gouvernementales hésitent à appliquer de telles règles en matière de transparence ou de contrôle judiciaire, ces règles resteront vides de sens. Dans un monde numérique en évolution rapide, chaque partie devrait adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction de diffusion d'informations fausses et trompeuses. Cependant, comment la détection, l'instruction et la poursuite de cette infraction peuvent-elles être imposées à un État où l'infraction a été commise si ce dernier se réserve le droit de ne pas appliquer concrètement ses obligations ?

## 2.11. Synthèse des propositions

134. Trois types de dispositions sont proposés :

- réglementations du droit numérique : conformément aux normes européennes et constitutionnelles, ces réglementations sont axées sur les prestataires de services. Au titre du principe de l'exonération de responsabilité et des diverses dispositions de l'Union européenne relatives à la transparence, ces dispositions légales exigent des prestataires de services qu'ils fassent preuve de transparence dans leurs activités et qu'ils protègent les données à caractère personnel. Une procédure judiciaire accélérée serait mise en place en cas d'urgence ;
- réglementations du droit électoral : des campagnes électorales plus longues, la transparence des ressources financières des fournisseurs et l'interdiction faite à une personne physique ou morale étrangère d'engager des dépenses pour des activités numériques liées à une campagne électorale pourraient constituer la base d'un cadre juridique efficace ;
- bonnes pratiques : d'autres mesures seraient axées sur la vérification des faits, la coopération avec toutes les parties prenantes, l'éthique, le développement de programmes d'éducation et l'autorégulation des prestataires de services, à l'appui d'un journalisme de qualité.

# 3. Programme d'action

135. Un programme d'action concernant la désinformation et les campagnes électorales pourrait constituer le cadre approprié pour relever les défis posés par cette question complexe.

Convaincus que la tenue d'élections libres et régulières est une priorité du Conseil de l'Europe pour renforcer la gouvernance démocratique et la participation des citoyens européens ;

Conscients que le rétablissement de la confiance dans les institutions fondamentales de nos démocraties est une lutte permanente et qu'il faut systématiquement redoubler d'efforts pour lutter contre les tentatives de dévalorisation de la vérité qui érodent la démocratie ;

Préoccupés par le risque que les médias sociaux puissent être utilisés comme un système mondial et un modèle commercial qui fragilisent le processus politique des campagnes électorales et convaincus que les questions soulevées par les algorithmes et l'intelligence artificielle, notamment pendant les campagnes électorales, influencent de manière significative le processus politique ;

Concernés par la rapidité vertigineuse des progrès technologiques et le fait que les activités de désinformation numérique touchent davantage d'électeurs que les techniques classiques ;

Conscients que la transparence des campagnes numériques est réduite en raison de l'utilisation de la publicité, des algorithmes, des « bots », ainsi que des limites de la surveillance et du manque de politiques publiques dans ce domaine ;

Compte tenu du nouveau Règlement général européen sur la protection des données (RGPD), qui vise au respect des données à caractère personnel et au consentement des utilisateurs et qui impose aux plateformes de médias sociaux des règles plus strictes que par le passé, et constatant qu'en raison d'un manque de réglementation les États membres de l'Union européenne et du Conseil de l'Europe ne disposent pas de moyens juridiques efficaces pour se protéger contre les mécanismes numériques de manipulation au cours d'une campagne électorale, et que, ce qui est paradoxal, l'électeur européen est moins protégé que le consommateur européen ;

Considérant qu'il existe des solutions non gouvernementales et gouvernementales pour s'attaquer à ces questions, certaines reposant sur l'autorégulation, d'autres sur des incitations et des mesures contraignantes ;

Se félicitant des actions récentes et d'autres développements de l'Union européenne dans la lutte contre la désinformation dans la perspective de l'élection du Parlement européen,

Les États membres du Conseil de l'Europe devraient, dans un délai imparti, adopter une stratégie globale sur les médias sociaux et les campagnes électorales qui combinerait des mesures réglementaires et d'autorégulation. À cet égard, ils seraient avisés de prendre les mesures suivantes :

- mettre leurs efforts en commun pour garantir une information libre et impartiale pendant les campagnes électorales, réglementer les pratiques de désinformation et éviter, lorsqu'ils mentionnent ces pratiques, de faire référence à des « fausses nouvelles », un concept qui n'est ni approprié ni adéquat pour un cadre juridique ;
- dresser un inventaire des différents types existants d'autorégulation et de réglementation que les États membres appliquent aux campagnes numériques ;
- définir la durée des campagnes électorales pour éviter le risque que des campagnes numériques massives aient lieu durant les périodes préélectorales ;
- exiger l'identification du matériel numérique pour savoir qui se trouve derrière les plateformes en ligne ;
- imposer aux plateformes en ligne de déclarer les dépenses qu'elles ont consacrées aux campagnes électorales numériques ;
- interdire à une personne physique ou morale étrangère d'engager des dépenses dans des campagnes numériques à des fins électorales ;
- s'inspirer du RGPD en demandant au citoyen de consentir à ce que ses données personnelles soient utilisées pour des campagnes électorales numériques, sauf si ce citoyen a des contacts réguliers avec un parti politique ou un candidat dans le cadre de ses objectifs et à condition que ces données personnelles ne soient pas divulguées sans le consentement du citoyen en question ;
- prévoir des obligations de loyauté et de vigilance s'appliquant aux plateformes et algorithmes en ligne ;
- permettre à un tribunal, en cas de diffusion généralisée de fausses informations, de bloquer immédiatement une plateforme en ligne qui diffuse des fausses nouvelles à grande échelle, en recourant à des procédures judiciaires accélérées ;
- encourager les initiatives de vérification des faits en créant un réseau reliant les États membres du Conseil de l'Europe en vue de mener des opérations de grande ampleur ;
- éduquer les utilisateurs pour qu'ils puissent mieux accéder aux informations en ligne et les exploiter, et les informer lorsque le contenu est généré ou diffusé par un « bot » ou des algorithmes ;
- favoriser l'éducation à l'éthique de tous les acteurs impliqués dans les technologies numériques ayant une incidence sur les élections ;

- renforcer l'éthique dans les activités des plateformes en ligne ;
- encourager les plateformes en ligne à adopter des bonnes pratiques en signant des accords avec elles, en prenant pour base des recommandations sur des politiques définies conjointement par les autorités publiques compétentes et les plateformes en question ;
- fournir un soutien aux organisations médiatiques de qualité et au journalisme ;
- créer une commission d'éthique dans chaque État membre et charger les commissions établies de mener des discussions sur les questions éthiques, politiques et sociales soulevées par le développement des technologies, notamment dans les campagnes électorales numériques ;
- prévoir des sanctions effectives, proportionnées et dissuasives en cas d'infraction à la réglementation applicable aux campagnes électorales numériques ;
- créer un groupe de coopération entre États membres afin d'appuyer et de faciliter une coopération stratégique ainsi que l'échange d'informations.

# Conclusion

136. La loi électorale fait partie de la souveraineté des États. Elle est liée à leur contexte historique et à l'organisation de leurs institutions. Il s'agit d'un domaine où il n'existe pas de réglementation commune, à l'exception des principes généraux sur des élections libres et équitables qui visent à garantir concrètement la libre expression de l'opinion des électeurs dans le choix de leurs représentants. Cependant, l'incidence de techniques numériques invasives dans le cadre de la mondialisation crée un nouveau contexte qui nécessite l'élaboration d'instruments internationaux pour protéger des démocraties européennes confrontées à des menaces communes.

137. Le Conseil de l'Europe est l'organe européen le plus approprié et le plus légitime pour engager des discussions dans ce domaine, et pour aller plus loin que la Commission européenne et la déclaration commune des Nations Unies et de l'OSCE, qui date de 2017.

138. Un instrument juridique européen élaboré sous l'égide du Conseil de l'Europe pourrait donner une direction commune à un cadre global. Un tel instrument pourrait établir des règles uniformes pour chaque État membre. Différents outils sont disponibles à cet égard.

139. Nous avons proposé un avant-projet de programme d'action. Un programme d'action contre la corruption, adopté par un groupe multidisciplinaire en 1995, a été le point de départ de plusieurs instruments juridiques du Conseil de l'Europe sur ces questions : conventions pénales et civiles, recommandations, résolutions et rapports. Cela étant, même si un programme d'action est un processus qui prend beaucoup de temps, il apparaît utile d'examiner les diverses mesures disponibles ainsi que les arguments en faveur et contre chacune de ces solutions potentielles.

140. Dans certains cas, des recommandations ou des résolutions ont précédé les conventions du Conseil de l'Europe. C'est notamment le cas pour la corruption privée ou la cybercriminalité. Des recommandations fixeraient des normes générales et encourageraient les États membres à adopter une législation. Il s'agirait de l'approche la plus raisonnable et la plus rapide pour aborder cette question. Cette option présente néanmoins l'inconvénient de laisser une marge d'interprétation aux États membres, alors que, pour être efficaces, les réglementations dans ce domaine doivent être uniformes et normalisées.

141. Les lignes directrices sont appropriées lorsqu'il existe déjà un cadre juridique établi qui vient appuyer soit un outil international, soit une législation dans les États membres. Les lignes directrices apportent des conseils stratégiques sur la mise en œuvre et en application des règlements existants.

142. Une convention a le mérite d'être un instrument contraignant. Un certain nombre de ratifications pourraient être déterminées pour faciliter son entrée en vigueur sans attendre que chaque État membre la ratifie. Deux autres arguments soutiennent cette option. La plupart des conventions du Conseil de l'Europe incluent un mécanisme de contrôle du respect des dispositions et prévoient la possibilité que les États non membres deviennent parties à l'instrument concerné. L'élaboration de cette convention partira de zéro car seuls quelques États membres ont adopté des règles axées sur ces questions. Cela pourrait faciliter sa rédaction s'il n'existe pas encore de mécanismes existants. Cependant, il faut du temps pour mener à bien le processus de négociation lié à une convention.

143. Compte tenu du consensus obtenu sur les menaces de désinformation qui pèsent sur le processus électoral, le Conseil de l'Europe doit choisir la forme juridique la plus appropriée pour répondre à cette question. Quelle que soit la forme choisie, celle-ci contribuera au renforcement de la démocratie en Europe et aidera le Conseil de l'Europe à mieux remplir sa mission consistant à garantir des élections libres et équitables, lesquelles sont devenues un élément fondamental de l'identité européenne et de ses valeurs constitutionnelles.

# Sales agents for publications of the Council of Europe
# Agents de vente des publications du Conseil de l'Europe

**BELGIUM/BELGIQUE**
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: + 32 (0)2 231 04 35
Fax: + 32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
c/o Michot Warehouses
Bergense steenweg 77
Chaussée de Mons
BE-1600 SINT PIETERS LEEUW
Fax: + 32 (0)2 706 52 27
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

**CANADA**
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: + 1 613 745 2665
Fax: + 1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

**CROATIA/CROATIE**
Robert's Plus d.o.o.
Marasovićeva 67
HR-21000 SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

**CZECH REPUBLIC/**
**RÉPUBLIQUE TCHÈQUE**
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: + 420 2 424 59 204
Fax: + 420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

**DENMARK/DANEMARK**
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: + 45 77 66 60 00
Fax: + 45 77 66 60 01
E-mail: reception@gad.dk
http://www.gad.dk

**FINLAND/FINLANDE**
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: + 358 (0)9 121 4430
Fax: + 358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

**FRANCE**
Please contact directly /
Merci de contacter directement
Council of Europe Publishing
Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81
Fax: + 33 (0)3 88 41 39 10
E-mail: publishing@coe.int
http://book.coe.int

Librairie Kléber
1, rue des Francs-Bourgeois
F-67000 STRASBOURG
Tel.: + 33 (0)3 88 15 78 88
Fax: + 33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

**NORWAY/NORVÈGE**
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: + 47 2 218 8100
Fax: + 47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

**POLAND/POLOGNE**
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: + 48 (0)22 509 86 00
Fax: + 48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

**PORTUGAL**
Marka Lda
Rua dos Correeiros 61-3
PT-1100-162 LISBOA
Tel: 351 21 3224040
Fax: 351 21 3224044
E mail: apoio.clientes@marka.pt
www.marka.pt

**RUSSIAN FEDERATION/**
**FÉDÉRATION DE RUSSIE**
Ves Mir
17b, Butlerova ul. - Office 338
RU-117342 MOSCOW
Tel.: + 7 495 739 0971
Fax: + 7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

**SWITZERLAND/SUISSE**
Planetis Sàrl
16, chemin des Pins
CH-1273 ARZIER
Tel.: + 41 22 366 51 77
Fax: + 41 22 366 51 78
E-mail: info@planetis.ch

**TAIWAN**
Tycoon Information Inc.
5th Floor, No. 500, Chang-Chun Road
Taipei, Taiwan
Tel.: 886-2-8712 8886
Fax: 886-2-8712 4747, 8712 4777
E-mail: info@tycoon-info.com.tw
orders@tycoon-info.com.tw

**UNITED KINGDOM/ROYAUME-UNI**
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: + 44 (0)870 600 5522
Fax: + 44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

**UNITED STATES and CANADA/**
**ÉTATS-UNIS et CANADA**
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel: + 1 914 472 4650
Fax: + 1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

**Council of Europe Publishing/Éditions du Conseil de l'Europe**
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81 – Fax: + 33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int

Depuis l'été 2016, les infox désignent la diffusion virale et délibérée de fausses nouvelles sur internet et dans les médias sociaux, dans le but, par exemple, de discréditer un parti politique, d'entacher la réputation d'une personne ou de remettre en cause une vérité scientifique. Cette pratique, qui empêche les citoyens de prendre des décisions éclairées, s'est beaucoup répandue. Son impact en est d'autant plus important que sa diffusion est extrêmement rapide et que l'identification des auteurs de telles initiatives et du matériel numérique utilisé est très difficile.

Ce rapport s'efforce de répondre aux questions soulevées par ce phénomène – tout spécialement pendant les campagnes électorales – et présente des propositions pour mettre en place un cadre juridique au niveau européen.

PREMS 006819

FRA

**www.coe.int**

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

**http://book.coe.int**
ISBN 978-92-871-8910-3
9 €/18 $US

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE