BRANCHU Emilie

2018/2019

Fake-news et propagande électorale ciblée : la mise en danger des concepts démocratiques par les réseaux sociaux

Mémoire de fin d'études

Double Master franco-espagnol : Droit du Cyberespace et des Nouvelles technologies et Bio-droit.

Sous la direction de : Monsieur Marcel MORITZ

Madame María Magnolia PARDO LOPEZ

Université de Lille / Université de Murcia

SOMMAIRE

REMERCIEMENTS

Au terme de ce travail, je tiens tout d'abord à remercier mes deux professeurs et directeurs de mémoire, Monsieur Marcel Moritz et Madame Maria Magnolia Pardo Lopez, qui ont fait preuve d'une grande disponibilité afin de me conseiller et de m'accompagner dans la rédaction de ce mémoire.

J'aimerais également remercier le personnel des Universités de Lille et de Murcia, notamment les bibliothécaires, qui ont su me renseigner avec pertinence sur les ouvrages et articles de revues pouvant éclairer ma réflexion.

J'adresse aussi mes vifs remerciements aux membres du jury pour avoir bien voulu examiner et juger ce travail.

Mes remerciements se tournent également vers Virginie Morgny et Maximilien Desmarais qui ont gracieusement accepté de corriger ce mémoire, et qui l'ont fait avec grande objectivité et clairvoyance.

Par ailleurs, je souhaite remercier mes parents et mon frère, Jacques, Corinne et Pierre Branchu, ainsi que mon compagnon de vie, Victor Sponga, pour le soutien qu'ils m'ont apporté aussi bien lors de cette rédaction que tout au long de mes études et pour avoir toujours cru en mes capacités.

De la même manière, j'adresse mes plus sincères remerciements à mes amis proches, Dylan Lacoustasse, Romain Nave, Alex Vercampt, Elies Adjem et Clément Prévost pour avoir développé chez moi des capacités de curiosité, de réflexion spontanée et de perpétuelle remise en question.

Enfin, je tiens à me remercier personnellement, pour la rigueur et la ténacité dont j'ai fait preuve tout au long de mes études et pour mener celles-ci à terme, ainsi que pour avoir appris des obstacles et difficultés rencontrés.

ABREVIATIONS

ABBRE : Abréviations.

AEPD: Agencia Española de Protección de Datos.

BCR : Règles d'entreprise contraignantes.

CDFUE : Charte des Droits Fondamentaux de l'Union Européenne.

CEDH : Convention Européenne des Droits de l'Homme.

CEPD : Comité Européen de Protection des Données.

CJUE : Cour de Justice de l'Union Européenne.

CNIL : Commission Nationale de l'Information et des Libertés.

CNRS : Centre National de Recherche Scientifique.

CRT: Comisión de Radio y Televisión.

CSA : Conseil Supérieur de l'Audiovisuel.

CSDHLF : Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales.

DUDH : Déclaration Universelle des Droits de l'Homme.

GT29 : Groupe de Travail de l'article 29.

IA : Intelligence Artificielle.

INE: Instituto Nacional de Estadística.

ISF : Impôt de Solidarité sur la Fortune.

LIL : loi Informatique et Libertés.

LOPD: Ley Orgánica de Protección de Datos.

LOREG: Ley Orgánica del Régimen Electoral General.

RGPD : Règlement Général de Protection des Données.

TFUE : Traité de Fonctionnement de l'Union Européenne.

UE : Union Européenne.

INTRODUCTION

De l'informatique aux réseaux sociaux

Depuis les années 1960, l'informatique fait partie intégrante de notre quotidien et ne cesse de se perfectionner afin de faciliter les communications. L'Académie française la définit en 1966 comme « la science du traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications dans les domaines techniques, économiques et sociaux ». Si cette définition laisse à penser que l'informatique n'est fondée que sur le seul partage des connaissances acquises, tel n'est pas le cas puisqu'elle s'avère être également un outil redoutable pour la collecte et le traitement d'informations relatives aux individus.

En 1973, le gouvernement français se saisit de l'opportunité qu'offre cette innovation technologique et fait naître le projet dit « SAFARI » (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus). Il a alors pour objet la création d'une base centralisée dans laquelle toutes les données des usagers sont rassemblées, le numéro de sécurité sociale les rendant identifiables individuellement. L'objectif n'est autre que de faciliter la circulation d'informations entre les différentes administrations.

Un an plus tard, le journal « le Monde » dévoile ce projet d'interconnexion des fichiers de l'administration et face à l'indignation publique, le gouvernement n'a d'autre choix que de l'abandonner. Le Premier Ministre de l'époque, Pierre Messmer, crée alors la Commission « Informatique et Liberté » afin que soit publié un rapport sur les dangers que présente l'informatique pour les données personnelles, à savoir toute information se rapportant à une personne physique identifiée ou identifiable[1].

En réponse à ce rapport, la loi dite « Informatique et Liberté »[2] (ci-après dénommée la LIL) est adoptée le 6 janvier 1978 et celle-ci crée la Commission Nationale de l'Informatique et des Libertés (ci-après dénommée la CNIL) qui vient en remplacement de la Commission créée en 1974.

[1] Article 4 du RGPD
[2] LOI n°78-17 *relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978.

Cependant, ce n'est qu'une trentaine d'années plus tard que l'informatique prend une toute autre dimension et que le rapport avec celle-ci s'accélère, notamment avec l'arrivée d'internet dans les foyers des citoyens. Ces derniers contribuent dorénavant à créer l'information, incluant les informations « nominatives » – c'est ainsi que s'appelaient les données personnelles dans la LIL de 1978 –, ainsi que la désinformation. Les partages sont intensifiés et les relations entre les individus sont simplifiées, pour ne pas dire démultipliées par l'apparition des réseaux sociaux dans les années 2000 (Facebook, Twitter, Google+, etc.). Un réseau social se définit traditionnellement comme un ensemble d'individus, organisations ou entités entretenant des relations sociales, fondées sur l'amitié, le travail collaboratif ou l'échange d'informations[3]. Cependant, une telle définition ne trouve pas à s'appliquer en ce qui concerne les réseaux sociaux informatiques. L'énumération des fondements sur lesquels sont sensés se baser les relations entre les individus est bien trop exhaustive et écarte totalement de ses considérations la politique, encore plus présente dans le monde virtuel que dans la vie de tous les jours.

Se sentant plus libres de s'exprimer sur internet, les réseaux sociaux informatiques permettent aux individus de se rassembler selon leurs affinités politiques et ainsi naissent des relations entre de véritables inconnus, sans aucun lien d'amitié et de travail. Une telle simplicité dans les communications et les rapports humains expliquent très certainement le succès des technologies de réseaux sociaux. Depuis 2005, elles se sont déployées partout dans le monde et ont été adoptées par les internautes avec une vitesse sans égale pour des technologies de l'information. En moins de 8 ans, 12% de la population mondiale a créé un compte sur le réseau social Facebook. Aujourd'hui, sur les 7,6 milliards d'habitants dans le monde, 3,3 milliards sont actifs sur les réseaux sociaux (soit 43% de la population mondiale) et Facebook, à lui seul, représente 2,2 milliards des individus connectés[4].

Ainsi, si la théorie de Dunbar estime que, pour assurer la reconnaissance des membres d'un réseau social, celui-ci ne peut être constitué de plus de 150 individus[5], on trouve aujourd'hui sur Facebook des communautés comme « Wanted » qui rassemblent à elles-seules plus de 800 000 membres[6].

[3] MERCANTI-GUERIN, M. Facebook, un nouvel outil de campagne : analyse des réseaux sociaux et marketing politique. *Direction et Gestion*, 2010. La Revue des Sciences de Gestion, n°242.
[4] https://www.blogdumoderateur.com
[5] MERCANTI-GUERIN, M. Facebook, un nouvel outil de campagne : analyse des réseaux sociaux et marketing politique, *op.cit.*
[6] SIGNORET, P. « Wanted : une communauté Facebook de 800 000 membres et pas un rond ». Le Monde, 5 mai 2018.

Aujourd'hui plus populaires que les journaux télévisés ou la radio, les auteurs nomment les réseaux sociaux « les nouveaux médias », plateformes sur lesquelles les informations, vraies ou fausses, font le tour du globe en un éclair : la nuit des attentats du 13 novembre 2015 à Paris, les premiers tweets[7] à propos des attaques sont publiés à 21h18, moins d'une minute après que la première explosion a retenti aux abords du Stade de France[8]. La désinformation sur les réseaux sociaux se présente ainsi comme un véritable fléau puisqu'il est estimé que 17% des français s'informent sur ceux-ci. La population des 18-24 ans serait encore davantage touchée dans la mesure où 63% des individus situés dans cette tranche d'âge ont recours aux « nouveaux médias » comme seule source d'informations[9].

C'est de ce contexte, où les échanges se font plus rapides que jamais et où les membres des réseaux sociaux sont de plus en plus actifs et engagés dans le partage d'informations, dont bénéficient (ou souffrent ?) les politiques dans leurs stratégies de communication. Depuis plusieurs années, ces derniers ont pris une place importante dans la sphère numérique soit directement, par la création de comptes officiels, soit indirectement, par la création de groupes de soutien ou d'opposition. Dans le domaine politique, la définition des technologies de réseaux sociaux évolue et elles sont plutôt considérées comme des supports permettant le développement d'un capital social, le capital social étant un ensemble de valeurs collectives qui pousse à l'engagement des individus[10].

Au-delà de l'information – ou de la désinformation – de ces derniers, le volume de données stocké mondialement doublant tous les ans, 67% des utilisateurs d'internet et des réseaux sociaux seraient concernés par l'utilisation de leurs données personnelles afin d'envoyer des messages politiques ciblés[11]. De cette manière, les réseaux sociaux se présentent comme une véritable aubaine pour les hommes politiques, que ce soit dans le cadre de simples stratégies de communication ou de campagnes électorales.

[7] Messages de 140 caractères maximums postés sur le réseau social Twitter
[8] DARMANIN, J., FERRAN, B. et RONFAUT L. « Minute par minute, le récit de la nuit de 13 novembre sur les réseaux sociaux ». *Le Figaro*, 25 novembre 2015.
[9] TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *Quaderni*, 2018. N°96.
[10] DUDEZERT, A. et KAROUI, M. Capital social et enjeux de pouvoir : une perspective socio-politique de l'appropriation d'une technologie de réseaux sociaux au sein d'une collectivité territoriale. *Systèmes d'information et management*, 2012. Volume 17.
[11] COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». Sound and transparent information for an informed and pluralistic democratic debate : practical steps to ensure the support of the online world. 26 et 27 novembre 2018.

La politique est la scène où s'affrontent des individus et des groupes en compétition pour l'exercice du pouvoir[12], et les réseaux sociaux sont devenus leur nouveau terrain d'affrontement. S'y expriment des intérêts collectifs communs ou contradictoires et les hommes politiques ne se limitent pas à en prendre connaissance, ils les utilisent aussi à leur avantage. De la même manière, ils prennent directement part aux débats existants sur les réseaux sociaux et s'expriment sur les différents sujets qui y sont développés. Le monde virtuel leur permet de mieux maîtriser leur image, de noyer les rumeurs et de toucher un panel toujours plus important de potentiels sympathisants. Ainsi, la « politique 2.0 » séduit les dirigeants parce qu'elle se caractérise notamment par :

- Une présentation du candidat plus authentique et accessible ;
- Une plate-forme d'idées, de réactions, un observatoire de l'opinion ;
- Un catalyseur de l'engouement pour un candidat ;
- Une remise en cause des structures d'autorité et de hiérarchie (groupes spontanés, décentralisation, auto-organisation) ;
- Une réintégration de certaines couches sociales (les jeunes) dans le débat politique ;
- Un nouvel outil marketing relationnel et de récolte de fonds ;
- Un palliatif au déclin des structures associatives, traditionnel relais local des politiques ;
- Un support pour les actions locales et l'évènementiel[13].

Si un tel schéma s'applique à tout type de « marketing politique », il s'applique encore davantage à celui mis en œuvre par les dirigeants d'Etats, que ça soit dans un contexte pré-électoral ou dans le cadre de la campagne électorale elle-même. En effet, non seulement il mobilise encore plus l'opinion des individus qui s'expriment de façon presque excessive et incontrôlée, mais il fait également l'objet de bien plus de médiatisation sur les réseaux sociaux. Les informations relayées à leur sujet sont nombreuses mais pas toujours avérées.

De la même manière, les données personnelles des individus sont au cœur de cette « politique 2.0 » parce qu'au-delà de leur permettre de suivre les activités des représentants politiques, ces derniers ont recours aux données accessibles publiquement, en plus d'avoir accès aux données publiques[14]. Avec l'entrée en vigueur du Règlement Général sur la Protection des Données[15]

[12] BRAUD, P. *La science politique*. 11ème édition. Paris : Que sais-je, 2017. 128 p.
[13] MERCANTI-GUERIN, M. Facebook, un nouvel outil de campagne : analyse des réseaux sociaux et marketing politique, *op.cit.*
[14] KRZATALA-JAWORSKA, E. Internet : complément ou alternative à la démocratie représentative ? *Boeck Supérieur*, 2012. Participations, n°2.
[15] PARLEMENT EUROPEEN ET CONSEIL. *Règlement (UE) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 27 avril 2016.

(ci-après dénommé le RGPD), un cadre juridique à l'utilisation de ces données est posé, bien qu'il se présente comme insuffisant après avoir effectué une analyse en profondeur.

Cet aspect de la protection des données personnelles, qui avait fait l'objet d'une réaction vive de la part du public en 1974, ne l'inquiète plus autant à notre époque – et c'est d'ailleurs peut-être une mauvaise chose puisque le partage de celles-ci ne fait que s'accroitre –. Cela peut très certainement s'expliquer par le rôle positif joué par internet – et les réseaux sociaux, devenus quasiment interdépendants – dans l'inclusion citoyenne. Internet est ainsi considéré comme le garant du renforcement de l'ordre établi par la démocratie représentative puisque ses réseaux sociaux permettent l'absorption des tensions et des conflits sociaux, le partage des risques entre les institutions politiques et les citoyens, ainsi qu'une légitimation des actions politiques. Par conséquent, internet se voit défini politiquement comme un nouveau canal de communication, une technologie susceptible d'être utilisée dans le processus de la consultation publique ou bien de la construction des politiques publiques [16]. Federica Mogheroni, haut représentant de l'Union Européenne pour les affaires étrangères et la politique de sécurité, a d'ailleurs déclaré qu'une saine démocratie repose sur un débat ouvert, libre et équitable[17] et une telle participation est rendue possible par les réseaux sociaux.

La participation n'est autre que l'activité des citoyens dans le but d'influencer le choix du gouvernement ou les décisions prises par ce dernier. Sur internet, la participation en ligne se caractérise par l'auto-organisation des internautes, qui prend la forme d'une gouvernance décentralisée et horizontale, et mène à une coproduction de données alternatives aux processus décisionnels classiques. La consultation via les réseaux sociaux se présente comme un instrument utile pour la co-construction des politiques publiques.

Ainsi, s'opposent deux groupes d'acteurs politiques différents à la participation en ligne :

- Les acteurs politiques, à savoir tout acteur collectif ou individuel capable d'affecter le processus de prise de décision dans le système politique[18] ;
- Les citoyens amenés à coconstruire les politiques publiques et à en bénéficier.

Pour le second groupe, il faut noter qu'il existe une forte inégalité et un déséquilibre entre le savoir de chacun pour utiliser internet : on parle d'ailleurs de « fracture numérique ». Pour cette

[16] KRZATALA-JAWORSKA, E. Internet : complément ou alternative à la démocratie représentative ? *op.cit.*
[17] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». 5 décembre 2018.
[18] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *Análisis*. Quaderns de Comunicacio i Cultura, n°56.

raison, et bien que les réseaux sociaux permettent le développement d'une démocratie plus saine quant à l'inclusion de minorités bien connues (les jeunes par exemple) dans le débat politique, d'autres faisant parties des processus électoraux traditionnels (les personnes âgées par exemple) sont exclues de fait de l'univers virtuel.

Par conséquent, les réseaux sociaux deviennent un problème clé dans le fonctionnement des démocraties parce qu'ils constituent une menace pour un processus électoral juste et démocratique. De surcroît, l'utilisation des données personnelles aux fins d'envois de messages politiques ciblés et la propagation de fausses informations entraîne la perte de confiance et de transparence dans les débats ouverts[19].

La révolution numérique a ainsi provoqué l'élargissement de l'espace public et, que ce soit un bien ou un mal, il semble difficile de faire machine arrière. De cette façon, il est difficilement reprochable aux dirigeants d'Etats de s'en approprier la maîtrise.

Cependant, l'élargissement de l'espace public, en y incorporant désormais une partie des conversations privées, bouleverse notre conception et nos pratiques de la démocratie. L'internet se présente ainsi comme une menace pour l'ordre établi, non seulement politique, mais aussi médiatique[20]. Ainsi, même si de prime abord les dirigeants d'Etats ne font que s'adapter aux pratiques actuelles, l'usage qu'ils font d'internet et des réseaux sociaux manque de clarté auprès des individus.

Origines de l'utilisation des réseaux sociaux dans la vie politique

Omniprésents sur les réseaux sociaux depuis maintenant quelques années, les hommes politiques se sont bel et bien appropriés cet outil dans le cadre de leur communication politique et c'est au cours des campagnes électorales qu'ils se montrent les plus actifs. En effet, internet et les réseaux sociaux se présentent durant cette période comme des outils très utiles de propagande.

Bien que le terme de « propagande » conserve la connotation absolument négative qu'il a acquise après 1918 et la Première Guerre Mondiale, il ne se définit finalement que comme étant l'action exercée sur l'opinion pour l'amener à avoir et à appuyer certaines idées politiques. A

[19] COMMISSION EUROPEENNE. *Commission guidance* : « The application of Union data protection law in the electoral context ». 12 septembre 2018.
[20] DOSQUET, F. (dir.). *Marketing politique et communication politique*. 2ème édition. Paris : EMS Management et Société, 2017. 302 p.

ce titre, Edward Luis Bernays, dans son ouvrage *Propaganda* (1928)[21], souhaitait déjà lui rendre son acception neutre et c'est pourquoi, en lieu et place de « communication politique », ce terme sera employé dans le reste de cette réflexion. A noter également qu'il visera essentiellement les actions de communication « numériques » s'inscrivant essentiellement dans le cadre de l'usage d'internet et des réseaux sociaux qui y sont afférents.

En effet, dès leur apparition, les candidats aux élections de 2000 se sont saisis de l'opportunité que présentaient les réseaux sociaux afin d'introduire les pratiques de propagande classique dans l'univers digitale : la mobilisation des bénévoles, la gestion communautaire, le lobbying, la recherche de financement, l'organisation des meetings, et l'amplification des messages à travers les médias sociaux[22].

Si jusqu'alors, tout cela semble bien traditionnel, l'utilisation des réseaux sociaux prend tout son sens quand les dirigeants politiques décident d'en extraire les données personnelles et de les utiliser à des fins de propagande électorale. Cela est d'autant plus intéressant dans la mesure où, à l'époque, la législation ne s'exprime pas ou peu sur le sujet, ce qui laisse une large possibilité de manœuvre aux politiques. Face à cela, la Suisse est l'une des premières à réagir et à approuver une résolution sur l'utilisation des données personnelles à des fins de communication politique[23].

En 2008, Barack Obama, futur Président des Etats-Unis, est le premier à utiliser les réseaux sociaux et à exploiter les données personnelles qu'ils contiennent, et ne se cantonne pas à un simple paysage politique dessiné par des données chiffrées collectées lors d'études de marché (sondage, panels, etc.), comme ont pu le faire ses prédécesseurs. En 2012 également, il est accompagné des consultants de Blue State Digital[24] et lors de ces deux campagnes, il se montre véritablement novateur en ce qu'il est le premier à utiliser des bases de données politiques et commerciales. En les croisant, il obtient des informations inaccessibles sur le comportement quotidien des citoyens, sur lesquels il est encore possible de greffer une multitude d'autres données, qu'elles soient économiques, sociales ou commerciales. Ainsi, il dispose des bases de

[21] BERNAYS, E. *Propaganda : comment manipuler l'opinion en démocratie*. New York : Zones, 1928. 144 p.
[22] DOSQUET, F. (dir.). *Marketing politique et communication politique, op.cit.*
[23] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019 sobre el tratamiento de datos personales relativos a opiniones políticas y envió de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del articulo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general*, 7 de marzo de 2019.
[24] « Elections : à la fête du client ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c'est terminé, N°149.

données des grandes surfaces, qui lui donnent un visu sur le détail de la consommation du client, des données personnelles d'audience de la télévision et des cookies[25].

Finalement, toutes ces informations collectées ou déduites permettent d'élaborer des profils qui vont eux-mêmes permettre d'élaborer des algorithmes de comportement individuel sur 3 aspects :

- L'abstention ou la non-inscription sur les listes ;
- La mobilisation des électeurs passés ;
- Les convictions des indécis[26].

Le dernier aspect apparait comme étant le plus important car il est plus aisé de convaincre les indécis en les ciblant et en leur proposant un programme sur mesure que de convaincre un sympathisant du camp adverse. Même si nous ignorons les résultats exacts sur les élections de Barack Obama en 2008 et 2012, l'application d'une telle technique a permis à François Hollande, ancien Président de la République française, de gagner 0,6% des voix en 2012[27].

Il a en effet été démontré qu'un électeur sur quatorze peut changer d'avis grâce à un porte-à-porte individualisé. C'est finalement ce qui est appelé la technique du « micro-targeting » : après avoir consolidé une base de données la plus complète possible afin d'obtenir des données individuelles – comme l'a fait Barack Obama –, un porte-à-porte individualisé peut être mené. Il en va de même pour l'envoi de messages personnalisés, bien que l'impact positif réel pour le dirigeant politique reste à démontrer dans la mesure où seul un électeur sur 100 000 serait amené à changer d'avis suite à la mise en œuvre de cette technique[28].

En fin de compte, Barack Obama a accompli le rêve Orwellien – ficher tout le pays – et depuis le succès de sa campagne « Obama for America » de 2012, le recours à l'analytique des données est devenu un pilier logistique des campagnes, aussi bien aux Etats-Unis qu'en France. Par ailleurs, le budget des campagnes électorales étant alloué différemment, en raison du caractère couteux de l'utilisation de ces techniques – les montants consacrés par Barack Obama à sa

[25] Petit fichier déposé sur le disque dur à l'insu de l'internaute, lors de la consultation de certains sites web, et qui conserve des informations en vue d'une connexion ultérieure.
[26] BILLE, J. Marketing politique et Big Data. *Commentaire SA*, 2015. Commentaire, n°150.
[27] « Elysée : des données pas données ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c'est terminé. N°149.
[28] THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

campagne électorale digitale se sont élevés à plus de 5 millions de dollars –, les réseaux sociaux remplissent maintenant deux objectifs :

- L'animation de l'appareil de campagne ;
- Et la récolte de fonds[29].

Le scandale Cambridge Analytica et l'élection de Donald Trump comme Président des Etats-Unis

« Comment Trump a manipulé l'Amérique »[30], c'est l'intitulé qu'Arte a donné à son reportage sur l'élection de Donald Trump, actuel Président des Etats-Unis, et le scandale qui a frappé Facebook. Spécialisée dans l'influence, la société Cambridge Analytica aurait collecté les données personnelles détenues par le réseau social à des fins politiques et aurait contribué à faire élire Donald Trump à la tête des Etats-Unis. Ce reportage fait suite aux révélations de Christopher Wylie, ancien salarié de Cambridge Analytica, qui, après avoir dénoncé le piratage des données personnelles de 87 millions d'utilisateurs de Facebook, a dévoilé comment ces données volées ont été utilisées pour influencer l'élection de Donald Trump.

Mais comment un réseau social a-t-il pu permettre d'investir un candidat, pourtant à l'audience faible en tout début de campagne électorale et maîtrisant peu les codes de la propagande politique ? Au-delà du financement de la campagne électorale indépendante du Président des Etats-Unis par les entreprises, rendu possible en 2010 par l'arrêt « *Citizens United v. Federal Election Commission* » de la Cour Suprême et grandement amplifié par la présence des réseaux sociaux, Cambridge Analytica a permis le ciblage d'individus en faisant du profilage psychologique, qu'elle appelle le micro-ciblage comportemental. Bien qu'elle l'intitule différemment, elle ne fait qu'appliquer la technique du micro-targeting employée par Barack Obama qui consiste à combiner les données personnelles des individus afin de déterminer leurs peurs et préoccupations, données personnelles qui ont été en grande partie rachetées à Facebook.

Le micro-targeting mis en œuvre par Cambridge Analytica a permis à Donald Trump d'orienter ses interventions publiques et surtout de les concentrer dans des Etats où il était susceptible de convaincre de nouveaux sympathisants. A ce titre, le slogan de la société est très évocateur : « Adresse un message à la bonne personne, au bon moment ».

[29] BILLE, J. Marketing politique et Big Data, *op.cit.*
[30] HUCHON, T. Comment Trump a manipulé l'Amérique ? *Arte*, 2018.

Développé par le cabinet d'études TargetPoint Consulting en 2004, le micro-targeting permet aux candidats à l'élection d'affiner leurs positions et propositions selon le groupe d'électeurs visés. Cependant, il ne peut exister de micro-targeting sans profilage et faire la différence entre les deux techniques n'est pas chose aisée. Le profilage se définit comme le traitement des données personnelles d'un individu en vue d'analyser et de prédire son comportement. Le profil individualisé établi est évidemment non statistique, possibilité écartée par Barack Obama dès 2008. Le profilage effectué, le micro-targeting peut être mis en œuvre et que ce soit par le biais d'un porte-à-porte individualisé grâce à la détention d'en moyenne 500 informations sur l'électeur – qui sont encore complétées à l'issue de l'entretien – ou par le biais de campagnes de télévision ciblées, ce système de gestion de la relation électeur a permis une croissance marquée du nombre de contributions par les petits donateurs – au-delà de se limiter à retenir l'attention des potentiels sympathisants –.

Cependant, il est difficile de savoir si, de prime abord, cela est rentable dans la mesure où la Commission Electorale Fédérale des Etats-Unis estime ce budget à 7 milliards d'euros[31].

Nous pouvons supposer que cela le devient dès lors que les réseaux sociaux s'allient à la propagande politique que mènent les candidats. Pour les élections présidentielles américaines de 2017, Youtube a rencontré la quasi-totalité des candidats pour leur proposer des chaînes de diffusion personnalisées. De même, la chaine de télévision ABC s'est associée à Facebook et a signé un accord avec celui-ci afin de fournir des flux d'information sociale pour chaque débat télévisé[32].

De la part de ces sociétés, cela semble opportun dans un contexte où les « news junkies » (les « accros de l'information » en français) augmentent considérablement l'utilisation des réseaux sociaux par les partis politiques[33]. Le problème est que le corollaire direct et naturel à la création de cette information politique n'est autre que la désinformation, mieux connue sous le nom de « Fake-news », terme qui sera dorénavant utilisé dans la suite de cette étude. La Fake-news est une information volontairement trompeuse, inexacte, truquée ou falsifiée. Il s'agit d'un faux article de presse publié sur un site d'actualité, faux ou non, destiné à abuser ou manipuler

[31] BILLE, J. Marketing politique et Big Data, *op.cit*
[32] DOSQUET, F. (dir.). *Marketing politique et communication politique*, *op.cit*.
[33] GALLARDO PAULS, B. y ENGUIX OLIVER, S. *Pseudopolítica: el discurso político en las redes sociales*. Valencia: Departamento de Teoría de los Lenguajes y Ciencias de la Comunicación, Universitat de València, 2016. 207 p.

l'électeur. Elle peut également avoir un but lucratif, mais dans le contexte électoral, cet objectif ne trouve pas vraiment à s'appliquer, bien qu'il existe.

A contrario du micro-targeting, la Fake-news est un outil puissant mais très peu onéreux et très rentable[34]. La campagne électorale de Donald Trump, en plus du micro-targeting, a également rendu cette pratique populaire. Cependant, nous n'irons pas jusqu'à avancer que l'actuel Président des Etats-Unis en a été l'initiateur direct et nous considérerons que son rôle a été entièrement passif dans la croissance de ce phénomène. Néanmoins, il est indéniable que les Fake-news ont influencé les votes en faveur – ou non – de Donald Trump[35].

Les Fakes-news sont souvent originaires d'un pays étranger à celui où se déroule le processus électoral, c'est pourquoi il est extrêmement difficile de lutter contre elles, d'autant plus que le contenu de ces dernières n'est en aucun cas illégal, et cela dépend sûrement du fait que les cadres législatifs en la matière sont quasi-inexistants. Ainsi naissent d'autres pratiques, des « petites sœurs » de la Fake-news qui sont tout autant, voire plus redoutables que celle-ci. Alliée à l'utilisation des données personnelles, la Fake-news peut devenir ciblée ou faire place au phénomène d'astroturfing. Ce dernier vise à simuler l'existence d'un ensemble d'internautes adhérant spontanément à une cause pour influencer de vrais citoyens[36]. Il s'agit souvent de faux comptes créés sur les réseaux sociaux, ou de comptes « robots » répondant à une programmation.

Force est de constater que la vie politique a été fortement modernisée par les pratiques américaines et ces dernières se sont déjà déployées jusqu'en Europe. L'affaire Cambridge Analytica a démontré l'importance de lutter contre l'opacité de l'information des personnes concernées sur l'usage de leurs données personnelles. De plus, il a lourdement affecté la liberté d'expression ainsi que la liberté de détenir des opinions et la possibilité de penser librement sans manipulation. C'est donc sans grande surprise que le public européen s'inquiète de l'arrivée de ces pratiques, et notamment de la protection de ses droits et libertés fondamentaux.

[34] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions* : « Lutter contre la désinformation en ligne, une approche européenne ». 26 avril 2018.
[35] "Fake news: contra las falsedades". *El país*, 12 de marzo de 2019
[36] CHAVALARIAS, D. « Fake news : l'arbre qui cache la forêt ». *AOC media*, 7 novembre 2018

Utilisation des réseaux sociaux dans la propagande française et espagnole

Dans le cadre de l'étude qui est menée, il ne semble pas approprié de s'intéresser à l'Union Européenne (ci-après dénommée l'UE) dans sa globalité. En effet, bien que le RGPD ait permis d'uniformiser la législation concernant la protection des données personnelles au niveau européen et que la Commission Européenne ait pris des mesures relatives au phénomène de Fake-news, il apparait davantage pertinent de s'intéresser à la législation nationale que les Etats-membres mettent en œuvre afin de sanctionner les utilisations abusives de cette propagande au sein de leur territoire.

Pour ce faire, notre réflexion portera uniquement sur la France et l'Espagne, pays voisins à la législation plus ou moins similaire puisque l'Espagne s'est fortement inspirée de ce qui existait en France afin de créer ses normes. Par ailleurs, il faut noter que tous deux ont été récemment concernés par des processus électoraux : l'élection présidentielle de 2017 pour la France et les élections générales de 2019 pour l'Espagne. En outre, Etats-membres de l'UE, ils ont aussi été concernés par l'élection européenne de 2019. Ainsi, ils se présentent comme les candidats idéaux pour notre étude.

Ces trois élections ont fait l'objet d'une forte médiatisation, et notamment d'une propagande digitale importante. Cela peut paraitre ironique car il faut rappeler que jusqu'en 1930, le visage et la voix des dirigeants d'Etats restent inconnus de la majorité des citoyens, et ce notamment à cause de la méfiance de ces derniers envers les médias dits « de masse »[37]. Aujourd'hui, cette époque est bel et bien révolue puisque les partis politiques ne les craignent plus et sont même devenus des utilisateurs très compétents de ces derniers.

« Vox », à titre d'exemple, est le parti politique espagnol avec le plus de « followers »[38] sur Instagram, le réseau social qui s'est le plus développé en 2018 selon un rapport de l'Association de la Communication Digitale en Espagne et le plus utilisé par les individus entre 16 et 30 ans. Vox, qui n'a créé son compte qu'en 2016, s'est parfaitement imprégné de ces données et cherche d'ailleurs à attirer les jeunes votants ainsi que les indépendantistes catalans. Comme cela s'est produit pour les partis politiques « Podemos » et « Ciudadanos », « Vox » s'est vu concéder une certaine présence parlementaire grâce à la propagande digitale qu'il a menée. Ce

[37] RIUTORT, P. *Sociologie de la communication politique*. Paris : La Découverte, collection « Repères », 2007, 121 p.
[38] Les personnes qui s'abonnent à un compte sur un réseau social

succès explique que les partis plus traditionnels, et pas seulement les partis politiques émergents, tentent eux-aussi de se saisir d'une telle opportunité et de sortir des sentiers conventionnels dans lesquels ils ont l'habitude de s'inscrire. Bien que plus populaires, ils ont également besoin de capter l'attention en diffusant leurs messages au travers de sympathisants et de détracteurs[39] et les réseaux sociaux se présentent comme la méthode la plus aisée pour y parvenir.

Ainsi, des partis politiques comme « les Républicains » (ancien « UMP ») ont eu recours en 2016 à des applications de stratégie électorale permettant d'identifier et de localiser des cibles électorales : ces dernières repèrent le sympathisant de droite qui a aimé ou retweeté[40] une publication et confirment leur intuition en croisant des dizaines de données collectées sur Facebook, Twitter, LinkedIn ou sur les listes électorales. Cela permet également de trouver l'adresse e-mail et de prospecter par ce moyen de communication par la suite. Trente millions d'e-mails ont de ce fait été envoyés par « les Républicains » et le « PS ». Ce mode de communication présente des avantages certains en ce que le ciblage peut se révéler précis, le coût est raisonnable et il est très facile de mesurer les taux d'ouverture des e-mails, les taux de clics et les renvois potentiels sur les sites web ou blogs de telle ou telle personnalité politique.

Cependant, ce sont les partis politiques émergents qui se démarquent finalement le plus sur les réseaux sociaux. Emmanuel Macron qui a fait le pari de créer son propre parti « En Marche ! » en est le meilleur exemple puisqu'il a su s'imposer et gagner les élections présidentielles françaises. Afin de mener sa propagande digitale, celui-ci a eu recours à la Société Big Data et à son logiciel de stratégie électorale ainsi qu'à la Poste et à l'INSEE en tant que « fournisseurs de données ». Il faut noter néanmoins qu'il s'est assuré au préalable de la légalité de ces pratiques auprès de la CNIL.

Les logiciels de stratégie électorale permettent d'optimiser la gestion des différentes données collectées par le candidat qui elles-mêmes permettent d'animer et de mobiliser les communautés en affinant la communication politique en fonction des profils des différents contacts et prospects[41]. Ainsi, les partis politiques « les Républicains » ou « En Marche ! » se

[39] VENTURA, B. "La fábrica de líderes: así contribuyen medios y redes sociales a elegir a los políticos". *Yorokubu*, 22 de noviembre de 2018
[40] Action de partager une publication sur twitter
[41] CNIL ET CSA. Guide : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». 2018.

sont vu proposer des services tels que des cartes interactives, des infographies, des bases de données interrogeables voire des plans de mobilisation[42].

La création et le développement de telles technologies ont été rendus possibles depuis maintenant quelques années grâce au phénomène du « Big data », souvent traduit pas « données massives ». Depuis l'apparition des nouvelles technologies, et notamment d'internet et des réseaux sociaux, environ 2,5 trillions d'octets de données sont produits par jour. De ce fait, les ensembles de données traités répondant aux caractéristiques de volume, vélocité et variété correspondent à la définition du Big data. Ce dernier permet aux dirigeants d'Etats de répondre à leurs deux besoins principaux, à savoir :

- La création d'une liste de citoyens, volontaires et donateurs à contacter ;
- La construction de modèles prédictifs pour faire des campagnes de propagande ciblée plus efficaces. Ces modèles sont basés sur trois scores différents : les scores de comportement (les comportements passés et les informations démographiques pour calculer des probabilités explicites que les citoyens vont s'engager dans des formes particulières d'activité politique), les scores de support (la prédiction des préférences politiques des citoyens) et les scores de réactivité (comment les citoyens vont-ils répondre aux programmes électoraux ?)[43].

Face à cette demande croissante de la part des politiques, de nombreux prestataires en Big data ont vu le jour tels que Liegey Muller Pons, Spallian, Emakira, Fédéravox, Netscouade, Databox…

C'est de cette quantité gargantuesque de données dont se nourrissent les dirigeants d'Etats, mais pas seulement. Il n'est pas rare d'omettre « l'Open data » (« données ouvertes » en Français) et c'est pourtant principalement par celui-ci qu'est alimenté le Big data. L'Open data est l'ensemble des données collectées par les organismes publics ou privés chargés d'un service public. Elles sont mises à disposition en format numérique sur des plateformes nationales ou locales, ce qui permet leur libre accès et leur réutilisation par les citoyens ou les organisations[44]. La loi dite « pour une République Numérique »[45] de 2016 a d'ailleurs considéré ces données

[42] THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *op.cit.*
[43] NICKERSON, D-W. and ROGERS, T. Political campaigns and Big Data. *Journal of Economic Perspectives*, 2014. Volume 28, n°2.
[44] LEHMANS, A. Les réinventions de la démocratie à l'aune de l'ouverture des données : du discours de la participation aux contraintes de la gouvernance. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.
[45] LOI n°2016-1321 *pour une république numérique*, 7 octobre 2016.

comme étant d'intérêt général. Mais cela n'a rien de surprenant en ce que cette affirmation s'inscrit dans la suite logique de la Directive dite « PSI »[46] sur la réutilisation des données publiques adoptée en 2003, de la création de la Plateforme data.gouv.fr en 2011 et de l'inscription de l'Open data comme principe gouvernemental en 2012.

Une telle affirmation s'explique également par le fait que le secteur public dispose d'informations sociales, économiques, géographiques et touristiques. Non seulement de telles données présentent un véritable avantage économique mais elles présentent aussi un véritable intérêt en ce qui concerne la garantie de la transparence de la vie publique. C'est pourquoi un droit de licence dit « ouvert » est concédé sur ces dernières : il s'agit d'un droit personnel, non exclusif et gratuit, de réutilisation des informations pour une durée illimitée[47]. Cependant, il va de soit que si ces données peuvent être réutilisées à des fins politiques, elles peuvent également l'être à des fins commerciales. Dans les deux cas, il est difficile de dire lequel des deux objectifs est le plus honorable mais le caractère politique de l'utilisation à des fins électorales lui permet au moins de ne pas quitter, en quelques sortes, le service public.

A priori, il ne parait néanmoins pas pertinent de se préoccuper du sort de ces données puisque, par définition, les données personnelles ne peuvent pas être des données publiques, que ce soit pour garantir le respect de la vie privée ou simplement pour respecter la condition *sine qua non* de l'Open data qui n'est autre que l'anonymat.

Malgré tout, il existe des exceptions à cette règle qui permettent de rendre publiques des données personnelles, à savoir :

- La personne y a expressément consenti ;
- Cela est prévu par une disposition légale ou réglementaire.

Le second point porte à controverse puisque, littéralement, cela signifie qu'un individu peut être contraint par la loi à diffuser des données personnelles et, qu'en cas de refus, il s'expose à une sanction pénale. C'était notamment le cas pour la déclaration de l'Impôt de Solidarité sur la Fortune (ci-après dénommé l'ISF) qui faisait l'objet d'une diffusion publique indirecte. Le problème qui se pose est qu'une identification indirecte est possible avec le croisement des données. De même, la base de données de l'INSEE, utilisée par Emmanuel Macron lors de sa campagne de 2017, qui est certes statistique, concerne des informations telles que l'emploi, le

[46] PARLEMENT EUROPEEN ET CONSEIL. *Directive 2003/98/CE sur la réutilisation des informations du secteur public*, 17 novembre 2003.
[47] BERGUIG, M. et COUPEZ, F. Faut-il réellement craindre l'open data pour la protection de nos données personnelles ? *Victoires éditions*, 2016. LEGICOM, n°56.

logement et l'immigration. Compte tenu de leur caractère hautement personnel, ces données présentent un risque réel de réidentification et il faut garder à l'esprit qu'avant d'être publiques ou statistiques, ces données sont bel et bien personnelles. Ainsi, il paraît indispensable de garantir un droit à l'oubli numérique et l'application de la notion de finalités incompatibles.

Cependant, peut-il être considéré que les données réutilisées dans le cadre d'une propagande électorale respectent la notion de finalités incompatibles alors même qu'elles ont été collectées pour une toute autre finalité par les services publics ? La question se pose davantage dès lors que l'utilisation de logiciels de stratégie électorale implique *de facto* l'utilisation d'algorithmes. Ces derniers sont des processus constitués par un ensemble d'opérations et de règles opératoires données pour un calcul. Ils entrainent nécessairement la prise d'une décision automatisée qui n'est autre que le résultat des calculs programmés et ce sont d'ailleurs eux qui permettent la mise à disposition de services comme ceux évoqués en aval.

Par conséquent, bien que le Big data électoral – intégrant aussi bien les données privées que l'Open data – soit mieux accepté en France depuis l'élection du Président Emmanuel Macron, il apparaît comme indispensable de réguler ces pratiques afin de ne pas tomber dans des schémas comme ceux qui ont frappé les Etats-Unis. En outre, bien que le phénomène des Fake-news n'ait pas été évoqué dans cette réflexion, il va de soi que la France et l'Espagne en ont également été les victimes. Néanmoins, celui-ci n'est véritablement dangereux pour les droits fondamentaux, notamment le droit à l'information et le droit à la vie privée qui sont au cœur de cette étude, que lorsqu'il fait l'objet d'un ciblage grâce à l'utilisation des données personnelles. C'est pourquoi notre pensée s'est essentiellement tournée vers cette dernière mais le phénomène de Fake-news n'est pas pour autant exclu d'une nécessité législative.

Insuffisance de la régulation française et espagnole en la matière

Face aux évolutions sociétales – dans lesquelles les innovations technologiques sont bien évidemment incluses – il est monnaie courante que la législation ne parvienne pas à anticiper et qu'elle intervienne après coup. C'est notamment le lot de la France et de l'Espagne qui, d'un point de vue constitutionnel, n'ont mis en œuvre aucune modification pouvant permettre une adaptation juridique au contexte actuel.

En effet, la propagande est toujours définie, dans les textes constitutionnels, comme l'action exercée sur l'opinion par le biais de tracts publicitaires, de la radio ou de la télévision pour l'amener à avoir et à appuyer certaines idées politiques. Bien que ces moyens de communication

soient en effet toujours utilisés, il est évident qu'il n'est plus l'outil préféré des dirigeants d'Etats souhaitant promouvoir leurs partis et programmes électoraux, les réseaux sociaux ayant pris une place centrale dans la mise en œuvre de cette propagande.

A ce titre, l'Espagne a tout de même tenté de réagir en modifiant, suite à l'adoption en novembre 2018 de la Ley Orgánica de Protección de Datos[48] (« Loi Organique de Protection des Données » en français, ci-après dénommée la LOPD), sa Ley Orgánica del Régimen Electoral General[49] (« Loi Organique du Régime Electoral Général » en français, ci-après dénommée la LOREG) et notamment en y insérant à l'article 58 bis l'un de ses principes qui permet aux partis politiques de faire du SPAM électoral et de la propagande personnalisée sur internet. Ainsi, avec l'approbation de cette loi, les pratiques suivantes deviennent légales :

- L'élaboration de profils idéologiques de votants ;
- La prise de contact avec les votants de manière privée ;
- L'envoi de propagande personnalisée[50].

Le dernier point se veut volontairement générique – « propagande » – car il peut finalement aussi bien concerner des messages ou du porte-à-porte personnalisés que des Fake-news ciblées. Ces dernières, qu'elles soient personnalisées ou non, ne font pas davantage l'objet de régulation constitutionnelle. En termes de communication audiovisuel, seuls des principes tels que la gestion du temps de parole de chaque candidat aux élections sont prévus. Même si cela ne semble être qu'un moindre mal, il faut néanmoins noter qu'une telle règle est difficilement applicable aux réseaux sociaux. Cela implique donc, que selon leurs moyens, les partis peuvent être plus ou moins avantagés et de fait, l'électeur plus ou moins influencé. Finalement, les Fake-news qui ne font pas l'objet d'un ciblage sont peut-être les plus dangereuses puisque, *a contrario,* les Fakes-news individualisées font au moins l'objet d'une régulation relative à l'utilisation des données personnelles et voient ainsi leur impact limité.

Cette régulation plus importante vise tout particulièrement à faire face à des phénomènes issus des réseaux sociaux comme ceux de la « bulle filtrante » et de la « chambre d'écho ». En effet, ces derniers portent finalement une lourde atteinte au principe fondamental du pluralisme politique qui repose sur la représentation de différents partis politiques, permettant ainsi aux

[48] LEY ORGANICA 3/2018 *de protección de datos personales y garantía de los derechos digitales*, 5 de diciembre de 2018.
[49] LEY ORGANICA 5/1985 *del régimen electoral general*, 19 de junio de 1985.
[50] DEL CASTILLO, C. y SARABIA, D. "Aprobada la ley que permitirá a los partidos hacer spam electoral y propaganda personalizada en internet". *El diario,* 21 de noviembre de 2018

électeurs de bénéficier d'une liberté de choix. La bulle filtrante et la chambre d'écho ont pour effet, par le biais d'un algorithme de recommandations, de personnaliser les fils d'actualité[51] des électeurs en fonction de leurs préférences déduites de leurs données personnelles collectées.

Le pluralisme politique n'est pas le seul principe a être touché négativement par ces nouvelles pratiques, et bien que l'électeur puisse toujours exercer son droit d'opposition aux différents traitements de données personnelles permettant la mise en œuvre d'une telle propagande, il sera mis en évidence que d'autres droits et principes aussi bien fondamentaux que démocratiques sont mis à mal par celle-ci, notamment le droit à l'information et le droit à la vie privée. Un recours d'inconstitutionnalité contre l'article 58 bis de la LOREG a d'ailleurs été exercé début mars 2019 par le Defensor del Pueblo (« Défenseur du peuple » en français), dont le dénouement sera détaillé plus en tard.

Une telle action a été rendue possible car, au-delà du fait que la propagande ciblée ne soit pas régulée en elle-même, le droit à la protection des données personnelles a acquis, depuis sa consécration à l'article 8 de la Charte des Droits Fondamentaux de l'UE (ci-après dénommée la CDFUE) et à l'article 16 du Traité sur le Fonctionnement de l'UE (ci-après dénommé le TFUE), une place autonome parmi les droits fondamentaux[52].

Avant d'être autonome, il s'inscrivait dans le droit au respect à la vie privée, ce qui rendait sa protection moins efficiente, même si dans son arrêt Safe Harbor[53], la Cour de Justice de l'UE (ci-après dénommée la CJUE) a considéré que « la protection des données à caractère personnel [joue un rôle important] au regard du droit fondamental au respect de la vie privée ». Finalement, le droit à la protection des données personnelles ne faisait que servir le droit au respect de la vie privée. Dorénavant, l'article 8 de la CDFUE précise que « le droit à la protection des données personnelles des citoyens de l'UE constitue un droit fondamental corollaire du droit au respect de la vie privée et, à ce titre, bénéficie d'un niveau élevé de protection ». En fin de compte, le droit à la protection des données personnelles se présente maintenant comme une conséquence du droit au respect de la vie privée, et il n'existe plus d'interdépendance entre ces derniers (une action en justice peut être menée sur le fondement du droit au respect à la vie privée sans impliquer le droit à la protection des données personnelles, et vice-versa).

[51] Disponibles sur tous les réseaux sociaux.
[52] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *Victoires éditions*, 2016. LEGICOM, n°56
[53] COUR DE JUSTICE DE L'UNION EUROPENNE. Affaire 362/14 dite « Safe Harbor », 6 octobre 2015.

Ainsi, de nombreux textes mettent aujourd'hui en œuvre la protection des données personnelles :

- Au niveau européen : le RGPD, la réglementation « e-Privacy » et les lignes directrices du Groupe de Travail de l'article 29 du RGPD, réunissant les autorités de contrôle de tous les Etats-membres de l'UE (ci-après dénommée le GT29) ;
- Au niveau national : la LIL et la LOPD.

Malgré tout, la protection qu'offrent ces textes reste générique et ils ne s'intéressent jamais vraiment à l'utilisation des données dans le cadre politique, et notamment électoral. Elle se veut donc insuffisante en la matière et, comme vu précédemment, elle porte atteinte à des principes démocratiques essentiels tels que le principe du pluralisme politique.

Malheureusement, ce n'est pas le seul pluralisme qui est atteint ; le pluralisme des médias l'est aussi. Si d'une part, il peut être considéré que les réseaux sociaux tendent à diversifier les offres de sources informationnelles, d'autre part, il peut aussi être considéré qu'ils contribuent à leur raréfaction avec le phénomène de bulles filtrantes. Ainsi, l'utilisateur ne se voit offrir que des informations provenant de médias correspondant à ses opinions politiques et, dans la mesure où presque 50% de la population s'informe sur les réseaux sociaux, lutter contre cet « isolement médiatique » se présente comme un enjeu majeur pour les gouvernements afin de garantir le droit de chercher librement l'information, de la diffuser et d'y avoir accès. En outre, et de façon assez ironique, les réseaux sociaux se gardent bien de contrôler et de sanctionner les Fake-news.

Pourtant, fournir aux citoyens une information « vraie » fait également parti des grands principes sur lesquels se fondent nos démocraties. Les médias sont en effet chargés d'une mission d'intérêt public concernant la diffusion d'une information honnête et complète et comme le mentionne le Rapport de la commission Kent rendu en 1981 : « La liberté de la presse n'est pas l'apanage des propriétaires de médias. Elle est un droit du peuple. Elle s'inscrit dans le droit à la libre expression, inséparable du droit à l'information ».

A ce titre, la France a adopté le 22 décembre 2018 une loi dite « Fake-news »[54] visant à lutter contre la manipulation de l'information, notamment en contexte électoral. Les actions de désinformation sont ainsi sanctionnées mais pour autant, cela ne semble pas suffisant sans un apprentissage citoyen visant à favoriser l'identification et la dénonciation des Fake-news, le phénomène étant difficilement contrôlable. A contrario, l'Espagne n'a encore pris aucune

[54] LOI n°2018-1202 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

mesure relative aux Fake-news mais il ne peut lui être reproché un quelconque retard puisque la France n'a de son côté pris aucune mesure, même obsolète, visant à réguler l'utilisation des données personnelles dans le cadre des campagnes électorales.

Au niveau national, seules la LOPD et la LIL se présente comme des remparts face aux potentiels abus politiques. N'étant finalement que des transpositions plutôt fidèles du RGPD, lui aussi insuffisant en matière de protection, l'intérêt est moindre. Bien que celui-ci prévoit, dans son considérant 56 et dans son article 9, une protection des données dites « sensibles » incluant les données relatives aux opinions politiques, les nombreuses exceptions existantes rendent ladite protection peu efficiente.

Face à une telle insuffisance législative, comment garantir la pérennité de nos principes démocratiques encadrant la mise en œuvre des campagnes électorales et l'élection des dirigeants d'Etats français et espagnol ?

Sans avoir la prétention de proposer un cadre à la propagande électorale actuelle qui s'exerce principalement par et grâce aux réseaux sociaux, ainsi qu'aux innovations techniques et technologiques qu'ils proposent, cette étude analysera les lacunes des régulations en vigueur, qu'elles soient européennes, constitutionnelles ou législatives, et les tentatives qu'elles font pour canaliser ces pratiques mettant en péril les droits et libertés fondamentaux. Pour ce faire, il convient de s'intéresser à la propagande électorale qui se mène de manière généralisée par le biais des Fake-news, mais davantage encore, il faut se pencher sur le danger que ces dernières représentent pour le droit fondamental à l'information (**PARTIE 1**), premier droit essentiel au bon fonctionnement de nos processus démocratiques. Ensuite seulement, après avoir pris connaissance du caractère néfaste que représente une information disséminée sur les réseaux sociaux, sans pour autant être individualisée, il sera possible de s'interroger sur la propagande électorale ciblée. En effet, en raison de l'utilisation des données à des fins politiques, celle-ci représente une grave atteinte au droit à la protection des données personnelles (**PARTIE 2**), garant des autres droits fondamentaux qui, eux aussi, seront au cœur de toute notre attention.

PARTIE 1. Propagande électorale généralisée : la mise en danger du droit fondamental à l'information par le phénomène des Fake-news

Le phénomène de Fake-news, rendu célèbre grâce – ou plutôt à cause – du scandale Cambridge Analytica et de l'élection de Trump, représente un véritable danger pour nos principes démocratiques et notamment, notre droit à l'information. Néanmoins, avant de pouvoir analyser les lacunes juridiques et de faire des propositions de régulation aux fins d'éviter un débordement de ce phénomène (**TITRE 2**) – à supposer que cela ne s'est pas déjà produit – il faut se pencher sur l'inscription de ce dernier dans notre notion actuelle de propagande électorale (**TITRE 1**). En effet, cette dernière fait surtout l'objet d'une régulation constitutionnelle. L'ennui est que celle-ci se veut particulièrement obsolète en la matière et peu adaptée à un phénomène si récemment connu du public comme celui de la Fake-news.

TITRE 1. Inscription du phénomène des Fake-news dans notre notion actuelle de propagande électorale

Le phénomène de Fake-news inquiète, certes, parce qu'il est un outil redoutable de manipulation de l'opinion, mais surtout parce qu'il porte directement atteinte au droit à l'information ainsi qu'à d'autres principes démocratiques français et espagnols (**Chapitre 2**) comme, par exemple, la liberté d'expression. Bien éloigné des conceptions actuelles qu'ont les droits français et espagnol de la propagande (**Chapitre 1**), la Fake-news est une notion difficilement apprivoisable en raison des nombreuses formes qu'elle peut prendre. Sa régulation en est ainsi d'autant plus complexe et délicate, ce qui n'explique qu'en partie la lenteur des gouvernements à agir en la matière.

Chapitre 1. Les notions actuelles de la propagande en droit français et espagnol

Dans l'imaginaire collectif, la propagande politique est un processus néfaste pour la démocratie qui a pour objectif de manipuler le consentement de l'électeur (**1.2**) et qui n'est mis en œuvre que dans les pays dictatoriaux. Cependant, elle n'est autre que la tentative de convaincre les électeurs et, à ce titre, elle se présente comme une forme normale d'organisation de la vie politique. Ainsi, une fois que son acception neutre lui est rendue, on s'aperçoit qu'elle existe dans nos démocraties française et espagnole qui tentent, ou pas finalement, de la réguler

constitutionnellement (**1.1**). Depuis l'arrivée des réseaux sociaux, l'espace public ne cesse de s'élargir et, posé comme référence normative de la communication politique – et donc de la propagande –, il représente la plus grande difficulté que rencontrent les gouvernements souhaitant réguler la propagande.

1.1. Régulation constitutionnelle de la propagande électorale

Lorsqu'un pays procède à l'élection d'un nouveau dirigeant d'Etat, une campagne électorale est systématiquement menée *a priori*. L'article 50 de la LOREG définit la campagne électorale comme l'ensemble des activités licites menées par les candidats, partis, fédérations, coalitions et groupes politiques dans le but de capter les suffrages des électeurs. Basée sur la communication politique, qui est l'ensemble des processus de communication qui soutiennent une démocratie, la campagne électorale – ou la propagande électorale comme nous préférons la nommer – tente ainsi d'orienter le vote de l'électeur qui lui se présente comme le processus politique nécessaire au maintien de la démocratie[55].

La démocratie, quant à elle, se caractérise par l'expression de la volonté du peuple au travers de ses gouvernants. Dans cette optique, il se soumet à une légalité constituée. Cependant, une telle soumission est-elle légitime dès lors que la propagande influe sur le vote des électeurs et donc, sur la volonté qu'il souhaite exprimer ?

Les informations transmises par la télévision ont la capacité de modifier les indices de valorisation du public sur les électeurs et sur les gouvernants. Ainsi, quand la manipulation d'opinion est si aisée, il devient indispensable de contrôler la propagande électorale. De surcroît, la télévision qui vient d'être prise en exemple ne fait qu'émettre des images pour un spectateur passif qui les regarde, alors que le cyberespace est un monde interactif avec des utilisateurs dynamiques[56]. Ainsi, les réseaux sociaux permettent l'exercice effectif de la démocratie inclusive, participative et représentative de tous les citoyens (participation égale des jeunes, des femmes et des autres minorités habituellement non représentées). Néanmoins, ils rendent dangereux l'impact de la propagande électorale sur ces derniers, dans la mesure où tout citoyen, sur les réseaux sociaux, peut produire sa propre propagande, une propagande qui ne répond bien évidemment pas aux règles constitutionnelles fixées par les gouvernements. De

[55] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. Montréal : Doctorat en Communication, Université du Québec à Montréal, 2012. 359 p.
[56] PIEDRA CARDOSO, J. Democracia y redes sociales. *Universidad Verdad*, 2017. 1(72).

cette manière, les minorités habituellement non représentées ont découvert qu'elles pouvaient influencer la majorité dans le sens de ses intérêts.

A ce titre, Bernays, dans son ouvrage *Propaganda* (1928), affirme très justement que « la propagande est l'organe exécutif du gouvernement invisible », à savoir les minorités politiques. Il la définit, dans son sens large, comme tout effort systématique et organisé afin de propager une croyance ou une doctrine particulière, ou afin d'obtenir le soutien du grand public pour une opinion ou une ligne d'action. Dans cette conception, la propagande électorale se présente finalement comme une forme parfaitement légitime de l'organisation humaine et elle ne devient mauvaise et répréhensible que lorsque ses auteurs s'emploient délibérément et en connaissance de cause à propager des mensonges, ou à produire des effets préjudiciables au public[57].

En bref, pour savoir si la propagande est un bien ou un mal, il faut d'abord se prononcer sur le mérite de la cause qu'elle sert et sur la justesse de l'information publiée. L'ennui avec les réseaux sociaux est que de nombreux abus existent et ce notamment, comme énoncé plus tôt, parce que les règles applicables à la propagande électorale ne trouvent pas à s'appliquer à celle-menée sur ces supports. En effet, d'un point de vue constitutionnel, la régulation en la matière, que ce soit en France ou en Espagne, est particulièrement obsolète.

En France, l'article 1er de la loi dite « Léotard » du 30 septembre 1986[58], garantie le respect du caractère pluraliste de l'expression des courants de pensée et d'opinion. Pour ce faire, il s'assure de l'expression la plus diverse possible des partis ou personnages politiques avec un temps de parole équilibré entre ces derniers. Cela permet notamment que l'information soit diversifiée afin de permettre à chacun de forger librement sa propre opinion. Bien que cette loi n'ait pas une valeur constitutionnelle, le Conseil Constitutionnel a estimé en 1986, puis en 1989, que « le respect du pluralisme est l'une des conditions de la démocratie » et plus largement qu'il « constitue le fondement de la démocratie »[59].

La loi relative à l'élection du Président de la République du 6 novembre 1962[60] s'intéresse également au principe du pluralisme politique. A proprement parler, elle n'a pas non plus une valeur constitutionnelle mais son article 3 – celui qui nous intéresse en l'espèce –, ayant été remplacé par l'article 15 de la loi organique relative au renforcement de l'organisation des

[57] BERNAYS, E. *Propaganda : comment manipuler l'opinion en démocratie*. *op.cit.*
[58] LOI n°86-1067 *relative à la liberté de communication*, 30 septembre 1986.
[59] CNIL ET CSA. Guide : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». *op.cit.*
[60] LOI n°62-1292 *relative à l'élection du Président de la République au suffrage universel*, 6 novembre 1962.

juridictions[61], a acquis une telle force. En effet, une loi organique est une loi complétant la Constitution afin de préciser l'organisation des pouvoirs publics. Elle est, dans la hiérarchie des normes, placée en dessous de la Constitution mais au-dessus des lois ordinaires. Ainsi, dans le paragraphe I bis de son article 3, elle s'assure que « les éditeurs de services de communication audiovisuelle respectent, sous le contrôle du Conseil Supérieur de l'Audiovisuel (ci-après dénommé le CSA), le principe d'équité en ce qui concerne la reproduction et les commentaires des déclarations et écrits des candidats et la présentation de leur personne ».

Afin de déterminer un temps de parole et d'intervention équitable entre les partis politiques comme le souhaite la loi de 1962, le CSA doit tenir compte de la représentativité des candidats en fonction des résultats obtenus aux plus récentes élections et de la contribution de chacun de ces derniers à l'animation du débat électoral. Pour rendre compte de ce partage équitable entre les partis politiques, le CSA publie, au moins une fois par semaine, le relevé des temps consacrés à la reproduction et au commentaire des déclarations et écrits des candidats à la présentation de leur personne.

De la même manière en Espagne, les articles 60 et 61 de la LOREG disposent que les partis, fédérations, coalitions et groupes politiques ont droit à des espaces gratuits de propagande dans les émissions de télévision et de radio de propriété publique durant la campagne électorale. Le respect du pluralisme y est assuré par la Comisión de Radio y Televisión (« Commission de Radio et Télévision » en français, ci-après dénommé la CRT). En revanche, le partage du temps de parole et des interventions se fait uniquement en fonction de numéro total de votes qu'ils ont obtenu au cours des dernières élections équivalentes, et non en fonction de leur contribution à l'animation du débat électoral – cette dernière condition est, en effet, relativement subjective et la contribution des différents dirigeants d'Etats semble également difficilement quantifiable –. Le CRT a ainsi fait le choix de définir un temps de parole et d'intervention précis pour chaque parti politique selon le nombre de votes qu'il a obtenu aux dernières élections.

Si nous sommes contraints de nous intéresser à des lois organiques plutôt qu'aux Constitutions française[62] et espagnole[63] en elles-mêmes, c'est notamment parce que ces dernières se désintéressent totalement de la propagande nécessairement menée en parallèle des élections. En effet, elles ne se préoccupent des élections du dirigeant d'Etat que dans leurs aspects procéduraux : par exemple, pour la France, on y retrouve les modalités d'élection du Président

[61] LOI ORGANIQUE n°2019-221 *relative au renforcement de l'organisation des juridictions*, 23 mars 2019.
[62] CONSTITUTION FRANCAISE, 4 octobre 1958.
[63] CONSTITUCION ESPAÑOLA, 6 de diciembre de 1978.

de la République Française ainsi que la durée de son mandat et, pour l'Espagne, on y retrouve les modalités d'élection du Chef du Gouvernement. Loin d'être exhaustifs, ces exemples permettent d'illustrer l'indifférence des Constitutions pour la régulation de la propagande électorale, qu'elles renvoient aux lois organiques. Cela explique notamment le manque d'adaptation aux nouvelles pratiques de ces deux pays.

En ce qui concerne la France, sa loi de 1962 a fait l'objet de nombreuses modifications. Des articles du Code Electoral ont notamment été intégrés à son article 3. A l'origine, ce Code ne concerne pas les élections présidentielles mais celles des députés, des conseillers départementaux, des conseillers municipaux, des conseillers communautaires et des sénateurs des départements. Dans le cadre de cette réflexion, il convient de ne s'intéresser qu'au Livre Ier du Code relatif aux députés, conseillers départementaux, conseillers municipaux et conseillers communautaires, et ce notamment parce que la loi de 1962 renvoie directement à son Chapitre V s'intéressant à la propagande.

En effet, bien qu'il traite majoritairement de la propagande traditionnelle – à savoir la propagande papier, télévisée ou radio –, il évoque tout de même à plusieurs reprises (articles L48-1 et L49 par exemple) « la propagande électorale diffusée par tout moyen de communication au public par voie électronique ». De même, dans son article L49-1, il s'intéresse aux systèmes automatisés d'appels téléphoniques. Cela traduit une volonté d'adaptation aux nouvelles technologies et aux nouvelles pratiques politiques qui en découlent. Néanmoins, quand on s'intéresse à la partie règlementaire qui est attachée à cette partie législative, on s'aperçoit qu'aucun cadre n'est donné en ce qui concerne l'usage de ces nouvelles techniques et technologies et, pire encore, elle ne s'intéresse qu'à la propagande politique papier qui semble être aujourd'hui totalement désuète. Ainsi, au-delà d'être en retard sur l'évolution sociétale à laquelle la démocratie française est confrontée, le Code Electoral ne propose qu'une solution partielle de régulation des nouvelles pratiques de propagande électorale puisqu'il ne donne aucune référence règlementaire pouvant permettre leur contrôle. De surcroît, les réseaux sociaux n'y sont que très peu mentionnés et ce, grâce à la loi Fake-news adoptée il y a peu.

La loi Fake-news est en effet la seconde modification apportée à la loi de 1962. Adoptée en deux textes, son premier est une loi organique[64] portant modification de l'article 4 de la loi suscitée. Néanmoins, elle n'est d'aucun intérêt pour ce développement puisqu'elle ne

[64] LOI ORGANIQUE n°2018-1201 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

s'intéresse pas à la propagande électorale. Son second texte en revanche, qui est une loi sans valeur constitutionnelle, montre davantage d'intérêts puisqu'il aborde pour l'une des premières fois les réseaux sociaux dans leur conception actuelle et également parce qu'il a permis la modification de certains articles du Code Electoral. Malgré tout, le second texte de la loi Fake-news fera l'objet d'un développement postérieur puisqu'il ne relève que du droit privé, et non du droit constitutionnel, comme l'est le but de ce chapitre.

En ce qui concerne l'Espagne, la LOREG dispose dans son article 50 que la campagne institutionnelle est destinée à informer les citoyens sur la date de vote ainsi que sur la procédure pour voter, sans influencer l'orientation du vote des électeurs. Cependant, il ne s'agit là que de la campagne institutionnelle et dès lors que la LOREG s'intéresse à la campagne électorale, la notion d'influence du choix des électeurs disparaît. De prime abord, cela semble assez logique puisque l'objectif même de la campagne électorale et de la propagande n'est autre que convaincre l'électeur. Cependant, au même titre que la loi française, un cadre devrait être posé en la matière afin d'éviter les abus.

C'est notamment ce qui s'est passé avec son article 58 bis qui, certes, a le mérite d'évoquer les réseaux sociaux et l'utilisation des données personnelles à des fins de propagande électorale ciblée mais qui a aussi rapidement fait l'objet d'une indignation publique au vu de l'atteinte au droit à la vie privée et à la protection des données personnelles qu'il engendrait. Son premier alinéa a depuis été annulé, et bien qu'insuffisant, nous reviendrons sur la décision prise par le Tribunal Constitucional (« Conseil Constitutionnel » en français) plus tard dans le développement.

Au-delà des droits fondamentaux auxquels il porte préjudice, l'article 58 bis suscite surtout l'inquiétude pour le champ des possibles qu'il ouvre : plus que jamais, les dirigeants d'Etats ont le pouvoir de manipuler l'opinion des électeurs et ce grâce aux informations personnelles de ces derniers dont ils disposent librement en vertu d'une loi à valeur constitutionnelle.

1.2. Manipulation du consentement des électeurs et élargissement de l'espace public « numérique »

Quand nous évoquons la propagande politique dans les médias, et cela concerne également les réseaux sociaux qualifiés de « nouveaux médias », nous viennent immédiatement à l'esprit des pays tels que la Corée du Nord, l'Iran ou le Kazakhstan. Pourtant, l'exemple donné par l'élection de Donald Trump et par la stratégie qu'il a mis en œuvre afin que sa campagne

électorale soit un succès nous démontre qu'elles existent également dans nos pays d'Amérique et d'Europe.

En effet, si la mission des médias est de donner une information objective et complète au public pour qu'il puisse participer de façon éclairée au processus politique, Noam Chomsky et Edward Herman démontre qu'il n'en est rien dans leur ouvrage *Manufacturing consent* (1988)[65]. Dans celui-ci, ils énumèrent les 5 filtres permettant de fabriquer le consentement du public à un régime politique :

- Taille, actionnariat, orientation lucrative : « la limitation de l'accès à la propriété d'un média avec une certaine diffusion si l'on ne dispose pas de moyens considérables, du fait de coûts rédhibitoires ». En résumé, il s'agit du contrôle qui ne peut être exercer que par les personnes les plus riches et donc, influentes. Un parti politique avec de grands moyens peut donc opérer un choix dans l'information qui est diffusée, au détriment des plus petits.
- La régulation par la publicité : « la cible des médias n'est plus pensée en fonction de la ligne éditoriale mais en fonction de son pouvoir d'achat, que le média va vendre aux publicitaires, et non ceux voulus par les journalistes ».
- Sources d'information : « dépendance informationnelle des médias de sources comme les gouvernements, les collectivités, les institutions, les entreprises et sociétés commerciales ».
- Contre-feux et autres moyens de pression : un lobbying direct ou indirect est exercé par les « personnes influentes », ce qui empêche finalement les médias d'émettre une opinion contraire à celle que ces dernières souhaitent véhiculer.
- L'anticommunisme : l'œuvre ayant été écrite en 1988, celui-ci représentait à l'époque le « mal-absolu ». De manière plus générale, ce dernier filtre consiste à désigner un ennemi (l'immigration ou le terrorisme par exemple) qui fasse oublier les problèmes de l'intérieur.

Les médias traditionnels ne seraient donc pas si indépendants qu'ils devraient l'être. Néanmoins, le constat fait par Noam Chomsky et Edward Herman reste à tempérer. Il faut en effet prendre en compte que l'ouvrage a été écrit en 1988, qu'il est peu adapté au contexte médiatique et politique actuel et qu'il est fortement politisé. De plus, il se base uniquement sur

[65] CHOMSKY N. et HERMAN, E. *Manufacturing consent : the political economy of the mass media*. New York : Pantheon Books, 1988.

les médias américains et il est bon de rappeler que, dans ce milieu, les acteurs privés sont plus nombreux aux Etats-Unis qu'en France ou en Espagne. Cependant, un tel schéma peut trouver à s'appliquer aux réseaux sociaux qui sont animés par un fort but lucratif. S'il ne nous est pas non plus possible d'affirmer qu'une telle technique de manipulation est appliquée en France et en Espagne, il nous est néanmoins possible de relever les quatre fonctions de manipulation que proposent ces réseaux sociaux aux partis politiques :

- Créer des « trending topics » (« sujet tendance » en français) en utilisant des hashtags[66] qui sont par la suite amplifiés par des comptes robots ;
- Identifier les hashtags réels et prévoir les attaques des comptes affiliés, qu'ils soient faux ou non ;
- Identifier les « trolls »[67] ou les comptes d'opposants ;
- Augmenter artificiellement les mentions « j'aime » du compte d'un politique[68].

Au-delà de ces nouvelles fonctions de manipulation que proposent les réseaux sociaux, il faut aussi souligner que ces derniers ont considérablement agrandi l'espace public. Utilisé comme référence normative pour la communication en démocratie, les auteurs parlent aujourd'hui d'espace public « numérique ». Légiférer dans un champ d'application si grand n'est pas chose aisé pour les gouvernements.

Jürgen Habermas, philosophe allemand, définit l'espace public comme le processus au cours duquel le public, constitué par les individus faisant usage de leur raison, s'approprie la sphère publique contrôlée par l'autorité et la transforme en une sphère où la critique s'exerce contre le pouvoir de l'Etat. C'est, en bref, un lieu situé entre l'Etat et la société civile où les citoyens privés se rassemblent, formant ainsi un public qui peut discuter librement et rationnellement[69].

A contrario de ce qui a été vu précédemment, les réseaux sociaux semblent ainsi renforcer la démocratie parce qu'ils permettent la communication entre les citoyens et entre les partis politiques et les citoyens. A ce titre, ils se présentent comme des outils importants d'information au service, certes, de la démocratie mais aussi, plus particulièrement, de la liberté d'expression[70]

[66] Utilisation du symbole « # » avant un mot pour accéder à un lien où sont regroupées toutes les publications référencées sous ce mot.
[67] Personne qui poste des messages tendancieux sur les forums internet afin d'alimenter les polémiques.
[68] GALLARDO PAULS, B. y ENGUIX OLIVER, S. *Pseudopolítica: el discurso político en las redes sociales*. *op.cit.*
[69] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. *op.cit.*
[70] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*

– qui, comme nous le verrons plus tard, est au centre des préoccupations de nos dirigeants d'Etats –.

Du point de vue des hommes politiques, la participation citoyenne sur les réseaux sociaux a également le grand avantage de nourrir l'Open data – et le contraire est aussi vrai : l'Open data nourrit la participation citoyenne –[71]. Là aussi, elle permet la stimulation de la démocratie et confère aux dirigeants d'Etats de nouveaux moyens d'agir. En ce qui concerne l'Open data, la loi pour une République Numérique a considéré qu'il s'agissait de données d'intérêt général en ce qu'elles garantissent une certaine lisibilité de l'espace public.

Un questionnement se pose sur le rôle de ces données personnelles (bien qu'appartenant aux données publiques, elles sont personnelles à l'origine) dans le fonctionnement de la démocratie contemporaine. Les dispositifs permettant l'accès à ces données répondent à une logique de gouvernance administrative et économique plus que démocratique. Néanmoins, et bien que l'Open data nourrit la participation citoyenne et interroge sur la possibilité de celle-ci à gérer le cycle de vie de l'information, deux types de légitimités contradictoires entrent en jeu :

- La première axée sur la démocratie et le dialogue autour de la thématique de la participation ;
- La seconde axée sur l'expertise technique et l'efficacité autour de la modernisation et de l'innovation, ce qui répond davantage à un schéma capitaliste plutôt qu'à un schéma utopiste.

En effet, du point de vue des politiques publiques, les données ouvertes reposent sur la mise en œuvre de principes affichés de transparence, de participation citoyenne et de modernisation de l'action publique par la collaboration entre les institutions et les citoyens. Cependant, un problème se pose quand la SNCF, UBER et AIRBNB, en tant que citoyens, communiquent sur l'ouverture de certaines de leurs données[72]. Dans cette hypothèse, la question qui reste en suspend est de savoir quelles données ces sociétés vont-elles rendre publiques : les leurs ou celles de leurs clients ? En effet, si cette question se pose, c'est notamment parce que les enjeux politiques de l'ouverture des données sont fortement liés à des questions économiques dans le cadre global du Big data qui, lui, s'alimente de cet Open data.

[71] LEHMANS, A. Les réinventions de la démocratie à l'aune de l'ouverture des données : du discours de la participation aux contraintes de la gouvernance. *op.cit.*
[72] *Ibid.*

En bref, l'espace public « numérique » ne fait que s'étendre puisque s'entremêlent l'Open data, le Big data, les données des sociétés et les données personnelles des individus… Cela explique que le concept soit flou et qu'en tant que référence normative, il se veut peu aisé pour les gouvernements de l'apprivoiser. Ainsi, sans pouvoir proposer une régulation satisfaisante, et parce que les citoyens contribuent à élargir chaque jour un peu plus cet espace public, des abus naissent. Le premier est celui de la désinformation qui nuit gravement à la participation citoyenne, à la démocratie et à certains droits et libertés fondamentaux.

Chapitre 2. La mise en danger du droit fondamental à l'information et des principes démocratiques français et espagnols par le phénomène de Fake-news

Avant de pouvoir constater l'insuffisance des régulations française et espagnole (**2.3**) en ce qui concerne le phénomène de Fake-news, insuffisance qu'elles justifient notamment par la crainte d'interférer avec la liberté d'expression, il faut d'abord s'intéresser de manière générale à ce phénomène complexe et tenter de lui donner la définition la plus précise qu'il soit (**2.1**). C'est au fur et à mesure de son étude qu'apparaît le danger qu'il représente pour le droit fondamental à l'information, pierre angulaire de la démocratie, ainsi que pour les principes essentiels de celle-ci (**2.2**).

2.1. Présentation et analyse du phénomène de Fake-news

Avant de s'intéresser aux propositions qui peuvent être faites en matière de législation ou en matière sociétale, il convient de s'intéresser au phénomène des Fake-news de manière générique. En effet, sans une définition précise de ce dernier et une connaissance solide de ses origines et de ses impacts, il semble difficile de l'appréhender.

Née en 1999 de l'émission satirique et parodique américaine le « Daily Show », la Fake-news est une information volontairement trompeuse, inexacte, truquée ou falsifiée. Ce faux article de presse, publié sur un faux site d'actualité ou non, est destiné à abuser ou à manipuler l'électeur[73]. Si cette définition a été retenue, c'est notamment parce qu'elle se veut particulièrement complète. Elle prend en compte toutes les méthodes de manipulation de l'information utilisées, les supports sur lesquels elle est publiée ainsi que ses objectifs premiers.

Grâce à cette définition, on note aisément que la Fake-news naît d'une intention délibérée de tromper et non d'une maladresse. Cette intention de tromper peut avoir un but politique ou un but lucratif. Dans ce dernier cas, il existe systématiquement un impact politique, même involontaire. Ainsi, de manière générale, le schéma est le suivant : si la Fake-news a été créée à des fins politiques, elle aura un effet économique et si elle a été créée à des fins économiques, elle aura un effet politique[74].

En ce qui concerne la maladresse, il faut tout de même remarquer qu'elle peut exister lorsque les journalistes diffusent une Fake-news sans la vérifier. C'est de cette façon que celle-ci peut

[73] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[74] JAYSON, H. (trad : RICHET, I.). Un guide critique des fake-news : de la comédie à la tragédie. *Le Seuil*, 2018. Pouvoirs, n°164.

se retrouver publiée sur un véritable site d'actualité. C'est ici que se présente le véritable danger des Fake-news : les citoyens peuvent certes tromper d'autres citoyens mais ils sont aujourd'hui également capables de tromper les journalistes eux-mêmes.

En la matière, les réseaux sociaux n'y sont pas pour rien. La rapidité avec laquelle réagissent les utilisateurs de ces derniers poussent les journalistes à réagir de la même façon et à être plus laxistes quant à la vérification des informations qu'ils véhiculent : dans ces circonstances, on parle même d'« instants articles » (« articles instantanés » en français) tant a diffusion d'informations est rapide. A titre d'exemple, « le Gorafi », journal satirique et ironique français notamment présent sur Facebook, a vu ses articles repris de nombreuses fois par des journaux tels que « Libération » ou « Le Monde ». Cela n'a cependant rien de véritablement surprenant puisqu'une étude menée par l'Université de Stanford a démontré que les Fake-news généraient plus de « likes »[75] que les vraies informations (9 millions contre 7 millions)[76]. Ainsi, au-delà de la simple maladresse, se pose également la question de savoir si le but lucratif ne primerait pas aujourd'hui sur l'éthique journalistique sur les réseaux sociaux ? Ces derniers auraient-ils inversé la tendance ?

A ce titre, il faut relever que les réseaux sociaux sont des intermédiaires redoutables à la Fake-news. Une fois qu'elle est produite, ils se chargent de la disséminer et de la financer[77]. La méthode de financement est notamment proportionnelle à la popularité de la Fake-news partagée et, donc, au nombre de « likes » qu'elle génère. Ainsi, en comparaison à une information vraie, les bénéfices augmentent de presque 30% – si on prend en compte les chiffres proposés par l'Etude de Stanford – et cela aussi bien pour le producteur de la Fake-news que pour le réseau social qui l'a disséminé. De cette manière, il est facile de s'imaginer le danger que représentent les Fake-news pour le droit à l'information et à la liberté d'expression, ainsi que la réticence des réseaux sociaux à lutter contre ces pratiques – ces deux problématiques étant étudiées plus tard dans le développement –.

Au-delà de l'intérêt lucratif, si les réseaux sociaux n'étaient pas vecteurs de désinformation et qu'ils favorisaient un accès aisé à des informations diversifiées de qualité, ils participeraient à rendre les processus démocratiques plus inclusifs[78]. En effet, les réseaux sociaux représentent toutes les classes sociales et en permettant à la population d'être informée, quel que soit son

[75] Action d'aimer une publication partagée sur le réseau social Facebook.
[76] JAYSON, H. (trad : RICHET, I.). Un guide critique des fake-news : de la comédie à la tragédie. *op.cit.*
[77] *Ibid.*
[78] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*

niveau de vie, la disparité « culturelle » s'effacerait. Néanmoins, ils se présentent aujourd'hui comme une véritable menace pour ce processus démocratique puisque les Fakes-news sont difficilement identifiables – ou ne le sont que par une population relativement avertie –, et soutiennent surtout des idées et activités radicales et extrémiste. De cette façon, elles alimentent la haine, la division et la défiance à l'égard de la démocratie[79], ressentis déjà existants au sein des communautés « délaissées », à savoir les minorités.

S'il est avéré que cette menace vient surtout d'acteurs extérieurs à l'UE, étatiques ou non– Andrus Ansip, Vice-Président de la Commission Européenne, a d'ailleurs affirmé que la Russie est la première source de diffusion massive de Fake-news, chose qu'elle a vivement nié[80] – il faut noter qu'elle peut également venir « de l'intérieur » et se présenter comme une véritable stratégie de la part des candidats aux élections.

Ainsi, les Fake-news s'apparentent à une marque d'appartenance à un groupe ou à une idéologie. Comme vu plus tôt, elles créent systématiquement la division et l'hostilité entre les communautés politiques. De cette manière, si l'impact créé par ces dernières est tel qu'il rend impossible le vote pour le candidat premièrement choisi (que ce soit en raison d'une perte de confiance ou simplement parce qu'il n'a pas accédé au second tour, ou encore parce que seul un vote « utile » pourrait être exprimé afin d'éviter le pire), l'électeur s'abstient. En conséquence, le candidat « manipulateur » a plus de chance d'être investi et tel aurait été le cas pour Donald Trump ou encore pour Jair Bolsonaro, Président de la République fédérative du Brésil.

Cependant, le phénomène de Fake-news, fortement accentué par les instants articles des réseaux sociaux, n'est pas le seul à peser dans la balance des élections et de la manipulation des votants. Le concept de « post-truth » (« post-vérité » en français) caractérise les circonstances dans lesquelles les faits objectifs ont moins d'influence sur l'opinion publique que les appels à l'émotion ou aux opinions personnelles[81]. Finalement un corollaire aux Fake-news, qui orientent leurs discours selon ses destinataires, le post-truth est davantage utilisé par les dirigeants d'Etats puisqu'il se veut plus éthique et donc moins sanctionnable moralement.

[79] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». *op.cit.*
[80] *Ibid.*
[81] TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *op.cit.*

Concept apparu aux Etats-Unis en 2004 – l'influence des Etats-Unis sur les nouvelles pratiques politiques n'étant plus à démontrer –, le « post-truth » désigne une culture politique au sein de laquelle les dirigeants d'Etats orientent les débats vers l'émotion en usant abondamment d'éléments de langage et en ignorant les faits et la nécessité d'y soumettre leur argumentation, ceci à des fins électorales. La Russie est une fois de plus considérée comme la plus grande utilisatrice de cette pratique et contrairement à ce qu'elle laisse paraître, elle ne fait pas que s'approprier des concepts déjà existants, sinon qu'elle s'en inspire pour en créer d'autres encore plus redoutables.

Elle a ainsi fait naître le phénomène de « deep-fake » (« hyper-trucage » en français) qui consiste en la manipulation de vidéos par des algorithmes. Ceux-ci, en synchronisant les sons avec les mouvements faciales, sortent les informations de leur contexte afin d'en créer de nouvelles. « El Mundo » [82] s'inquiète à juste titre que cette pratique devienne la manipulation du futur, car bien qu'elle soit encore très peu utilisée, les techniques actuelles la rendent difficilement identifiable. Finalement, les dirigeants d'Etats sont aussi victimes des nouvelles technologies et de la désinformation car celles-ci peuvent conduire à ce qu'ils soient très rapidement décrédibilisés.

En outre, au-delà des principes démocratiques régissant les campagnes électorales, le droit fondamental à l'information est particulièrement mis à mal par ces nouveaux phénomènes, et ce notamment parce qu'ils ne répondent à aucune règle ni à aucune éthique journalistique.

2.2. Risques existants pour le droit fondamental à l'information et les principes démocratiques

Le développement antérieur nous a permis de démontrer que les Fake-news sont un outil dangereux de propagande, tant par leur maîtrise compliquée que par leurs impacts difficilement mesurables. En effet, l'étude de l'Université de Stanford précédemment citée a également estimé que chaque adulte se rappelait au moins d'une Fake-news durant le temps de la campagne électorale[83]. Pourtant, les conséquences sur cette adulte ne sont jamais les mêmes selon qu'il sache identifier la Fake-news ou non.

[82] HERRAIZ, P. "Deep fake: así será la manipulación del futuro". *El mundo*, 8 de mayo de 2019.
[83] GAYA, V. "Clases contra las "fake-news" ¿Son los universitarios analfabetos mediáticos?". *El mundo*, 10 de abril de 2019.

La première cause de l'amplification de ce phénomène n'est autre que la technique. Les réseaux sociaux disposent de différents mécanismes de prolifération permettant la diffusion des Fake-news auprès d'un large panel d'utilisateurs :

- Basés sur des algorithmes : « les critères utilisés par les algorithmes pour hiérarchiser l'affichage des informations sont influencés par le modèle économique des plateformes, lequel accorde la priorité aux contenus personnalisés et sensationnels, généralement plus susceptibles d'attirer l'attention des utilisateurs et d'être partagés »[84] ;
- Axés sur la publicité : le placement d'annonces sur des sites web à contenus sensationnalistes qui jouent sur les émotions des utilisateurs, y compris les Fake-news, sont facilités. Les réseaux sociaux sont d'excellents supports à contenus viraux et répondent parfaitement au modèle économique cité plus tôt : plus les publications sont partagées et « likées », plus les publicités qui y sont afférentes génèrent du bénéfice ;
- Fondés sur la technologie : les comptes robots (également appelés « bots ») sont des faux comptes qui amplifient artificiellement la propagation des Fake-news ;
- Diffusés par les utilisateurs eux-mêmes : les utilisateurs sont finalement les acteurs les plus néfastes à la lutte contre la désinformation. Ayant pour fâcheuse habitude de partager les contenus sans les vérifier, ils augmentent considérablement la vitesse de circulation des Fake-news sur les réseaux sociaux[85].

Le dernier « mécanisme » - si on peut véritablement considérer qu'il en s'agit d'un – est finalement le plus dangereux. Les utilisateurs sont incontrôlables, *a contrario* des moyens techniques déployés afin de diffuser massivement les Fake-news. Il est également difficile d'envisager de sanctionner un utilisateur pour le seul fait d'avoir partagé une Fake-news, sans en être le producteur.

La seconde cause d'amplification du phénomène de Fake-news est l'absence de règles et d'éthique journalistique sur les réseaux sociaux. En effet, les médias traditionnels (à savoir la radio, la télévision ou encore les journaux) répondent à un Code déontologique. Ainsi, ils sont soumis à certaines règles, notamment l'impartialité, le pluralisme, la diversité culturelle, le

[84] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[85] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*

contenu préjudiciable, la publicité et le contenu sponsorisé[86]. De ces règles découlent de nombreuses responsabilités relatives à leur fonction d'information :

- Ils doivent fournir aux individus un compte rendu des évènements véridique, complet et intelligible dans un contexte qui leur donne un sens ;
- Ils doivent mettre à disposition des individus un forum d'échanges afin de nourrir l'information et de répondre aux diverses interrogations ;
- Ils doivent donner une image représentative des groupes constitutifs de la société ;
- Ils doivent respecter, ainsi que représenter, les buts et valeurs de la société ;
- Ils doivent fournir aux individus un accès total aux informations du jour[87].

Au-delà de ces règles et responsabilités, il faut garder à l'esprit que les médias traditionnels sont libres et indépendants. Loin de constituer leur seule différence avec les réseaux sociaux, également appelés les « nouveaux médias », elle se veut néanmoins importante car, animés par un fort objectif lucratif, les réseaux sociaux répondent à un modèle économique qui ne correspond pas à celui d'une obligation d'information. Comme vu précédemment, la popularité de l'information prime sur la qualité de cette dernière pour ces derniers. Ainsi, la Commission Européenne a constaté que 55% des européens sont concernés par des restrictions et de la censure du débat politique sur les réseaux sociaux[88].

Par conséquent, la question se pose de savoir si les réseaux sociaux sont des acteurs politiques comme le sont les journalistes et médias traditionnels ? Comme énoncé plus tôt, si l'information – ou la désinformation – est créée à des fins économiques, elle aura nécessairement des effets politiques. L'impact qu'ont les publications mises en avant par les réseaux sociaux est indéniable et, de la même manière, elles favorisent systématiquement un dirigeant d'Etat plutôt qu'un autre. Cependant, plus qu'un acteur politique, les réseaux sociaux se présentent davantage comme un outil politique car ils ne génèrent pas de contenu informatif propre, ils ne font finalement que le diffuser à large échelle.

Les hommes politiques se sont amplement saisis de ce nouvel outil car il leur permet d'éviter l'intervention des entreprises journalistiques. L'absence d'éthique et de critères journalistiques minimum de vérification ou de validation des sources sur les réseaux sociaux leur permet

[86] *Ibid.*
[87] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. *op.cit.*
[88] COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». Sound and transparent information for an informed and pluralistic democratic debate : practical steps to ensure the support of the online world. *op.cit.*

d'avoir recours aux discours sensationnels, à savoir la technique de post-truth[89]. Ainsi, les hommes politiques deviendraient presque trop transparents en usant abusivement de ces supports. Donald Trump en est le meilleur exemple puisque, en raison de son usage quasi compulsif des tweets comme moyen de communication, il est sans conteste le premier « tweet-président ». Il faut par ailleurs noter que les mots qu'il emploie dans les tweets qu'il publie personnellement sont généralement chargés émotionnellement, au contraire de son équipe qui est plus factuelle : l'ère du post-truth est bel et bien avérée.

De même, on constate ces dernières années une professionnalisation de la propagande politique digitale. Les candidats aux élections créent des équipes de gestion des réseaux sociaux et des salles virtuelles de presse. Le problème est que l'audience ne peut être qu'imaginative dès lors qu'elle se repose sur un monde virtuel. D'un côté, les réseaux sociaux nourrissent l'idée de participation et d'accès direct de la voix du spectateur à la sphère publique : on assiste ainsi à l'enrichissement démocratique des citoyens. D'un autre, l'homme politique s'expose à des messages insultants ou de boycott, voire à l'exposition à des commentaires abusifs ou offensifs[90].

Tout ceci est sans compter l'existence du phénomène de Fake-news qui prolifère à une vitesse affolante et ce notamment – en plus des raisons déjà suscitées – parce qu'il n'existe pas de sanction ni de responsabilité du producteur de ces dernières, au contraire du journaliste soumis à une éthique[91].

Même s'il existe une forme d'injustice entre un « informateur » et un autre, les journalistes ne doivent pas se désintéresser de ce problème. En effet, 43% des utilisateurs s'informent sur les réseaux sociaux sans en vérifier la source[92] et c'est dans ce périmètre que les journalistes doivent intervenir. Une étude espagnole sur l'impact des Fake-news a démontré que seule 14% de la population sait les identifier. A ce titre, le manque d'éducation relative à ces dernières représente la deuxième cause d'amplification du phénomène.

En réponse à cela, des cours spécifiques sur les Fake-news ont été mis en place dans plusieurs universités[93]. Cependant, ces derniers ne sont qu'à destination des journalistes, qui représentent

[89] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*
[90] *Ibid.*
[91] JAYSON, H. (trad : RICHET, I.). Un guide critique des fake-news : de la comédie à la tragédie. *op.cit.*
[92] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*
[93] GAYA, V. "Clases contra las "fake-news" ¿Son los universitarios analfabetos mediáticos?". *op.cit.*

pourtant la population la plus avertie en termes d'identification de ces dernières. Afin de lutter contre celles-ci, ils conviendraient que d'autres étudiants, voire même des professeurs, puissent y assister. Plus encore, que faisons-nous des citoyens qui ne poursuivent pas des études universitaires ? Une sensibilisation et une éducation à la Fake-news devraient être mises en œuvre avant que ne soit atteint l'âge de 16 ans, âge jusque lequel l'enfant doit obligatoirement être scolarisé. Les impacts de ces dernières ne sont à négliger sur aucun citoyen qui, tôt ou tard, devient lui aussi un votant.

Au-delà des citoyens eux-mêmes, la manipulation de l'information porte surtout préjudice à nos démocraties. Les systèmes actuels ne sont pas parfaits, ou ne le sont plus en raison de leur défaut d'adaptation constitutionnelle aux nouvelles pratiques de propagande électorale. Ainsi, les défauts des modes de scrutin de nos démocraties contemporaines sont largement décuplés par les opérations de manipulation d'opinion.

De nombreux auteurs soulèvent donc que les Fake-news tendent à augmenter le nombre de courants politiques, ce qu'ils appellent la division. Si, de prime abord, cela peut sembler être un bien puisqu'elle tend à intensifier le pluralisme politique et la représentation de toutes les communautés – y compris les minorités –, en pratique elle réduit le pourcentage de voix à atteindre pour que le candidat puisse se présenter au second tour.

C'est dans cette phase qu'entre en jeu la polarisation, à savoir l'augmentation de l'incompatibilité et des conflits entre courants politiques. Comme énoncé plus tôt dans le développement, c'est dans ces circonstances, où l'hostilité prime, qu'augmentent les choix de vote « utile » pour éviter le pire ou simplement d'abstention. De cette manière, les Fake-news augmenterait l'accession au pouvoir de candidats néfastes pour la démocratie. Il faut en effet rappeler que, de manière générale, les Fake-news soutiennent les positions ou activités extrêmes[94].

Néanmoins, le danger que représente la désinformation reste à tempérer. Selon l'étude menée par le Politoscope – projet français ayant pour objectif d'analyser les utilisations faites de Twitter par les politiciens – seuls 0,1% des messages Twitter contiendraient une Fake-news. De plus, ils ne visent généralement que des communautés bien précises qui sont, sans surprises, les partis politiques dits « extrémistes ». Ainsi, la communauté de Marine le Pen, présidente du Rassemblement National (anciennement connu sous le nom du « Front National ») et candidate

[94] CHAVALARIAS, D. Au-delà des « fake news » : à l'ère numérique, nos démocraties doivent évoluer pour ne pas mourir. *HAL*, 2018.

aux dernières élections présidentielles françaises de 2017, représente à elle-seule 22,21% des tweets contenant des Fake-news[95].

Il faut cependant noter que l'étude menée par le Politoscope ne concerne que le réseau social Twitter – notamment parce qu'il se présente comme le meilleur outil digital de propagande politique grâce à sa méthode de fonctionnement : les tweets, les retweets[96], etc –, et qu'elle ne nous propose pas une analyse des autres réseaux sociaux tels que Facebook, Instagram ou Youtube dont les méthodes de fonctionnement sont très différentes. Les communautés d'utilisateurs qui y sont présentes ne sont pas non plus les mêmes – Instagram touchant davantage la population des 16-30 ans – et le contenu de la communication politique effectuée n'est donc, *a fortiori*, pas le même non plus.

En fin de compte, l'adaptation est le maître mot des dirigeants d'Etats voulant mener une campagne de communication digitale. Les enjeux de ces dernières évoluent en fonction de l'évolution des moyens technologiques qui, eux, ne font que s'accroître au fil des années. L'arrivée du deep-fake n'a donc, en ce sens, rien de surprenant et son perfectionnement dans les années à venir ne le sera pas davantage. C'est pourquoi il paraît indispensable de rapidement réguler ces très nombreuses pratiques de manipulation de l'information. De même, si à l'heure actuelle l'impact du marketing digital en politique reste relativement modeste, il est néanmoins limité aux partisans les plus engagés[97]. Les partisans les plus engagés ne seraient-ils pas finalement ceux dont la position est la plus extrême et hostile envers la démocratie ? C'est avant tout aux fins de protéger les principes démocratiques qu'il convient d'agir, mais pour autant, la régulation actuelle en France et en Espagne reste très insuffisante.

2.3. Insuffisance de la régulation actuelle en France et en Espagne

Loin de s'attarder de nouveau sur la régulation constitutionnelle de ces deux pays, dont le manque d'adaptation au contexte actuel n'est plus à démontrer, il faut relever que la régulation en droit privée n'est pas plus développée en la matière. Totalement inexistante en Espagne, la France a néanmoins tenté de légiférer avec sa loi « Fake-news ». Néanmoins, comme il le sera démontré dans la suite de cette réflexion, elle se veut insuffisante, voire décevante car elle ne traite finalement le problème qu'en surface.

[95] TORRES DEL CERRO, A. "La lucha contra las "fake news" es un "talón de Aquiles" de las democracias". *El confidencial*, 20 de septiembre de 2018.
[96] Action de partager un tweet publié par un autre utilisateur.
[97] DOSQUET, F. (dir.). *Marketing politique et communication politique. op.cit.*

Pourtant, les journalistes tirent la sonnette d'alarme et estime qu'en 2022 – soit dans seulement 3 ans – le public consommera plus de fake-news que d'informations avérées[98]. Ainsi, comment expliquer que les gouvernements peinent à agir ? Nous n'irons pas jusqu'à affirmer que le profit qu'ils tirent de la manipulation d'opinion est telle qu'ils ralentissent les processus de régulation – d'autant qu'il a été démontré plus tôt qu'ils étaient aussi victimes du phénomène de Fake-news – mais nous pouvons néanmoins considérer qu'ils ne dominent plus les impacts des techniques de communication développées sur des principes fondamentaux existants et irrévocables, ce qui fait naître certaines craintes.

La crainte majeure en la matière est due au risque d'interférer avec le droit à la liberté d'expression. L'article 10 de la Convention Européenne des Droits de l'Homme (ci-après dénommée la CEDH) définit la liberté d'expression en disposant que « 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 »[99]. Par ailleurs, le Conseil Constitutionnel a reconnu en 1994 que la liberté d'expression est une « liberté fondamentale d'autant plus précieuse que son existence est une des garanties essentielles du respect des autres droits et libertés ».

Lorsque l'article 10 de la CEDH énonce que le droit à la liberté d'expression s'exerce « sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière », il condamne notamment la censure et s'assure que le débat public soit inclusif et pluraliste. A ce titre, la liberté qu'offre les réseaux sociaux de divulguer l'information de manière instantanée de la part de n'importe quel citoyen est l'une des meilleures expressions de la démocratie[100], en ce qu'elle n'exclue aucune minorité du débat public. Néanmoins, il faut rappeler que nombreux sont les utilisateurs des réseaux sociaux qui ont été victimes de censure des débats politiques, en raison d'algorithmes de recommandations filtrant les contenus auxquels ils ont accès. Ainsi, il est difficile d'affirmer que les réseaux sociaux prônent fermement la démocratie telle qu'on la connait dans nos sociétés.

En effet, la désinformation qu'ils véhiculent pour répondre à leur modèle économique nuit gravement à la liberté d'expression qui comprend :

---

[98] GAYA, V. "Clases contra las "fake-news" ¿Son los universitarios analfabetos mediáticos?". *op.cit.*
[99] COMMISSION EUROPEENNE. *Report of the Independent High Level Group on Fake-news and online disinformation* : « a multi-dimensional approach to disinformation ». 2018.
[100] PIEDRA CARDOSO, J. Democracia y redes sociales. *op.cit.*

- Le respect de la liberté et du pluralisme des médias : si le but uniquement lucratif des réseaux sociaux venait à s'étendre, les médias traditionnels ne seraient plus libres et indépendants comme ils le sont actuellement, et les réseaux sociaux deviendraient l'unique média ce qui nuirait directement au respect du pluralisme.
- Le droit des citoyens d'émettre des opinions et de recevoir ou de communiquer des informations et idées : si les médias traditionnels venaient à s'éteindre au profit des algorithmes de recommandations, les opinions des citoyens seraient vraisemblablement faussées, d'autant que ces derniers incluraient également des Fake-news.

Ainsi, une solution technique a été proposée : utiliser l'intelligence artificielle (ci-après dénommée l'IA) afin d'éradiquer les Fake-news des réseaux sociaux. Cependant, un problème se pose : que se passerait-il pour les erreurs de citation, la critique, la satire, la parodie, les discours dissidents ou choquants, l'information et les commentaires partisans[101] ? Si l'IA n'est pas en mesure de différencier ces derniers des Fake-news et qu'elle venait à supprimer tous ces contenus, cela constituerait manifestement un abus et donc, une atteinte à la liberté d'expression.

Par conséquent, afin d'éviter une telle atteinte, la Commission Européenne recommande la lutte contre les Fake-news seulement s'il est établi que la diffusion de telles informations procède de la mauvaise foi et d'une intention délibérée de nuire[102]. Cependant, une telle recommandation se veut inapplicable en la pratique et ce, notamment, en raison de son flou conceptuel : comment démontrer l'intention de manipuler par rapport à un comportement normal et comment attribuer l'action de désinformation à un individu ou à un groupe ? C'est en analysant la régulation de droit privé déjà mise en œuvre par la France et l'Espagne, ainsi qu'en formulant des propositions de modifications juridiques et sociétales, qu'un éclaircissement à toutes les interrogations soulevées dans ce premier titre pourra être donné.

[101] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[102] GIREL, M. « De quoi parle le projet de loi sur les Fake News ? » *AOC media*, 04 juin 2018.

TITRE 2. Propositions de régulation aux fins d'éviter un débordement du phénomène de Fake-news

Si, de prime abord, il semble en effet possible de limiter le phénomène de Fake-news par une régulation législative plus adaptée et (quelques) changements sociétaux (**Chapitre 1**), la tâche n'en est pour autant pas si aisée. En effet, la notion de Fake-news étant toujours difficilement définissable, un véritable travail d'analyse et d'anticipation est nécessaire afin de l'apprivoiser. De plus, ce phénomène est en constante évolution et, depuis sa création relativement récente, des pratiques tendant encore davantage à manipuler l'opinion des électeurs sont apparues : l'astroturfing et la Fake-news ciblées (**Chapitre 2**).

Chapitre 1. La possible limitation du phénomène de Fake-news par une régulation législative et des évolutions sociétales

Malgré une volonté européenne de contrer le phénomène de Fake-news encourageant des tentatives de régulation en France et en Espagne (**1.1**), les efforts de ces Etats-membres se veulent encore extrêmement insuffisants, pour ne pas dire décevants. Cela peut sembler ironique lorsqu'on s'aperçoit que ce sont les mêmes reproches qui sont faits aux réseaux sociaux. Néanmoins, avec l'arrivée du Code de bonnes pratiques proposé par la Commission Européenne, certaines réseaux sociaux tentent de s'impliquer dans ce combat qui est le lot de tous. Malgré tout, afin de garantir le plein succès de toutes ces mesures prises, aussi bien par les autorités étatiques que par les plateformes de réseaux sociaux, des évolutions sociétales sont peut-être à envisager afin de s'adapter au contexte d'hyper-connectivité actuel (**1.2**).

1.1. Impulsion européenne et tentatives de régulation française et espagnole

Face aux nombreuses interrogations que soulèvent l'insuffisance de la régulation constitutionnelle et l'ampleur du phénomène de Fake-news, l'UE a pris l'initiative de créer le projet « EUvsDisinfo » qui s'inscrit dans la campagne « Task Force East Stratcom », menée depuis 2015, visant à lutter contre la désinformation provenant des activistes pro-Kremlin[103]. Cependant, il est aujourd'hui avéré que la diffusion de masse des Fake-news ne provient pas uniquement de Russie, mais de n'importe quel pays : les Etats-Unis, les pays d'Amérique du Sud et même les pays d'Europe… Ainsi, la Commission Européenne a elle aussi décidé de réagir face à ce phénomène, pour palier l'inactivité des Etats-membres de l'UE – dont la France

[103] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». *op.cit.*

et l'Espagne – en la matière et pour limiter la propagation des Fake-news et, à défaut, leurs impacts.

A ce titre, elle a pris de nombreuses recommandations, la première listant les bonnes pratiques à adopter afin de lutter contre la désinformation :

- La transparence des sources d'information ;
- Une éducation des individus visant à leur apprendre à lire, mais surtout à déchiffrer et interpréter les médias et les informations ;
- La valorisation des utilisateurs et des journalistes, par exemple en leur permettant de débattre et en leur attribuant un « score » de fiabilité ;
- La diversité et la durabilité de l'écosystème européen des médias d'information, notamment en garantissant un panel important et varié de sources d'information ;
- La mise en avant de la recherche et l'implication des chercheurs dans l'identification des sources d'information peu fiables[104].

La dernière bonne pratique visée par la Commission Européenne s'inscrit dans son objectif de renforcer la vérification des faits, les connaissances collectives et la capacité de contrôle en matière de désinformation. Pour ce faire, en plus des chercheurs universitaires, elle mobilise des « vérificateurs de faits » indépendants qui, au même titre que les journalistes, doivent obéir à des règles d'éthique et de transparence strictes reprises dans un Code de principes du réseau international de vérification de faits. Dans le cadre de leurs fonctions, les vérificateurs de faits se voient confier quatre missions principales par la Commission Européenne :

- La surveillance continue du phénomène de Fake-news ;
- Le repérage et la cartographie des phénomènes d'amplification ;
- La contribution à l'élaboration d'indicateurs de fiabilité des informations ;
- Le partage des connaissances.

Ces dernières visent à promouvoir la responsabilité en ligne et tirer parti des nouvelles technologies[105]. En effet, une fois que les vérificateurs – ou les chercheurs universitaires – ont identifié la Fake-news, une riposte coordonnée et une sensibilisation des citoyens (c'est à cela

[104] COMMISSION EUROPEENNE. *Final report of the High Level Expert Group on Fake News and Online Disinformation*. 12 mars 2018
[105] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions*. *op.cit.*

que se réfère la Commission Européenne lorsqu'elle évoque « le partage des connaissances ») afin de leur donner les moyens d'agir peuvent être menées.

Cependant, sans l'aide des plateformes de réseaux sociaux, la Commission Européenne et les vérificateurs de faits ne peuvent assurer le bon déroulement de ces missions. C'est pourquoi la Commission Européenne a adopté, fin 2018, un Code de bonnes pratiques contre la désinformation. Celui-ci a déjà été signé par les réseaux sociaux les plus influents sur internet, à savoir Facebook, Twitter et Google. Néanmoins, sa portée reste faible puisqu'il ne s'impose qu'aux signataires, et non à tous les réseaux sociaux. Il se présente comme un gage de fiabilité et de confiance pour les utilisateurs mais qu'advient-il des autres réseaux sociaux ? Instagram et LinkedIN, pour ne citer qu'eux, ne font l'objet d'aucun contrôle de la part de la Commission Européenne et, surtout, d'aucune sanction en cas d'irrespect du Code de bonnes pratiques contre la désinformation.

Cependant, les réseaux sociaux signataires font l'objet d'une surveillance étroite de la mise en œuvre de ce Code par la Commission Européenne. A ce titre, ils devaient, jusqu'aux élections européennes de mai 2019, lui rendre un rapport mensuel sur les progrès effectués en matière de lutte contre le phénomène de Fake-news. Celui-ci vise l'adoption de mesures concernant les points suivants :

- L'amélioration du contrôle des placements de publicité ;
- La garantie de la transparence des contenus sponsorisés, politiques et engagés ;
- L'augmentation des efforts visant à fermer les faux-comptes ;
- La mise en place d'indicateurs de fiabilité des sources ;
- La dilution de la visibilité des Fake-news ;
- La mise en place d'un système de marquage des comptes-robots ;
- La mise en place d'outils de personnalisation en ligne, d'interaction et d'alerte à la désinformation ;
- La mise en place de garanties contre la désinformation ;
- L'amplification de la collaboration avec les vérificateurs de faits et les chercheurs universitaires[106].

[106] *Ibid.*

L'objectif de ces rapports n'est autre que d'établir une évaluation globale au bout de 12 mois[107], ce qui permettrait notamment à la Commission Européenne de prendre diverses mesures – possiblement règlementaires – ainsi que de proposer des lignes directrices relatives à la lutte contre la désinformation. Malgré tout, dans sa volonté de soutenir un journalisme de qualité, qui se présente comme le rouage essentiel d'une société démocratique, et afin d'éliminer les menaces de désinformation internes et externes, la Commission Européenne a procédé à l'augmentation de ses ressources en la matière et a également mis en œuvre différente mesures de communications stratégiques[108].

Elle a en effet créé un système d'alerte rapide, opérationnel depuis mars 2019, permettant la détection quasi-immédiate de la diffusion de masse de Fake-news. De même, elle a élaboré un plan d'action relatif à la promotion de l'enseignement et de l'éducation aux médias des citoyens. En parallèle, les Etats membres ont créé un réseau national de coopération électorale réunissant les autorités concernées, telles que les autorités chargées des élections, de la cybersécurité, de la protection des données et les services répressifs. Ils ont par ailleurs désigné un point de contact pour participer à un réseau de coopération électorale au niveau européen[109].

Au-delà des mesures mises en œuvre conjointement, les Etats-membres ont aussi, parfois, pris des initiatives de manière individuelle. C'est notamment le cas de la France avec l'adoption de sa loi Fake-news. Présentée comme un complément à la loi sur la liberté de la presse de juillet 1881, elle a pour objectif de réprimer la circulation de fausses informations, surtout si elles sont de nature à troubler l'ordre public lors d'une consultation électorale[110].

Ainsi, son champ d'application est relativement restreint puisqu'il pose comme conditions une conséquence et un cadre temporel : il ne se consacre qu'aux Fake-news ayant pour conséquence de porter un préjudice à l'ordre public ainsi qu'à celles s'inscrivant dans un contexte électoral. De cette manière, il apparaît que la question de vérité et de qualité de l'information n'est traitée qu'en surface par la loi et que cette dernière s'intéresse davantage à la question de la manipulation. Cela explique donc que trois critères cumulatifs président l'application de la loi Fake-news : le contenu de l'information doit être manifestement faux, viral et artificiellement

[107] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». *op.cit.*
[108] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions*. *op.cit.*
[109] COMMISSION EUROPEENNE. *Déclaration relative au code de bonnes pratiques contre la désinformation* : « la Commission invite les plateformes en ligne à fournir davantage de précisions sur les progrès réalisés ». 28 février 2019.
[110] GIREL, M. « De quoi parle le projet de loi sur les Fake News ? ». *op.cit.*

amplifié. Cela réduit encore d'autant plus le champ d'application de cette loi puisque le fait que la Fake-news soit artificiellement amplifiée sous-entend que la production de celle-ci soit de nature intentionnelle.

A ce titre, la définition de Fake-news proposée par la loi n'apporte pas plus de perspective puisqu'elle considère qu'il s'agit de « toute allégation ou imputation d'un fait dépourvue d'éléments vérifiables de nature à la rendre vraisemblable ». Il faut noter que cette définition a été prise postérieurement par amendement de Naïma Moutchou, députée du Val d'Oise, soit parce que la première définition proposée était incomplète ou inadaptée, soit parce qu'aucune définition de la Fake-news n'avait été proposée. Quelles que soient les circonstances, la proposition actuelle se veut elle aussi insatisfaisante.

Le premier point qu'il faut soulever est la notion de « toute allégation ou imputation (…) dépourvue d'éléments vérifiables ». En plus de réduire considérablement son champ d'application, la loi exclut une grande partie des Fake-news car, comme cela a été vu plus tôt, nombreuses sont celles qui mixent des éléments de fait véritables et vérifiables avec des éléments de fait faux. Ainsi, cette définition se veut trop large, si on considère les énoncés théologiques ou les promesses politiques, ou trop étroite si on considère les opinions fausses, légères ou illusoires non intentionnelles mais avec des éléments vérifiables. Cette définition est donc très contestable dans son interprétation et présente le risque d'une insécurité juridique permanente.

Néanmoins, la loi Fake-news a tout de même permis d'apporter quelques modifications au Code électoral, puisqu'il entre dans son champ d'application, et notamment de le rendre un peu plus adapté au contexte actuel. L'article L163-1 mentionne les réseaux sociaux sous le nom de « plateformes en ligne » et considère que celles-ci sont tenues, « au regard de l'intérêt général attaché à l'information éclairée des citoyens en période électorale et à la sincérité du scrutin », de certaines obligations d'information dès lors que leur « activité dépasse un seuil déterminé de nombre de connexions sur le territoires français » (5 millions de visiteurs uniques par mois[111]). Ainsi, elles doivent fournir à l'utilisateur une information loyale, claire et transparente sur l'identité de la personne physique ou moral qui lui verse des rémunérations « en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ». De même l'utilisateur doit être informé sur l'utilisation de ses données personnelles « dans le cadre

[111] DECRET n° 2019-297 *relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général*, 10 avril 2019.

de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général ». Sur ce point, la loi Fake-news se réfèrent notamment aux Fake-news ciblées et orientées en fonction des profils personnels des utilisateurs. Enfin, si les montants perçus par la plateforme de réseaux sociaux dépassent un certain seuil (100€ hors taxes[112]), ceux-ci doivent être rendu public.

Au regard des seuils fixés par le décret d'application de la loi Fake-news, il faut tout de même noter une volonté de la part de la législation française de contrôler toutes les plateformes de réseaux sociaux et tous les partis politiques qui auraient recours à ces dernières.

L'article L163-2 du Code électoral s'intéresse, quant à lui, aux recours abusifs à la désinformation et aux réseaux sociaux de la part de toute personne physique ou moral. De façon assez surprenante, une autre définition a été reprise par la loi Fake-news afin de l'insérer dans cet article. Cette définition, qui se veut plus complète, considère la Fake-news comme « toute allégation ou imputation inexacte ou trompeuse d'un fait, de nature à altérer la sincérité du scrutin à venir, qui est diffusée de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne ». Bien que son champ d'application soit toujours limité au contexte électoral et à la nature intentionnelle, on s'aperçoit que cette définition inclut davantage de types de Fake-news et à ce titre, elle se rapproche de la définition que nous avons choisi dans l'introduction. Néanmoins, le fait qu'il existe deux définitions engendre là encore le risque d'une insécurité juridique, d'autant plus que l'article dont il est question vise à sanctionner les comportements abusifs.

En effet, il permet au juge des référés, à la demande du Ministère Public, de tout candidat, de tout parti ou groupement politique ou de toute personne ayant intérêt à agir, et sans préjudice de la réparation du dommage subi, de prescrire toutes mesures proportionnées et nécessaires pour faire cesser cette diffusion. A la lecture de cet article, nous comprenons donc que celui qui produit la Fake-news n'est en fait pas sanctionné, sinon celui qui la diffuse. Cela a d'ailleurs été confirmé par la décision du Conseil Constitutionnel du 20 décembre 2018[113] qui reconnaît la conformité de l'article L163-2 ainsi que « d'une procédure pouvant avoir pour effet de faire cesser la diffusion de certains contenus d'information » à la Constitution et à la liberté d'expression. Là aussi, le Conseil Constitutionnel ne s'intéresse qu'à celui qui diffuse et non celui qui produit. Serait-ce une façon induite de responsabiliser davantage les réseaux sociaux ?

[112] *Ibid.*
[113] CONSEIL CONSTITUTIONNEL. *Décision n° 2018-773 DC*, 20 décembre 2018.

C'est ce que laisse penser l'article L112 du même Code qui sanctionne la diffusion massive de Fake-news d'un an d'emprisonnement et de 75 000€ d'amende. C'est une peine relativement lourde mais qu'il faut tempérer par plusieurs éléments : au-delà de la prison, l'amende se veut presque « ridicule » pour des géants des réseaux sociaux comme Facebook ; la sanction ne peut être prononcée que si le caractère inexact ou trompeur de l'information est manifeste et il en est de même pour le risque d'altération de la sincérité du scrutin qui doit également être manifeste. En plus du champ d'application relativement restreint de la loi Fake-news et donc, des articles du Code électoral modifié, les conditions sont nombreuses afin qu'une sanction soit prononcée.

En l'état de ces constatations, la loi Fake-news se veut peu efficace afin d'éradiquer le phénomène de Fake-news. Néanmoins, la France a au moins le mérite d'avoir légiféré en la matière, ce qui n'est pas le cas de l'Espagne. A ce jour, la seule mesure que cette dernière a mis en œuvre est la création d'une « Unidad contra la desinformación » (« Unité contre la désinformation » en français). Constituée par le responsable du département de sécurité nationale et le secrétaire d'Etat à la communication en 2005[114], elle a surtout pour objectif d'identifier les Fake-news. A ce jour, elle en a repéré 5000 qui avaient pour objectif de déstabiliser la démocratie et le système institutionnel européen[115]. Néanmoins, cela est loin d'être suffisant et face à des mesures de si faibles ampleurs, il est compréhensible que l'investissement des réseaux sociaux soit plutôt contestable. Au-delà d'une évolution législative, il faudrait peut-être davantage songer à une évolution sociétale.

1.2. Implication des réseaux sociaux et évolution sociétale

Les réseaux sociaux sont la pierre angulaire du phénomène de Fake-news. Ils donnent, certes, la possibilité à chacun d'exercer son droit à la liberté d'expression mais ils facilitent surtout la propagation de la désinformation, quitte à la rendre incontrôlable. Comme cela a été vu plus tôt, les réseaux sociaux répondent à un modèle économique tout à fait différent de celui des médias traditionnels : leur but premier est lucratif et les publications sensationnelles mais non avérées produisant davantage de bénéfices que les publications vraies et factuelles, il paraît logique qu'ils privilégient celles-ci. Ainsi s'explique dans un premier temps la réticence des réseaux sociaux à agir.

Au-delà des Fake-news, les réseaux sociaux font également preuve d'opacité en ce qui concerne le soutien qu'ils portent à certains partis politiques et la publicité qu'ils mènent pour eux. De

[114] ABELLAN, L. "El Gobierno activa una unidad contra la desinformación ante las elecciones". *El país*, 11 de marzo de 2019.
[115] "Fake news: contra las falsedades". *op.cit.*

cette manière, ils amplifient le phénomène de Fake-news puisque l'utilisateur, non informé, ne peut efficacement identifier les actions de désinformation et par conséquent, la perte de confiance envers les partis politiques et la démocratie devient inévitable. C'est pourquoi 80% des européens seraient en faveur d'une publication des sommes qu'ils perçoivent de la part des partis politiques et groupes de campagnes lorsqu'ils mettent en avant leurs publicités. De la même manière, ils sont invités à publier les sommes qu'ils allouent aux partis politiques et groupes de campagnes à titre de soutien financier[116].

C'est pour lutter contre cette opacité et la réticence des réseaux sociaux à combattre les Fake-news que la Commission Européenne a adopté fin 2018 le Code de bonnes pratiques. Facebook, Twitter et Google en sont les premiers signataires mais il a vocation à s'étendre à toutes les plateformes de réseaux sociaux. En effet, la Commission Européenne dispose de peu de moyens de sanction pour les non-signataires bien qu'en tant que diffuseurs, ils sont tenus responsables de ces dernières (comme cela a été vu précédemment, est sanctionnée la diffusion et non la production de la Fake-news, ce qui devrait avoir un effet dissuasif sur les réseaux sociaux). *A contrario,* les réseaux sociaux signataires sont tenus de respecter le Code de bonnes pratiques.

Ce dernier fixe une série d'engagements qui s'articule autour de cinq domaines :

- Le tarissement des ressources publicitaires des comptes et des sites web qui déforment les informations ainsi que la fourniture aux annonceurs d'outils de sécurité adéquats et d'informations sur les sites web propageant de la désinformation ;
- La mise en avant de la véritable publicité à caractère politique et des publicités engagées ;
- L'élaboration d'une politique claire et accessible au public en ce qui concerne l'identité des diffuseurs et des comptes robots ainsi que l'adoption de mesures visant à fermer les faux comptes ;
- La fourniture d'informations et d'outils pour aider les citoyens à prendre des décisions en connaissance de cause ainsi que la facilitation d'accès à une diversité de points de vue sur des sujets d'intérêt général, tout en donnant la priorité aux sources fiables – et non plus aux plus lucratives – ;

[116] COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». Ensuring fair elections, pluralistic political debate and online and offline freedom of expression. 26 et 27 novembre 2018.

- La mise à disposition aux chercheurs d'un accès aux données qui soit respectueux de la vie privée, pour leur permettre de cerner et de mieux comprendre la propagation et l'incidence de la désinformation[117].

Dans son second point, la Commission Européenne met en avant que son objectif n'est pas de lutter contre la propagande politique et d'en revenir à des campagnes purement institutionnelles – ce qui, en l'état, se veut contraire au droit constitutionnel aussi bien français qu'espagnol – sinon seulement et uniquement de lutter contre la désinformation. Ce Code se veut gage de transparence et en l'acceptant, les réseaux sociaux s'engagent à, eux-aussi, combattre le phénomène de Fake-news et à faire preuve de moins d'opacité. Néanmoins, la Commission Européenne n'exige pas d'eux de prendre des mesures immédiates, notamment pour la bonne foi démontrée par ces derniers en signant le Code et surtout parce que cela ne se voudrait pas pertinent. Son objectif premier étant de préserver les élections européennes, elle impose seulement que des mesures soient prises avant celles-ci et qu'ils fournissent un rapport mensuel détaillant ces dernières[118].

Les premiers rapports sur les actions prises durant le mois de janvier 2019 délivrés à la Commission Européenne par Facebook, Twitter et Google se sont voulus décevants. Ceux-ci se sont notamment distingués par un grand manque de détails démontrant que les nouvelles mesures prises par les trois plateformes de réseaux sociaux allaient être déployées à temps et avec assez de ressources. De plus, les résultats des mesures déjà prises ne faisaient pas non plus l'objet d'une analyse plus détaillée. Ainsi, les plateformes ont démontré avoir échoué dans la fourniture de références spécifiques afin de mesurer si ces mesures avaient contribué à réduire la désinformation[119]. Il faut donc relever que ces trois réseaux sociaux, malgré la signature de ce Code de bonnes pratiques, restent frileux à la transparence. Le fait qu'ils ne divulguent pas leurs résultats peut démontrer l'existence de pratiques peu légales dans le passé, guidées notamment par leur modèle économique, l'absence de résultats probants ou une simple crainte de la concurrence. Dans tous les cas, l'engagement qu'ont pris ces derniers semblent l'avoir été à moitié, ou sans véritable considération des enjeux.

Néanmoins, la Commission Européenne, dans un communiqué sur son site internet, a encouragé les mesures de police qu'ont développé ces trois plateformes. En effet, bien que peu démontrées

[117] COMMISSION EUROPEENNE. *Déclaration relative au code de bonnes pratiques contre la désinformation* : « la Commission invite les plateformes en ligne à fournir davantage de précisions sur les progrès réalisés ». *op.cit.*
[118] *Ibid.*
[119] COMMISSION EUROPEENNE. *First monthly intermediate results of the EU Code or Practice against disinformation*. 28 février 2019.

dans leurs rapports, Facebook, Twitter et Google auraient adopté des mesures concernant la surveillance et le contrôle des placements de publicité, la fermeture des faux comptes et les systèmes de marquage pour les robots informatiques automatisés. En ce qui concerne la transparence des publicités politiques, seul Facebook a affirmé avoir élaborer et mis en œuvre des mesures visant à détecter les publications « à risques » et à assurer la transparence des publicités engagées. Google et Twitter ont échoué en la matière et cela pose un véritable problème puisque les débats publics clivants sont propices à la désinformation.

De son côté, Facebook tente de développer sur son réseau social une fonctionnalité permettant à un groupe d'utilisateurs de signaler, avec une bannière ou une étiquette rouge, les informations de véracité douteuse. L'idée est que dès qu'une publication est signalée par plusieurs utilisateurs, elle est envoyée à des superviseurs externes de vérification de données avec qui Facebook aurait obtenu un accord (ABC News par exemple). Si celle-ci ne fait pas l'objet d'une vérification, pour une raison ou pour une autre, elle pourra être vu mais sera marquée publiquement comme étant « questionnée par des vérificateurs externes » [120]. Le fait que Facebook ne souhaite doter tous les utilisateurs de cette possibilité peut s'expliquer sur la confiance qu'il porte à certains et non à d'autres. Cependant, la question qui se pose est de savoir comment seraient choisis ces utilisateurs ? Comment considérer un utilisateur comme étant fiable et un autre non ? Bien qu'une telle initiative responsabilise une partie des utilisateurs en les rendant pro-actifs, elle en délaisse une autre qui, très certainement, subira les choix effectués par la première.

Cette mesure étant difficile à mettre en œuvre face aux possibles réactions négatives de la part du public, Facebook travaille également à différencier les informations qui sont partagées par les utilisateurs après avoir seulement lu le titre et celles partagées après avoir lu le texte complet[121]. Néanmoins, cela est tout aussi complexe à mettre en œuvre d'un point de vue technique.

Dans l'attente de trouver une réponse à ces problématiques, Facebook a adopté des règles visant à sanctionner les publicités au contenu médiocre, perturbateur, trompeur ou faux, ainsi que les tentatives de contourner le système. De la même manière, Twitter a pris l'initiative de refuser certaines annonces si celles-ci relevaient de pratiques de communication inacceptables ou de mauvaise qualité. Plus encore, il a mis au point un processus de certification qui, s'il est

[120] PIEDRA CARDOSO, J. Democracia y redes sociales. *op.cit.*
[121] *Ibid.*

inachevé, rend impossible la publication de l'information. De cette manière, Twitter prohibe la diffusion d'informations trompeuses sur la manière de participer aux élections ainsi que l'intimidation des électeurs. Google, quant à lui, a procédé à la suppression d'un grand nombre de chaines Youtube pour cause de spams, pratiques trompeuses, escroqueries et usurpations d'identités.

Il faut tout de même noter que Facebook reste le réseau social le plus actif dans la lutte contre la désinformation. Il a procédé à l'ouverture d'un centre d'opérations en vue des élections grâce auquel il a pu démanteler un réseau à « comportement coordonné non authentique » originaire de Russie et ciblant l'Ukraine[122]. De même, il a fourni aux chercheurs un nouvel accès à une interface de programme et à son ensemble de données URL[123]. Le public, de son côté, a dorénavant à une bibliographie d'annonces à caractère politique.

Ainsi, cela explique que la Commission Européenne a constaté des progrès en ce qui concerne les opérations de désinformation coordonnées de la part de ces réseaux sociaux – bien que provenant surtout de Facebook –. Néanmoins, elle relève des efforts insuffisants pour ce qui est de l'intégrité des services de publicité et de l'élargissement de la coopération avec les vérificateurs de faits afin de donner aux utilisateurs et aux chercheurs les moyens d'agir. Elle préconise également la collaboration avec les médias traditionnelles afin d'élaborer des indicateurs de transparence et de fiabilité[124].

La Commission Européenne semble faire preuve d'un certain laxisme – ou d'une certaine pédagogie – et le Code de bonnes pratiques se veut ainsi aussi peu contraignant pour les plateformes de réseaux sociaux signataires que pour les non-signataires. A ce titre, la France a décidé d'agir dans le même temps en adoptant sa loi Fake-news qui tend davantage à s'appliquer puisqu'elle se montre plus sévère.

L'article 11 de cette loi, qui vient en complément de l'article L163-1 du Code Electoral, souligne que les « opérateurs de plateforme en ligne » – comme énoncé plus tôt, il fait partie des rares articles du Code Electoral s'intéressant directement aux réseaux sociaux –, sans distinction, sont tenus de mettre en œuvre « des mesures en vue de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité des

[122] COMMISSION EUROPEENNE. *Déclaration relative au code de bonnes pratiques contre la désinformation* : « la Commission invite les plateformes en ligne à fournir davantage de précisions sur les progrès réalisés ». *op.cit.*
[123] Adresse d'un site ou d'une page hypertexte sur Internet.
[124] COMMISSION EUROPEENNE. *Déclaration relative au code de bonnes pratiques contre la désinformation* : « la Commission invite les plateformes en ligne à fournir davantage de précisions sur les progrès réalisés ». *op.cit.*

scrutins ». Malheureusement, une fois encore, cet article ne s'intéresse qu'aux Fake-news diffusées dans un contexte électorale et non à toute période. Parmi les mesures que sont tenus d'adopter les réseaux sociaux, la loi Fake-news exige que doivent figurer des mesures portant sur :

- La transparence de leurs algorithmes, et notamment ceux de recommandation ;
- La promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle, en ce qu'elles sont gages de fiabilité ;
- La lutte contre les comptes robots propageant massivement de fausses informations ;
- L'information des utilisateurs sur l'identité du parti politique leur versant des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;
- L'information des utilisateurs sur la nature, l'origine et les modalités de diffusion des contenus, point sur lesquels les réseaux sociaux se veulent particulièrement opaques ;
- L'éducation aux médias et à l'information.

Les réseaux sociaux seront tenus de rentre publiques ces mesures, ainsi que les moyens qu'ils y consacrent. A ce titre, ils devront adresser chaque année au CSA une déclaration dans laquelle sont précisées les modalités de mise en œuvre de ces dernières.

Au-delà de l'idée de sanction existant dans la loi Fake-news et non dans le Code de bonnes pratiques, c'est uniquement en ce point que ladite loi se veut moins contraignante puisqu'elle n'exige qu'un rapport annuel quand la Commission Européenne en exige un tous les mois. Néanmoins, et de manière générale, la loi Fake-news a repris le Code de bonnes pratiques – ou l'inverse ? – sauf en ce qui concerne la notion d'éducation aux médias pour laquelle elle impose aux réseaux sociaux d'adopter des mesures. Cependant, est-ce vraiment aux réseaux sociaux de procéder à cette éducation ? Cela ne fait-il pas partie des prérogatives de l'Etat ? Celui-ci semble en effet s'exonérer d'une certaine responsabilité en la délégant aux plateformes de réseaux sociaux qui, techniquement, n'ont aucun moyen d'éduquer des millions d'utilisateurs.

En parallèle, il faut malgré tout noter l'idée particulièrement intéressante qu'évoque l'article 11 de la loi Fake-news qui souhaite faire de l'utilisateur des réseaux sociaux un acteur pro-actif de la lutte contre les Fake-news, comme tente de le faire Facebook. En effet, il évoque que les opérateurs de plateforme en ligne ont l'obligation de mettre « en place un dispositif facilement accessible et visible permettant à leurs utilisateurs de signaler [les fausses informations], notamment lorsque celles-ci sont issues de contenus promus pour le compte d'un tiers », ce

dernier point s'intéressant en fait aux ambitions peu honorables de générer du bénéfice au détriment des principes essentiels de la démocratie – l'information des citoyens pour ne citer que lui –.

Cet alinéa de l'article 11 traduit l'idée selon laquelle les réseaux sociaux, bien qu'obligés par la loi de lutter contre le phénomène de Fake-news, ne sont pas les seuls acteurs de sa propagation sinon que ses consommateurs en sont également les plus grands responsables. Ainsi, une telle législation ne pourra être appliquée de manière viable sans une prise de conscience publique et collective, d'où l'intérêt pour l'Etat de s'investir dans l'éducation de la population. Une autre solution, plus radicale, visant à garantir les principes démocratiques attenants aux élections, serait de faire évoluer en fonction du contexte actuel le mode d'élection du dirigeant d'Etat, aussi bien dans la société française que la société espagnole.

Une première idée serait d'exiger des partis politiques qu'ils rendent publiques leurs dépenses de communication afin de savoir quel budget ils y allouent mais surtout, dans quel contenu[125]. Dans la mesure où les réseaux sociaux sont déjà tenus de dévoiler le financement des placements de publicité qu'ils effectuent, une telle obligation semble déjà à moitié rempli même si l'initiative n'appartient pas aux partis politiques. Il est vrai que la loi semble les oublier, voir les délaisser, en déresponsabilisant ces derniers, pourtant acteurs du phénomène de Fake-news au même titre que les réseaux sociaux et leurs utilisateurs. Il faut en effet garder à l'esprit que Marine le Pen elle-même avait diffusé une Fake-news concernant l'actuelle Président, Emmanuel Macron, lors des dernières élections présidentielles françaises de 2017.

En derniers recours, David Chavalarias, directeur de recherche du Centre National de la Recherche Scientifique (ci-après dénommé le CNRS), préconise d'appliquer la méthode majoritaire se basant sur un principe de majorité et un principe de majorité négative. Il s'agit d'un système de vote par valeurs – les électeurs ne sont pas appelés à choisir un candidat ou à classer les candidats mais à les juger chacun indépendamment – qui se distingue par l'utilisation d'appréciations verbales plutôt que numériques, et la détermination du gagnant par la médiane – la majorité des électeurs jugent qu'un candidat mérite au moins cette mention – plutôt que la moyenne[126].

[125] GAYA, V. "Clases contra las "fake-news" ¿Son los universitarios analfabetos mediáticos?". *op.cit.*
[126] CHAVALARIAS, D. Au-delà des « fake news » : à l'ère numérique, nos démocraties doivent évoluer pour ne pas mourir. *op.cit.*

73% des européens étant exposés à la désinformation ou à la mésinformation en ligne durant la période pré-électorale[127], l'inquiétude des auteurs s'entend tout à fait, d'autant que des phénomènes encore plus dangereux, et toujours plus élaborés, font leur apparition. L'astroturfing et la Fake-news ciblées se présentent comme les « petites-sœurs » de la Fake-news mais n'en sont pas moins redoutables pour l'opinion des électeurs et les principes démocratiques.

[127] COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». Ensuring fair elections, pluralistic political debate and online and offline freedom of expression. *op.cit.*

Chapitre 2. L'astroturfing et les Fake-news ciblées : vers une manipulation de l'opinion des électeurs

C'est par le mariage de toutes les avancées technologiques et des contextes permissifs actuels que des pratiques particulièrement néfastes ont pu naître. L'astroturfing qui, littéralement, usurpe de l'identité citoyenne dans l'espace public numérique (**2.1**) en est le premier exemple. Cependant, il n'est pas le seul et dès lors qu'est combinée l'utilisation des données personnelles à ces évolutions technologiques et ces flous juridiques, apparaît la Fake-news ciblée. Cette arme redoutable utilisée contre la démocratie menace sérieusement d'anéantir les principes démocratiques électoraux (**2.2**).

2.1. Astroturfing ou l'usurpation de l'identité citoyenne sur les réseaux sociaux

L'astroturfing qui, de prime abord se présente comme une évolution technique et technologique de la Fake-news, n'est en réalité pas un concept si simple à cerner. En effet, il vise à simuler l'existence d'un ensemble d'internautes adhérant spontanément à une cause pour influencer de vrais citoyens[128]. Les comptes robots, ou « bots » ont permis l'émergence de cette pratique et c'est pour cette raison que la Commission Européenne met un point d'honneur à ceux que les réseaux sociaux les signalent ou les suppriment.

Grâce à des techniques manuelles ou algorithmiques, mais surtout grâce au Big data qui s'alimente de l'Open data, ces bots peuvent envoyer des messages ciblés à des internautes choisis selon certaines caractéristiques[129]. De cette façon, l'astroturfing permet une propagation plus rapide des Fake-news puisqu'elles sont adressées « aux bonnes personnes, au bon moment » pour reprendre le slogan de Cambridge Analytica. Ainsi, plus qu'une évolution, l'astroturfing est un outil de la désinformation.

D'un autre côté, l'astroturfing se présente également comme une véritable stratégie de communication dont la source réelle est occultée et qui prétend, à tort, être d'origine citoyenne et/ou défendre les intérêts des citoyens[130]. En ce sens, une telle pratique se veut réellement dangereuse pour la démocratie puisque le compte robot usurpe finalement de l'identité citoyenne dans l'espace public « numérique » qui, comme cela a été vu plus tôt, ne cesse de

[128] CHAVALARIAS, D. « Fake news : l'arbre qui cache la forêt ». *op.cit.*
[129] *Ibid.*
[130] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. *op.cit.*

s'accroître chaque jour et, *de facto*, il en va de même pour le nombre de potentiels cibles de celle-ci.

Le fait qu'une telle stratégie trompeuse, modifiant sa source et mentant sur son origine réelle, ait pu naître traduit parfaitement le manque de régulation en la matière. La propagande a alors pris sa forme la plus négative, comme le redoutait Edward Luis Bernays qui souhaitait – peut-être à tort – lui rendre son acception neutre, avec tout de même une petite différence : cette dernière ne se nourrit plus uniquement de la communication gouvernementale ou politique sinon qu'elle s'alimente également de la communication publique. A ce titre, les entreprises privées sont les premiers acteurs de l'astroturfing en représentant 62% de ces derniers. Reste cependant à savoir si les réseaux sociaux sont inclus dans ces statistiques. Néanmoins, il n'est pas l'apanage de ce seul type d'acteurs. Les citoyens, malgré leurs faibles moyens politiques, représentent à eux seuls 5% des initiateurs d'astroturfing, ce qui équivaut presque au score du gouvernement qui lui représente 6% de ces acteurs.

Il faut tout de même relever qu'en ce qui concerne les citoyens, nombreux sont ceux qui l'exercent à leur insu. En effet, ils sont les premières cibles de ces pratiques et il est difficile d'imaginer qu'ils soient bourreaux et martyres. L'opinion publique, en ce sens, se présente véritablement comme une zone de danger, d'autant que le gouvernement représente 33% des victimes de l'astroturfing et s'il est lui-même trompé, il paraît difficile de rétablir la vérité ainsi que la confiance auprès de cette opinion publique.

Pour parvenir à ses fins, celui qui met en œuvre l'astroturfing peut avoir recours à différente stratégie. La première repose sur une action ponctuelle qui s'appuie sur une seule intervention. Peu pertinente, puisqu'il est difficile d'envisager qu'un individu soit convaincu de l'existence d'un groupe par cette seule action, on peut supposer qu'elle est finalement très peu utilisée. En revanche, la campagne d'astroturfing qui est une stratégie reposant soit sur une action répétée périodiquement, soit sur un amalgame de plusieurs actions diversifiées visant toutes un seul et même objectif, se veut plus intéressante puisqu'elle permet de laisser naître la confusion chez le citoyen. Néanmoins, l'astroturfing atteint son apogée quand, en tant que façade prétendant avoir l'appui de l'opinion publique ou en tant que groupe ayant effectivement l'appui de celle-ci mais recruté à l'aide d'arguments mensongers ou partiellement véridiques, parvient à convaincre les citoyens de soutenir une stratégie autour d'un enjeu ponctuel – et notamment les élections –[131].

[131] *Ibid.*

A ce titre, l'astroturfing, sur la base de cette communication mensongère et trompeuse relativement à sa source, rend impossible une intersubjectivité authentique qui est pourtant la condition *sine qua non* de l'agir communicationnel et d'une éthique de la discussion, elle-même gardienne d'une saine communication démocratique.

Pour résumer, il existe astroturfing dès lors que les deux caractéristiques suivantes sont remplies :

- La source de la communication est sciemment tue et s'exécute totalement à l'insu de sa cible ;
- Toujours à l'insu de sa cible, le producteur de l'astroturfing s'approprie illégitimement et stratégiquement l'identité citoyenne pour améliorer la crédibilité de la source présumée et des informations diffusées auprès du public visé[132].

En conclusion, l'astroturfing tire parti de toutes les technologies récemment rencontrées (Big data, Open data, algorithmes) ainsi que du contexte législatif actuel quasi-inexistant et de la propagation croissante des Fake-news. De cette manière, il regroupe toutes les innovations possibles et se présente comme une arme redoutable pour les principes démocratiques actuels. Une autre pratique, moins effrayante de prime abord mais pourtant tout aussi dangereuse, est celle de la Fake-news ciblées qui met gravement en péril le libre-arbitre de l'électeur.

2.2. Vers l'anéantissement des principes démocratiques électoraux

La Fake-news ciblée diffère de l'astroturfing en ce qu'elle n'usurpe pas de l'identité citoyenne et ne tait pas sa source de communication. Elle tire seulement parti des avancées technologiques et profite des progrès de ciblage algorithmique pour s'adresser à un panel plus restreint d'individus, plutôt que de viser l'ensemble de la population avant de passer rapidement dans l'oubli. Des exemples concrets nous permettent de démontrer la grande efficacité de cette pratique. Pour ne citer qu'eux, les partisans des « gilets jaunes »[133] étaient persuadés être plus nombreux que les chiffres annoncés par les médias traditionnels car, dans leur fil d'actualités Facebook, ne s'affichaient que les publications et commentaires soutenant le mouvement, et jamais ceux s'opposant à ce dernier. Ainsi, certaines Fake-news relatives aux « gilets jaunes »

[132] *Ibid.*
[133] Mouvement de protestation politique non structuré apparu en France en octobre 2018.

ont été visionnés plus de 105 millions de fois et ont fait l'objet de centaine de milliers de partages[134].

Par conséquent, que ça soit l'astroturfing ou la Fake-news ciblée, force est de constater que ces pratiques nuisent toutes deux gravement au libre-arbitre et au libre-choix de l'électeur. De la même manière, c'est un premier pas vers une intrusion dans la vie privée puisque c'est en s'alimentant du Big data, et donc des données personnelles des utilisateurs, qu'un tel phénomène est rendu possible. Il semblerait que les révélations d'Edward Snowden, en 2013, annonçant l'utilisation des données personnelles détenues par les géants du web par les services de renseignement américains n'aient pas freiné ceux-ci à les partager.

En effet, le ciblage s'effectue en fonction du contenu consulté ou recherché, de la localisation de l'internaute et/ou du moment de navigation. A ce titre, des profils peuvent être établis en fonction :

- Du comportement des internautes ;
- Des informations communiquées par les personnes concernées ;
- D'une action prise par un internaute.

On constate donc deux pratiques. L'une étant la collecte de données « active » qui n'est autre que la récupération d'informations fournies par les internautes eux-mêmes, l'autre, par opposition, étant la collecte « passive » qui s'exerce sur les données de l'individu à son insu, sans qu'il puisse donner son consentement. C'est ainsi que l'utilisateur des réseaux sociaux se retrouvent piégés dans une situation d'enfermement algorithmique, aussi appelée la « gouvernementalité algorithmique »[135].

Pourtant, en ce qui concerne la collecte « passive » de données en y accédant sur les équipements terminaux des internautes, la directive européenne dite « EPrivacy »[136] de 2002 prévoit que ces données sont soumises, sauf exception, au consentement de la personne concernée à l'exclusion des bases juridiques prévues par la LIL ou le RGPD. Cependant, cette directive ne prime sur ces deux dernières normes que dans ce cas précis. Ainsi, la question qui se pose est de savoir ce qu'il advient lorsque les données sont collectées « passivement » d'une

[134] « Les Fake-news partagées sur Facebook par les « gilets jaunes » visionnées plus de 105 millions de fois ». *Le Nouvel Obs*, 13 mars 2019.
[135] DUBOIS, L. et GAULLIER, F. Publicité ciblée en ligne, protection des données à caractère personnel et Eprivacy : un ménage à trois délicat. *Victoires éditions*¸ 2016. LEGICOM, n°56.
[136] PARLEMENT EUROPEEN ET CONSEIL. *Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*, 12 juillet 2002.

autre façon. Une fois de plus, le flou juridique présent, et notamment parce que plusieurs normes finalement insuffisantes s'opposent, tend à créer une véritable insécurité juridique aussi bien néfaste pour ceux qui collectent et traitent les données que pour les individus victimes de ces pratiques.

L'autre problématique, encore plus importante, qui se pose est de savoir ce qu'il advient dans le cas de collecte « passive » de données sensibles – cette notion fera l'objet d'un développement plus tard dans cette réflexion – bénéficiant d'une protection accrue. D'autant que ces données peuvent être finalement collectées de manière totalement involontaire. A ce titre, les règles EPrivacy ne distinguent pas les données personnelles qui sont sensibles de celles qui ne le sont pas et elles retiennent uniquement le consentement de l'intéressé comme base légale. Cela est applicable quand c'est bien la directive EPrivacy qui prime. Dans le cas contraire, le principe voudrait que la collecte de telles données soit interdite ce qui, comme nous le verrons, est finalement loin d'être le cas en raison des nombreuses exceptions la permettant.

Néanmoins, le GT29 déconseille vivement un tel ciblage compte tenu du « grave risque de porter atteinte aux données personnelles si ce type d'informations est utilisé à des fins de diffusion de publicité comportementales » et recommande le consentement de l'intéressé[137].

Au fil de la première partie de ce développement, il a été mis en avant que les pratiques actuelles de propagande se voulaient particulièrement dangereuses pour la démocratie. Que ça soit la liberté d'expression, la liberté de communication, le droit à l'information, le libre-arbitre que tant d'autres, les réseaux sociaux n'épargnent aucun droit et font, à ce titre, véritablement partie intégrante de notre quotidien. Néanmoins, le phénomène de Fake-news, d'astroturfing et de Fake-news ciblées ne représentent que la facette visible du danger et d'autres pratiques, notamment basées sur l'utilisation des données personnelles, comme le micro-targeting, sont tout autant redoutables, voire plus.

[137] DUBOIS, L. et GAULLIER, F. Publicité ciblée en ligne, protection des données à caractère personnel et Eprivacy : un ménage à trois délicat. *op.cit.*

PARTIE 2. Propagande électorale individualisée : la mise en danger du droit fondamental à la protection des données personnelles par leur utilisation politique

Au même titre que le phénomène de Fake-news, la propagande électorale individualisée grâce aux données personnelles menace de nuire à nos principes démocratiques les plus anciens et essentiels. Le droit à la protection des données personnelles a été reconnu comme un droit fondamental et cela n'a jamais été sans arrières pensées. En effet, ce dernier se présente comme le garant de tous les autres droits fondamentaux : en le garantissant, les problèmes relatifs à la propagande électorale ciblée trouvent leurs solutions d'eux-mêmes. Ainsi, avant de pouvoir analyser les tentatives de régulation afin de protéger les droits et libertés fondamentaux, notamment le droit à la vie privée, face à l'utilisation des données personnelles à des fins politiques et de relever les lacunes que ces tentatives présentent (**TITRE 2**), il convient de matérialiser les dangers existants pour les principes démocratiques français et espagnols (**TITRE 1**).

TITRE 1. Matérialisation des dangers pour les principes démocratiques français et espagnols d'une propagande électorale individualisée

La mise en œuvre d'une propagande électorale ciblée n'est pas sans conséquence, que ce soit sur la perception qu'ont les électeurs de la démocratie ou que ce soit sur les droits fondamentaux de ces derniers. Pour mener cette propagande ciblée, il faut en effet que les partis politiques collecte et traite les données personnelles de ces électeurs. Ainsi, le premier danger qui existe lorsque la régulation nationale se veut insatisfaisante en la matière, n'est autre que celui qui pèse directement sur le droit fondamental à la protection des données personnelles (**Chapitre 2**). Néanmoins, nombreux sont ceux qui sont mis en péril par cette propagande individualisée : finalement, tous les droits fondamentaux sont concernés (**Chapitre 1**).

Chapitre 1. Les risques actuels d'une propagande individualisée sur les droits fondamentaux des électeurs

La propagande en elle-même n'est pas un danger pour nos démocraties, ni pour les droits fondamentaux des électeurs. C'est lorsqu'à cette dernière sont ajoutées les évolutions technologiques et leurs utilisations mal intentionnées qu'elle devient néfaste pour nos processus électoraux. Au-delà de la seule désinformation, plutôt employée par des acteurs étrangers et des opposants politiques, les hommes politiques préfèrent diffuser une information avérée mais ciblée : une fois de plus, le slogan « adresser le bon message à la bonne personne, au bon moment » de Cambridge Analytica prend tout son sens. Néanmoins, cette pratique présente un premier risque non négligeable de l'anéantissement du libre-arbitre de l'électeur (**1.1**). En effet, le phénomène de bulle filtrante contribue gravement à réduire le champ de ses options. De même, utiliser les données personnelles aux fins de cette propagande est une véritable intrusion dans la vie privée (**1.2**), bien qu'elle présente un enjeu majeur pour les dirigeants d'Etats.

1.1. Anéantissement du libre-arbitre de l'électeur

Comme cela a déjà été vu à plusieurs reprises, les réseaux deviennent un véritable problème pour nos démocraties actuelles dès lors qu'ils faussent la perception du monde des utilisateurs et qu'ils nuisent au droit à l'information. Indirectement, la désinformation nuit également à des concepts plus vastes et moins palpables comme celui du libre-arbitre de l'électeur. Il a aussi été constaté plus tôt que cette désinformation atteignait son paroxysme dans la manipulation de l'opinion dès lors qu'elle s'intéressait aux données personnelles des individus. Quoi de plus efficace qu'une propagande personnalisée, répondant en tout et pour tout aux attentes des votants ? L'efficacité de cet alliage entre la technique et le Big data n'est plus à démontrer, l'astroturfing et la Fake-news ciblée nous ayant tous deux enseigné leurs capacités destructrices. Néanmoins, sans parler de désinformation, une propagande basée sur des éléments factuels avérés mais ciblée est tout aussi dangereuse.

Lorsque des publications politiques sont diffusées sur les réseaux sociaux à un panel restreint d'individus, choisi en fonction d'un profil idéologique établi grâce à leurs données personnelles, on parle du phénomène de bulle filtrante. Pour parler plus « techniquement », des bots capables

d'automatiser la diffusion du contenu répondent à la programmation d'une suite d'algorithmes dits « de recommandations »[138].

De prime abord, l'idée se veut particulièrement intéressante : l'utilisateur ne voit apparaître dans son fil d'actualités que des publications répondant à ses centres d'intérêts. Cependant, une telle approche ne peut s'appliquer qu'au domaine commercial où l'utilisateur ne souhaite pas être « pollué » par des informations qui ne l'intéressent pas et où le commerçant gagne en visibilité auprès de ses acheteurs : chacun y gagne. Le problème est que cette pratique est également utilisée dans le domaine politique, où le votant doit normalement pouvoir émettre une opinion éclairée, à savoir la plus informée possible.

Dans cette hypothèse, la bulle filtrante et ses algorithmes de recommandations donnent à l'utilisateur une conception du monde faussée. L'internaute se retrouve enfermé dans un espace numérique conforme à ses préjugés et qui conforte son biais de confirmation[139]. A ce titre, les réseaux sociaux renforcent gravement l'appauvrissement de la pluralité de l'information – déjà mise à mal par ces derniers et par le phénomène de Fake-news – et de la démocratie[140].

En effet, une information diversifiée permet à chacun de se forger librement se propre opinion[141]. Le phénomène de bulle filtrante, puisqu'il réduit *de facto* l'information et les opinions des électeurs, augmente considérablement le risque de polarisation politique et idéologique[142] ainsi que l'omniprésence et la persuasion des histoires fausses et des conspirations[143]. Force est de constater que le phénomène de Fake-news et l'utilisation des données personnelles à des fins de propagande politique sont toujours étroitement liées : sans l'un n'existe pas l'autre, et inversement. Le danger que représentent les réseaux sociaux pour la démocratie n'est, à ce titre, nullement négligeable. Les auteurs, face à cette propagande manipulatrice et nuisible, considèrent que nous nous trouvons dans un régime de « démocrature ». C'est la situation dans laquelle les citoyens, qui pensent avoir le choix du dirigeant d'Etat, ne l'ont pas vraiment. Effectivement, ils ne sont plus en mesure de formuler un avis éclairé en raison des réseaux sociaux et de leurs pratiques qui orientent ce choix.

---

[138] TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *op.cit.*

[139] LAUSSON, J. « Facebook pourrait menacer la démocratie, selon un ex-patron des renseignements britanniques ». *Numerama*, 8 décembre 2018.

[140] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*

[141] CNIL ET CSA. Guide : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». *op.cit.*

[142] LOBO, S. Como influyen las redes sociales en las elecciones. *Nueva Sociedad*, 2017. n°269.

[143] SUPERVISOR EUROPEO DE PROTECCION DE DATOS. *Dictamen 3/2018 sobre la manipulación en línea y los datos personales*. 18 de marzo de 2018.

A ce titre, Mark Zuckerberg, PDG de Facebook, a été sanctionné d'une amende de 45 000 000 de dollars pour le dommage irréparable qu'il a causé « au débat démocratique et à la discussion civilisée dans le monde entier »[144]. Depuis, son équipe tente tant bien que mal d'atténuer ce phénomène de bulle filtrante[145]. Néanmoins, les résultats sont peu probants et un contrôle de la distribution des emplacements de publicité, comme l'a déjà sollicité la Commission Européenne, de la part de Facebook – et de toutes les plateformes de réseaux sociaux – devrait être fait, les algorithmes de recommandations restant opaques et étrangers à la volonté de l'utilisateur.

Il faut noter que le risque d'emprisonnement dans cette « bulle idéologique » est très fort pour les personnes peu engagées politiquement et à faible intérêt pour l'actualité[146] : les partisans actifs d'un parti politique ne se verront jamais proposer les publications d'un autre parti en raison des algorithmes de recommandations et, si tel n'était pas le cas, ils y seraient insensibles ; et un individu ayant un fort intérêt pour l'actualité a toujours la possibilité de contourner les algorithmes de recommandations, ne serait-ce qu'en s'informant par le biais des médias traditionnels.

Néanmoins, le phénomène de bulle filtrante reste le plus dangereux puisqu'internet a rendu parfaitement incontrôlable et imprévisible la rencontre des individus et des messages. Cela n'est pas sans conséquences :

- Les informations n'ont plus aucune attache, sauf celle des intentions idéologiques et des intérêts de leurs producteurs ;
- Chez les individus « forts » de la société connectée, les effets sont faibles mais *a contrario* pour les individus « faibles » à l'attention captive, les effets sont forts[147].

En résumé, les réseaux sociaux sont des vecteurs de (dés)information avec une grande précision de ciblage[148]. Un autre terme employé que celui de la bulle filtrante est celui de la « chambre d'échos ». Ce dernier s'applique davantage au contexte politique puisque les informations relatives à ce dernier ont tendance à circuler en vase clos au sein des communautés politiques.

[144] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*
[145] LAUSSON, J. « Facebook pourrait menacer la démocratie, selon un ex-patron des renseignements britanniques ». *op.cit.*
[146] CARDON, D. « Pourquoi avons-nous si peur des fake-news ? ». *AOC Media*, 20 juin 2019.
[147] *Ibid.*
[148] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions*. *op.cit.*

De la même manière, la chambre d'échos contribue grandement à augmenter l'importance des Fake-news individualisées, comme cela a été le cas pour les « gilets jaunes ».

Une telle précision dans le ciblage des individus est, comme cela a déjà été énoncé, rendu possible par la collecte de données personnelles et le Big data. La technique de l'« empowerment » (« autonomisation » en français) qui consiste à donner à chaque échelon une relation directe avec le sommet, lui procurant le pouvoir de parler et d'agir au nom du candidat, se veut particulièrement efficace aux fins de consolider cette base de données déjà colossale. En effet, le candidat envoie des informations au militant, motivé par des messages personnels sur les réseaux sociaux – lui aussi faisant l'objet d'une propagande individualisée – et créant chez lui un sentiment d'appartenance. En retour, le militant renvoie des informations au candidat. A chacun, cela leur permet d'adapter leur discours et leurs arguments[149].

Cette pratique est difficilement condamnable puisque les informations données par l'individu au militant, puis transmise au candidat, sous-entendent un consentement. Pourtant, au même titre que la propagande individualisée menée grâce au phénomène de bulle filtrante, cela constitue une intrusion dans la vie privée de l'électeur.

1.2. Anéantissement du droit au respect de la vie privée de l'électeur

L'article 12 de la Déclaration Universelle des Droits de l'Homme (ci-après dénommée la DUDH) pose la vie privée comme droit fondamental. Il dispose en effet que « nul ne fera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation ; toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». Au même titre, l'article 8 de la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales (ci-après dénommée la CSDHLF) consacre ce droit mais y ajoute qu'il « ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit ».

Au vu de ce qui a été développé plus tôt, force est de constater que, de manière assez ironique, l'autorité publique est aujourd'hui l'une des plus grandes menaces pour ce droit à la vie privée. En effet, dans le contexte actuel de propagande virtuel, les messages personnalisés et l'information personnalisée sur la base des intérêts personnels, du style de vie, des habitudes et

[149] BILLE, J. Marketing politique et Big Data. *op.cit.*

des valeurs présentent une grave intrusion dans la vie privée et donc, un sérieux risque pour la confiance et l'intégrité du processus démocratique[150].

En France, les primaires ouvertes[151] constituent une source d'informations sans pareille pour les hommes politiques. Ces derniers profitent de cette consultation pour constituer des fichiers d'électeurs, de participants potentiels ou de sympathisants souhaitant être recontactés par les partis organisateurs. Ils collectent et traitent d'importants volumes de données personnelles susceptibles de faire apparaître les opinions politiques des participants qui, au sens du RGPD, sont considérées comme des données « sensibles » – cette notion fera l'objet d'un développement plus tard dans cette étude –[152].

De cette manière sont réalisés des profils invasifs de milliers de personnes qui, souvent à tort, sont classées comme sympathisantes, adhérentes ou membres d'un parti[153]. Par principe, tous les fichiers doivent être supprimés à la proclamation du vote, sauf celui des sympathisants qui peuvent retirer leur consentement à tout moment[154]. Cependant, s'il est permis aux partis politiques de les considérer comme tels pour la simple prise de contact avec celui-ci, cela revient à dire que ces fichiers ne sont jamais supprimés et qu'ils font l'objet d'une utilisation postérieure. De plus, certains « sympathisants » ignorent très certainement faire partie de cette base de données et ne peuvent, en conséquence, retirer leur consentement. Alors certes, les listes électorales qui constituent le socle de cette base de données est librement communicable et ne fait pas l'objet d'un recueil de consentement ni d'une information, mais les hommes politiques vont beaucoup plus loin en « se servant » sur les plateformes en ligne.

C'est face à tous ces dangers pesant sur la vie privée que doit intervenir le droit à la protection des données personnelles afin de la renforcer. L'union de ces derniers donnent naissance au droit à l'oubli, ou à l'effacement des données personnelles que tout individu peut solliciter d'un organisme. Il se présente comme un moyen de garantir la protection de la vie privée, cependant une question se pose : est-il excessif ou indispensable ? En effet, il s'impose au détriment de la liberté d'expression et du droit à l'information et il convient donc de faire une balance entre ces deux principes fondamentaux avec le droit à la vie privée et la protection des données

[150] EUROPEAN DATA PROTECTION BOARD. *Statement 2/2019 on the use of personal data in the course of political campaigns*. 13 mars 2019.
[151] Consultation ouverte à l'ensemble des électeurs afin de désigner un candidat en vue des élections.
[152] CNIL. « Les fichiers constitués dans le cadre des primaires ouvertes ». 8 novembre 2016.
[153] SUPERVISOR EUROPEO DE PROTECCION DE DATOS. Dictamen 3/2018 sobre la manipulación en línea y los datos personales. *op.cit.*
[154] CNIL. « Les fichiers constitués dans le cadre des primaires ouvertes ». 8 novembre 2016.

personnelles[155], ce que ne parviennent pas à faire les gouvernements. Cela explique peut-être le caractère obsolète ou inexistant des régulations française et espagnole en matière de propagande individualisée…

[155] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *op.cit.*

Chapitre 2. La mise en danger du droit fondamental à la protection des données personnelles par une régulation nationale obsolète ou inexistante

De la même manière que pour le phénomène de Fake-news, les régulations constitutionnelles française et espagnole se veulent particulièrement inadaptées et désuètes (**2.1**) concernant le phénomène de propagande individualisée. Si les mesures en la matière, prises à plus petit niveau, proposées par ces deux pays se voulaient plus restrictives, ce phénomène n'inquièterait pas tant. Malheureusement, elles sont tout aussi insuffisantes que la régulation constitutionnelle en vigueur (**2.2**), ce qui ne peut pas leur être reproché puisque le soutien des gouvernements va finalement très peu en leur faveur. Ainsi, un tel vide juridique et règlementaire n'est pas sans danger (**2.3**) et on peut imaginer que des abus naissent en raison de la libre interprétation que celui-ci rend possible.

2.1. L'inexistence de la régulation constitutionnelle en France et en Espagne

En France, au-delà des règles constitutionnelles déjà évoquées qui intègrent vaguement la notion de réseau social, il n'existe à proprement parler aucun article s'intéressant directement à l'utilisation des données personnelles aux fins de mener une propagande ciblée. Passée sous silence, cette pratique ne se voit réguler que par des lois de droit privé, notamment la LIL et le RGPD. Cela traduit une fois de plus le caractère obsolète du droit constitutionnel français mais aussi les difficultés qui sont rencontrées pour l'adapter.

A contrario, en Espagne, une tentative a été faite. Après l'adoption de la LOPD, l'article 58 bis a été inséré dans la LOREG en décembre 2018. Ce nouvel article, votée par les partis politiques PSOE et PP, prévoyait notamment que « la collecte de données personnelles, relatives aux opinions politiques des personnes, que mettent en œuvre les partis politiques dans le cadre de leurs activités électorales sera comprise dans l'intérêt public uniquement quand sont offertes des garanties adéquates ».

Cet article – qui, rappelons-le, a valeur constitutionnelle en tant que loi organique – permet aux partis politiques d'utiliser les données personnelles, et notamment les données sensibles, afin de faire de la propagande ciblée. Il leur autorise à collecter, à partir de pages web et d'autres sources d'accès public, « les données personnelles relatives aux opinions politiques des personnes dans le cadre de ses activités électorales », et ce sur la seule base de l'intérêt public, à savoir l'intérêt légitime du responsable de traitement. Ainsi, la collecte et le traitement de

données sensibles, pourtant interdits au sens du RGPD, sont légitimés durant la campagne électorale et ne nécessitent plus le consentement des personnes concernées[156].

De cette manière, la réalisation de profils idéologiques – ou de micro-targeting – devient possible, même si cette notion n'est qu'induite et qu'elle n'est pas évoquée en tant que telle dans l'article 58 bis de la LOREG. Le fait qu'elle ne soit pas mentionnée est d'autant plus dangereux puisque cela signifie qu'aucun cadre juridique ne lui est donné et qu'aucune sanction n'est prévue en cas d'utilisation abusive de la part des partis politiques – bien qu'une utilisation afin de réaliser des profils idéologiques, permise par le droit constitutionnel espagnol, puisse déjà paraître abusive dans un certain sens –.

Le seul « cadre » posé par l'article 58 bis pour l'utilisation des données personnelles dans le cadre d'une propagande électorale est finalement très permissif puisqu'il estime que cette dernière ne sera pas considérée comme de la communication commerciale et, en ce sens, ne sera pas soumise à ses règles, à savoir l'obligation de transparence, d'information et de consentement[157].

A ce titre, l'Agencia Española de Protección de Datos (« l'Agence de Protection des Données Personnelles » en français, ci-après dénommée l'AEPD) a considéré que l'article 58 bis devait s'interpréter de façon restrictive car il ne doit pas s'opposer aux droits fondamentaux, tel que le droit à la protection des données personnelles, le droit à la liberté idéologique, le droit à la liberté d'expression et d'information ou le droit à la participation politique[158].

Néanmoins, et bien que cet article prévoie également la possibilité pour les individus d'exercer leur droit d'opposition – cette notion sera développée ultérieurement dans le développement – de façon simple et gratuite, les recommandations de l'autorité de contrôle espagnole n'ont pas été suffisantes et le nouvel article de la LOREG a suscité l'indignation publique. L'avocat Borsa Adsuana a considéré qu'il était particulièrement dangereux dans la mesure où il permet aux partis politiques d'élaborer des Fake-news[159]. Bien que, d'une certaine manière, il n'ait pas tort, ce n'est pas le seul préjudice que l'article 58 bis puisse porter aux individus.

En effet, face au grand danger pour le droit à l'intimité et à la vie privée que cet article représente, un recours d'inconstitutionnalité a été exercé à son encontre devant le Defensor del Pueblo (« Défenseur du Peuple » en français). Ce recours a été admis, et le premier alinéa de

[156] GALDON CLAVELL, G. "Los partidos quieren tus datos". *El país,* 24 de marzo de 2019.
[157] *Ibid.*
[158] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[159] PEREZ-LANZAC, C. "No les pongas el trabajo fácil". *El país,* 24 de marzo de 2019.

l'article 58 bis a été annulé (l'article suscité) aux motifs qu'il portait atteinte au droit à la liberté idéologique comme à la protection des données personnelles, ainsi qu'à la liberté d'expression et de participation politique[160].

Néanmoins, nous ignorons si son annulation est une bonne chose puisque, dès lors, il existe un sérieux vide juridique et l'absence de régulation laisse à penser que de nouveaux abus peuvent être commis par les partis politiques. De la même manière, les mesures proposées par l'Espagne ainsi que la France se veulent insuffisantes, ce qui ne tend pas à proposer une protection efficace des données des citoyens de ces deux pays.

2.2. L'insuffisance des mesures proposées par la France et l'Espagne

Face au caractère inexistant ou obsolète des régulations constitutionnelles française et espagnole, des mesures d'initiative « privée », à plus petite échelle, ont été prises. L'Espagne, de son côté, propose plusieurs options à ses citoyens pour s'opposer à l'envoi de propagande électorale, ciblée ou non :

- L'association des internautes met à disposition un formulaire d'accès et d'opposition aux traitements de données personnelles ;
- Les citoyens espagnols peuvent formuler le souhait de ne pas recevoir de publicité politique par le biais de SMS, de WhatsApp[161] ou des réseaux sociaux de manière générale ;
- Ils peuvent également demander à l'Instituto Nacional de Estadística (« Institut National de Statistique » espagnol, ci-après dénommé l'INE) de ne pas divulguer leurs données personnelles aux partis politiques quand il leur fournit les fiches de recensement électoral ;
- Ils peuvent s'inscrire sur la « lista viernes » [162].

La première option qui est proposée aux individus espagnols par l'association des internautes s'applique de manière générique à tous les traitements effectués sur internet. En effet, il est possible d'accéder et de s'opposer à ces derniers, qu'ils relèvent de la propagande électorale ou non. Ainsi, elle se montre peu efficace en ce qu'elle n'est pas spécifique.

[160] "El Constitucional anula la reforma de la ley que permitía a los partidos recopilar datos de votantes". *El Mundo*, 22 de mayo de 2019.
[161] Application de messagerie instantanée.
[162] PEREZ-LANZAC, C. "No les pongas el trabajo fácil". *El país*, 24 de marzo de 2019.

L'option proposée par l'INE se veut, quant à elle, quelque peu surprenante. La LOREG prévoit que les partis politiques peuvent avoir accès aux données contenues dans le recensement électoral, afin notamment de mener leurs campagnes institutionnelles et électorales et d'adresser, à chaque citoyen espagnol, un programme politique en vue des élections. De cette manière, cette option semble s'opposer directement à la loi organique puisqu'elle tendrait à limiter l'accès à ces données aux partis politiques. Il est possible que la subtilité existante entre les données personnelles du recensement électoral pour lesquelles les individus peuvent s'opposer à leur divulgation, et les données personnelles du recensement électoral auxquelles les partis politiques ont légalement accès ne soit pas lisible en l'état. Cela peut s'expliquer notamment par le fait que, en la pratique, cette option soit peu employée par les individus. Néanmoins, si elle venait à être plus utilisée et à nuire au droit des partis politiques, ainsi qu'au processus électoral et démocratique, une balance devrait être directement faite entre l'intérêt supérieur des citoyens espagnols et l'intérêt public. A l'heure actuelle, il est difficile de s'exprimer sur la viabilité de cette proposition.

L'INE propose également un autre outil, celui-ci permettant de s'opposer à l'envoi postal de propagande électorale[163]. Cet outil se voulait très certainement utile dans le passé mais, aujourd'hui, il se caractérise surtout par son caractère obsolète. La propagande papier, bien que toujours menée, n'est plus celle sur laquelle mise les partis politiques pour convaincre les électeurs. Ceux-ci, comme cela a déjà été vu plus tôt, sont bien plus réactifs à la propagande menée sur les réseaux sociaux, dans la mesure où ils y sont pro-actifs et non plus de simples spectateurs passifs.

La dernière option proposée aux individus espagnols vient compléter cet outil offert par l'INE. S'inscrire sur la « lista viernes », qui est une liste disponible sur internet, permet aux citoyens de s'opposer à la réception de propagande électorale par téléphone ou par courrier électronique[164]. Bien que plus adaptée, cette liste ne s'intéresse pas non plus aux réseaux sociaux et à la propagande qui y est menée. C'est ce que vient faire la seconde proposition, mais de manière assez floue puisqu'aucune indication n'est donnée aux électeurs sur la manière d'exercer ce droit. Quand bien même des indications seraient données, il est difficilement envisageable qu'un électeur espagnol puisse exprimer son souhait, à Facebook par exemple, de

[163] GALDON CLAVELL, G. "Los partidos quieren tus datos". *op.cit.*
[164] *Ibid.*

ne pas faire l'objet d'un traitement ayant pour finalité de lui envoyer de la propagande personnalisée. En pratique, cela semble techniquement impossible à mettre en œuvre.

En résumé, toutes les options qui sont proposées aux individus espagnols semblent insuffisantes ou tout simplement irréalisables, voire irréalistes. C'est pourquoi l'AEPD s'est penchée sur le sujet, avec pour objectif de donner un cadre règlementaire à ces pratiques et palier le vide juridique existant. A ce titre, elle a publié deux circulaires qui énumèrent toutes deux les garanties adéquates et spécifiques que doivent offrir les partis s'ils utilisent des données personnelles, et notamment des données relatives aux opinions politiques[165] qui, rappelons-le, sont considérées par le RGPD comme des données sensibles.

L'AEPD considère que seuls les partis politiques, les fédérations, les coalitions est groupements d'électeurs qui présentent les candidatures correspondantes peuvent être responsables de traitement. Elle ajoute que, à aucun moment, les données collectées par ces derniers aux fins de propagande politique ne peuvent être communiquées ni transférées à des tiers[166]. Bien que le périmètre qu'elle offre soit relativement large, la première question qui se pose est de savoir ce qu'il advient des entreprises privées offrant des services aux partis politiques, notamment des applications permettant le ciblage électoral. Certes, elle interdit le transfert des données personnelles à des tierces personnes, mais elle ne s'intéresse à ces dernières qu'en tant que destinataire et non en tant que sous-traitant.

L'AEPD ne s'exprime jamais sur le sort et le statut des sous-traitants auxquels peuvent faire appel ces responsables de traitement. Pourtant, la question devrait être creusée puisqu'il faut rappeler que grand nombre de ces entreprises sont américaines – la pratique de ciblage électoral étant née aux Etats-Unis – et que cela implique donc un transfert des données personnelles des citoyens européens hors de l'UE. Au sens du RGPD, le transfert de données hors de l'UE est possible, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant différents outils juridiques :

- Les Clauses Contractuelles Types de la Commission Européenne : il s'agit de modèles de contrats de transfert de données personnelles adoptés par la Commission Européenne ;

[165] *Ibid.*
[166] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*

- Les règles d'entreprise contraignantes (ci-après dénommée les « BCR »[167]) : elles constituent un code de conduite, définissant la politique d'une entreprise en matière de transferts de données personnelles[168].

Néanmoins, l'AEPD ne s'y intéressant pas – la sous-traitance en matière de données personnelles étant peut-être toujours un sujet sensible, difficile à maitriser – aucune preuve n'est donnée par les partis politiques (ou autres) du respect de ces règles et de ces codes de conduites.

L'AEPD considère également que le traitement ne sera licite que durant la période électorale, à savoir la période définie par la LOREG, et ne pourra s'appliquer qu'aux activités de propagande électorale et aux actes de campagne électorale. Par ailleurs, le responsable de traitement devra déterminer la finalité ou les finalités poursuivies en relation avec l'activité électorale[169]. A ce titre, elle pose certaines restrictions :

- Les partis devront la consulter 14 semaines avant le début de la campagne électorale sur les données qu'ils souhaitent réunir (3 semaines pour les élections de 2019) : pour ce faire, ils devront lui remettre un document précisant les mesures adoptées afin d'évaluer l'impact de la collecte des données personnelles et de minimiser les risques.
- L'utilisation du Big data et de l'IA devra être strictement délimitée ;
- L'interdiction du micro-targeting et de tout système tendant « à forcer ou dévier la volonté des électeurs » ;
- Les données personnelles devront être détruites une fois la campagne électorale terminée.

En plus de ces restrictions, l'AEPD a posé l'interdiction de collecter des données pour interpréter l'opinion politique. Néanmoins, il est possible de collecter celles qui sont exprimées publiquement[170]. Comme nous le verrons plus tard, cela s'aligne sur les règles proposées par le RGPD en matière de protection des données sensibles. De même, cela vise, en quelques sortes, à protéger les droits à la liberté idéologique et à la liberté d'expression qui sont exercés par les individus lorsqu'ils expriment librement leurs opinions politiques. Les partis politiques peuvent donc collecter ces opinions dès lors qu'elles sont exprimées sur des pages web et des sources d'accès public. Par sources d'accès public, l'AEPD entend celles dont la consultation peut se

[167] "Binding Corporate Rules"
[168] BOTCHORICHVILI, N. Transferts de données personnelles hors de l'Union Européenne : quelles nouveautés avec la RGPD ? *Victoires éditions*, 2016. LEGICOM, n°56.
[169] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[170] GOMEZ, R-G. "Protección de Datos limita el acceso de los partidos a información personal". *El país*, 11 de marzo de 2019.

faire par n'importe quelle personne. Sont donc exclues celles dont l'accès est restreint à un cercle déterminé de personnes. Néanmoins, l'AEPD ne détaille pas les personnes entrant dans ce cercle limité, ce qui laisse une fois de plus place à une insécurité juridique pour les individus.

Dans l'hypothèse où le responsable de traitement souhaite obtenir des données de la part d'un tiers, il doit s'assurer que ces données ont été obtenues de manière licite et que ce tiers détient une légitimation spécifique pour avoir obtenu ces données. De plus, il doit vérifier qu'il a informé expressément les personnes concernées de la finalité de cession à des partis politiques[171]. Là encore, aucun détail n'est donné sur la façon dont doivent être informés les individus, ni dans quelle mesure il est considéré qu'ils sont informés. Par exemple, si un individu s'inscrit sur un site internet permettant le visionnage de débats politiques, cela induit-il qu'il est informé que ses données seront utilisées à des fins de propagande électorale ciblée ?

De la même manière que la législation ou que les mesures proposées, le cadre proposé par l'AEPD se veut insatisfaisant puisqu'il soulève de nombreuses interrogations et de nombreuses incertitudes. De même, la question de savoir pourquoi ses circulaires ne font pas l'objet d'une loi, qui traiterait précisément de la propagande électorale ciblée et qui se voudrait plus contraignante ainsi que plus dissuasive, reste en suspens. Néanmoins, il faut rappeler que cette dernière a une capacité de sanction[172], bien que très peu utilisée en pratique. A son initiative propre ou à la demande des citoyens, elle peut contrôler et, si elle constate un manquement au RGPD et à la LOPD, sa sanction peut s'élever à 20 millions d'euros (ou 4% du chiffre d'affaire annuel mondial pour les entreprises, comme le précise le RGPD) [173].

Du côté de la France, aucune mesure particulière n'a été prise afin de limiter la collecte le traitement de données personnelles, qu'elles soient sensibles ou non, aux fins de mener une propagande ciblée. En revanche, la CNIL, particulièrement active depuis 2012 sur le sujet, a émis plusieurs recommandations.

De la même manière que l'AEPD, elle a posé certaines restrictions en ce qui concerne le responsable de traitement. Ce dernier ne peut être que le parti, le groupement à caractère politique, les élus ou candidats à des fonctions électives ainsi que toute personne ou association développant des opérations de communication à caractère politique[174]. Cette limitation se veut, comme pour l'Espagne, peu restrictive finalement et pire encore, elle se veut encore plus large

[171] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[172] GOMEZ, R-G. "Privacidad: Los partidos suspenden en la protección de datos". *El país*, 12 de marzo de 2019.
[173] GOMEZ, R-G. "Protección de Datos limita el acceso de los partidos a información personal". *op.cit.*
[174] CNIL. *Déclaration NS34* « Communication politique ». 29 mars 2019.

en ce qu'elle permet à « toute personne ou association développant des opérations de communication à caractère politique » d'être responsable de traitement. Ainsi, il peut être imaginé que des entreprises privées, comme celles développant des logiciels de stratégie électorale, soient considérées comme des responsables de traitement. Peu limitative, cette restriction est finalement tout le contraire de ce qu'elle devrait être : elle est excessivement permissive et permet à chacun d'être considéré comme responsable de traitement. Néanmoins, la question du transfert de données hors de l'UE se pose moins dans cette hypothèse puisque, au sens du RGPD, un responsable de traitement traitant les données de citoyens européens est soumis à celui-ci.

En ce qui concerne plus précisément les logiciels de stratégie électorale énoncés plus tôt, la CNIL a considéré que la collecte massive de données issues des réseaux sociaux n'est pas légale en l'absence d'information des personnes concernées qui doivent, tout particulièrement, être informées de l'existence du droit d'opposition – ce droit fera l'objet d'un développement plus tard dans le raisonnement –. De la même manière, il existe un dangereux flou quant aux modalités de mise en œuvre de ce droit d'information : comment les personnes concernées doivent-elles être informées ? Par qui doivent-elles l'être (par le parti politique ou le réseau social en question ?) ? Quand est-il considéré qu'elles sont valablement informées ? A ce sujet, la CNIL précise seulement que les modalités de communication doivent être adaptées. Là encore, des interrogations se posent : comment l'information doit-elle être adaptée ? Quand est-il considéré que cette dernière ne l'est pas ?

Par ailleurs, elle ajoute que l'usage des réseaux sociaux ne doivent pas conduire les responsables de traitement à attribuer des opinions politiques aux internautes. Au même titre que l'AEPD, cela signifie que l'opinion politique ne peut pas être déduite d'un croisement de plusieurs données personnelles[175].

En effet, la CNIL considère que les données personnelles faisant apparaître, directement ou indirectement, l'opinion politique réelle ou supposée d'un individu sont exclues des données pouvant être utilisées par les partis politiques dans le cadre de leur propagande électorale ciblée. Néanmoins, elle permet à ces partis de traiter ces données sensibles si :

- Le traitement est limité aux données sensibles correspondant à l'objet de l'organisme ;
- Le traitement ne concerne que les membres des partis et associations, ainsi que les « contacts réguliers », à savoir ceux qui ont accompli une démarche positive en vue

[175] CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». 2018.

d'établir des rapports réguliers avec le parti politique et touchant directement à son action politique ;

- Les données ne sont pas communiquées à des tiers, sauf dans le cas du consentement exprès de la personne concernée[176].

La première limitation est, en l'espèce, totalement inutile puisque les opinions politiques sont nécessairement l'objet du « parti, groupement à caractère politique, des élus ou candidats à des fonctions électives et de toute personne ou association développant des opérations de communication à caractère politique ». La seconde limitation porte à davantage d'interrogations, et notamment en ce qui concerne les « contacts réguliers ». Bien que la CNIL précise qu'il s'agit de ceux ayant accompli une démarche positive en vue d'établir des rapports réguliers avec le parti politique, la définition se veut imprécise puisqu'elle ne détaille pas à partir de quel moment il est considéré qu'il existe une démarche positive ou non.

En effet, dans ses recommandations de 2016 (n'ayant pas été mises à jour depuis, on peut supposer qu'elles sont toujours applicables au contexte actuel), la CNIL fait la différence entre les contacts réguliers et les contacts occasionnels. Elle considère que les contacts réguliers sont les « amis » (pour Facebook) ou les « followers » (pour Twitter) et que les contacts occasionnels sont ceux qui aiment les publications, les commentent, les partagent ou les retweetent[177].

D'un côté, les contacts réguliers doivent faire l'objet d'une information sur les conditions de traitement de leurs données par le biais des onglets « politique de vie privée ». Cette information doit indiquer, de manière claire, la nature des données collectées, l'objectif du traitement et les modalités d'opposition[178]. Néanmoins, une telle information peut être mise en œuvre par le parti politique sur son site internet, par exemple. En pratique, cela semble techniquement impossible de la mettre en œuvre sur un réseau social : on imagine difficilement un parti politique sollicitant Facebook afin qu'il modifie sa politique de confidentialité en vue d'informer ses contacts réguliers. Là encore, les recommandations faites se veulent peu adaptées au contexte pratique et si elles sont inapplicables, il est facile d'imagine que des abus soient commis et que l'information ne soit pas correctement donnée.

[176] *Ibid.*
[177] CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». *op.cit.*
[178] CNIL. « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ». 8 novembre 2016.

Les partis ou candidats peuvent également traiter les données « supplémentaires » d'un contact régulier qu'ils ont collecté. Cependant, pour ce faire, ils doivent répondre à certaines règles. L'adresse mail d'un contact régulier Facebook, afin de lui proposer d'entretenir des contacts réguliers par voie électronique, ne pourra être utilisée qu'après avoir obtenu son consentement sur ce réseau social. Si ce contact régulier refuse ou ne répond pas, l'adresse mail devra être supprimée. Il en va de même pour le profil Facebook d'un follower à qui serait adressé un message privé via Twitter pour lui proposer d'entretenir des contacts réguliers sur Facebook.

En ce qui concerne les contacts occasionnels, ces derniers peuvent devenir des contacts réguliers et c'est d'ailleurs l'objectif principal des partis politiques. Leurs coordonnées peuvent être utilisées une première fois afin de leur proposer de devenir un contact régulier. Si l'individu accepte, il devient un contact régulier des responsables de traitement. S'il refuse ou qu'il ne répond pas, ces données devront, pour lui aussi, être effacées. Néanmoins, la CNIL rappelle que l'acceptation ou le refus ne peuvent être utilisés pour en déduire une sensibilité ou orientation politique réelle ou supposée. Ce rappel s'inscrit dans la lignée de sa restriction selon laquelle seul l'établissement de contacts réguliers permet aux candidats et aux partis de traiter les opinions politiques des personnes concernées.

Par ailleurs, la collecte de données personnelles « supplémentaires » de contacts occasionnels est strictement interdite par la CNIL. En effet, celle-ci se voudrait déloyale puisqu'aucune information ne serait donnée à ce type de contacts. Le responsable de traitement a l'obligation de rechercher son consentement par le biais du vecteur habituel et s'il refuse ou ne répond pas, la donnée ne peut être collectée. Il faut d'ailleurs noter que la CNIL ne précise rien concernant les modalités d'information des contacts occasionnels et qu'à ce sujet, elle ne s'est intéressée qu'aux contacts réguliers. Néanmoins, la CNIL rappelle qu'il est impossible d'utiliser le carnet d'amis de l'internaute, puisqu'il s'agit de personnes tierces[179].

La dernière restriction de la CNIL, affirmant que « les données ne peuvent être communiquées à des tiers, sauf dans le cas du consentement exprès de la personne concernée », ne s'intéresse qu'aux destinataires des données, comme l'a fait l'AEPD, et non au sous-traitant. De la même manière, le problème de transfert de données hors de l'UE se pose. C'est pourquoi la CNIL invite les partis politiques à garantir une sécurité accrue aux données en raison du caractère

[179] *Ibid.*

souvent sensible de ces dernières[180]. De son côté, elle a mis en place depuis 2012 un observatoire des élections ayant pour missions :

- D'informer les électeurs de leurs droits « Informatique et Libertés » ;
- De réagir rapidement aux méconnaissances de la LIL et de mener des contrôles (elle a d'ailleurs mis à disposition des électeurs un formulaire afin que ceux-ci puissent signaler les potentielles atteintes) ;
- D'accompagner les partis et candidats dans la mise en place de leur communication politique conforme à la LIL (ce qu'elle a fait, par exemple, pour Emmanuel Macron, actuel Président français) [181].

Face à cette initiative, la Cour de Cassation et le Conseil d'Etat se sont tous deux prononcés. Ils ont considéré que le traitement des données présente sur internet et les réseaux sociaux doit être loyal et licite. Que la collecte soit directe ou indirecte – cela signifiant que les données peuvent être collectées auprès d'un tiers, comme s'y est intéressée l'AEPD – les personnes concernées doivent systématiquement faire l'objet d'une information, notamment en ce qui concerne l'exercice de leur droit d'opposition. Contrairement à la CNIL, la Cour de Cassation et le Conseil d'Etat considère qu'une information générale dans une politique de confidentialité est insuffisante[182]. Une telle opposition, entre les hautes juridictions et l'autorité de contrôle françaises, porte un véritable préjudice aux individus – comme cela a déjà été vu – puisqu'à chaque fois qu'il existe un tel conflit d'opinions, il existe également une grande insécurité juridique, ce qui ne peut être permis dans l'état actuel d'une réglementation particulièrement insuffisante.

En effet, les faibles efforts actuels des autorités étatiques pour contrer l'utilisation des données personnelles issues des réseaux sociaux peuvent être contournés par l'utilisation de référentiels et de bases de données constituées à la volée. Avec la professionnalisation croissante des pratiques digitales, ces tendances vont se multiplier à courte échéance[183].

2.3. Les risques représentés par l'absence de régulation

Ce vide juridique découlant de l'insuffisance des régulations française et espagnole, ainsi que des mesures prises, n'est pas sans conséquence. En effet, le fichier des donateurs aux

[180] CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». *op.cit.*
[181] CNIL. « Election 2016/2017 : quelles règles doivent respecter les candidats et partis ? ». *op.cit.*
[182] CNIL. « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ». *op.cit.*
[183] DOSQUET, F. (dir.). *Marketing politique et communication politique*. *op.cit.*

partis politiques devient une base de données de militants actifs et engagés qui peut être utilisée[184] : ils sont considérés comme des contacts réguliers. Le simple don vaut consentement, consentement qui est obligatoire pour faire partie de la liste de communication politique d'un parti[185]. Cela s'oppose directement à l'idée selon laquelle une quelconque affinité à un parti politique ne peut être déduite lorsqu'un contact occasionnel accepte ou refuse de devenir un contact régulier. C'est finalement l'expression la plus parlante des dangers que représente l'insécurité juridique : face à l'imprécision de la réglementation, les partis politiques font leurs propres interprétations ce qui, en l'état, n'est pas condamnable et ne peut d'ailleurs être condamné sur aucun fondement juridique – puisque, rappelons-le encore, ils sont inexistants.

Par ailleurs, l'utilisation des listes électorales à des fins de prospection politique est chose possible, comme cela avait déjà été constaté grâce à l'outil proposé par l'INE de s'opposer à l'utilisation des données personnelles figurant dans le recensement électoral. Cela prend tout son sens puisque l'accès à ce dernier est libre et qu'il n'est pas interdit aux partis politiques d'effectuer des tris sur ces listes afin de « s'adresser à une catégorie particulière de votants ». Ainsi apparaît le phénomène de micro-targeting. Néanmoins, il faut noter que l'enregistrement des sympathisants dans un fichier constitué à partir des listes électorales doit être fait sur un support distinct afin d'éviter la constitution d'un document faisant apparaître, directement ou indirectement, les opinions politiques. Cela est presque ironique puisque les partis politiques, comme cela a été vu plus tôt, ont le droit de collecter ces opinions politiques de façon plutôt libre à la vue de l'efficience contestable des restrictions posées par la CNIL et l'AEPD.

Par ailleurs, l'hypothèse de « relance des abstentionnistes » devient pratique courante. En effet, il apparaît comme plus « efficace de mobiliser les électeurs de son propre camp risquant de s'abstenir que d'essayer de convaincre les indécis ou les électeurs du camp adverse ». A titre d'exemple, un indice de mobilisation potentielle a été élaboré pour François Hollande, ancien Président de la République Française. Cet indice pouvait être appliqué à chaque bureau de vote du pays, en multipliant le taux d'abstention local par son vote pour les candidats de gauche aux élections depuis 1998. Les bureaux jugés prioritaires ont fait l'objet d'une campagne de terrain envers les abstentionnistes, individualisés et démarchés en porte à porte[186]. Ce n'est peut être que le début du micro-targeting, qui sera étudié juste après, mais c'est tout de même très inquiétant… C'est pour cette raison que des propositions de régulation doivent être faites, et

[184] BILLE, J. Marketing politique et Big Data. *op.cit.*
[185] CNIL. « Les fichiers constitués dans le cadre des primaires ouvertes ». *op.cit.*
[186] BILLE, J. Marketing politique et Big Data. *op.cit.*

notamment afin de protéger le droit fondamental à la vie privée des individus qui, comme le droit fondamental à l'information mis en péril par le phénomène de Fake-news, s'accompagne de beaucoup d'autres droits et libertés.

TITRE 2. Tentatives de régulation afin de protéger le droit fondamental à la vie privée

Sans apporter une régulation satisfaisante en matière de protection des données personnelles, il semble peu aisé de lutter contre des phénomènes tendant à nuire directement au droit fondamental à la vie privée : tel est le cas du micro-targeting et du profilage (**Chapitre 2**). Ainsi, il faut s'intéresser de plus près à la régulation apportée par le RGPD et à la protection qu'il offre, aussi bien de façon générale que de façon spécifique, concernant les données relatives à l'opinion politique (**Chapitre 1**). C'est en analysant ses lacunes que des propositions pourront naître, celles-ci découlant nécessairement des interrogations que ces failles suscitent.

Chapitre 1. La régulation apportée par le RGPD et la protection spéciale offerte à la donnée politique

Face aux nombreux risques que représente la propagande individualisée pour les droits à l'intimité et à la vie privée, le droit à la protection des données personnelles se présente de prime abord comme un garant du respect de ces derniers. Lorsqu'il a été adopté, le RGPD s'est présenté comme la norme la plus adaptée pour protéger ces droits fondamentaux et pour permettre l'exercice efficace du droit à la protection des données personnelles. De manière générale, il a pour ambition de protéger les données personnelles des individus lors de la collecte et du traitement de ces dernières (**1.1**). De manière plus spécifique, il s'intéresse aux données sensibles et apporte, à ce titre, une protection spécifique aux données relatives aux opinions politiques (**1.2**). Néanmoins, ces protections se veulent-elles véritablement à la hauteur des engagements qu'a pris le RGPD ?

1.1. La protection apportée par le RGPD lors de la collecte et le traitement de données personnelles

Par suite des révélations d'Edward Snowden en 2013, l'opinion publique s'est indignée, elle qui pensait ses données personnelles protégées et qui préférait ignorer que les géants du web les revendaient à des tierces personnes. De son côté, l'UE s'est alors aperçue que sa directive de 1995[187] relative à la protection des données personnelles n'était pas convaincante et qu'elle faisait l'objet de nombreuses lacunes. Cela était également – et est toujours –le cas

[187] PARLEMENT EUROPEEN ET CONSEIL. *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995

des Etats membres, qui ne parvenaient pas à proposer une régulation satisfaisante, en raison de conflits avec leurs législations internes. Pour remédier à cela, l'UE a adopté le RGPD en 2016. Comme cela a déjà été énoncé, son objectif était d'offrir un cadre protecteur aux données personnelles des individus et d'harmoniser la législation des Etats membres en la matière. Si sa mission d'harmonisation a été accomplie, il n'en va pas de même pour celle de proposer un cadre suffisant de protection des données personnelles, comme cela sera vu ultérieurement.

Néanmoins, il faut reconnaître que le droit à l'information, qui soulevait de nombreuses interrogations plus tôt, a été renforcé par le RGPD. Ce dernier le hisse dès lors comme l'un de ses « piliers » et y ajoute la notion de droit à la compréhension. Ce dernier droit implique que l'information soit adaptée à chacun, afin de s'assurer qu'elle soit comprise par tout individu. Ainsi, elle doit être délivrée sous forme concise, transparente, intelligible et d'accès facile, dans un langage clair et simple. Si cela résulte impossible ou que cela suppose un effort disproportionné, l'information doit être facilitée par une forme électronique sur le site internet du responsable de traitement, sur les réseaux sociaux ou tout service équivalent[188]. Néanmoins, la question de savoir comment mettre en œuvre techniquement ce droit à l'information et à la compréhension sur un réseau social se pose toujours. Comme nous l'avions déjà relevé, la politique de confidentialité d'un réseau social est propre à celui-ci et se veut donc applicable à tous les traitements qu'il met en œuvre. En ce sens, cette politique est générique et ne s'applique pas précisément aux traitements effectués par un parti politique qui, rappelons-le, se veut bien plus néfaste pour les principes démocratiques et fondamentaux que de la publicité commerciale.

En ce qui concerne le contenu de l'information, lui aussi a considérablement été renforcé. En effet, l'information des personnes concernées doit indiquer :

- L'identité du responsable de traitement, à savoir le parti politique en question ;
- L'identité du délégué à la protection des données personnelles qui est, au sens du RGPD, obligatoire lorsque le traitement est effectué par une autorité publique ou un organisme public ;
- La/les finalité(s) du traitement ;
- Les transferts de données possibles, hors de l'UE ou non ;
- Le caractère obligatoire ou non de la fourniture de certaines données et les conséquences de l'absence de cette fourniture ;

[188] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*

- La durée de conservation de ces données et leur sort après la mort de l'individu (droit à l'oubli), tout en sachant que le problème ne devrait pas vraiment se poser puisque les partis politiques ont l'obligation d'effacer les données à l'issu du processus électoral ;
- Les droits des personnes concernées, avec une mention toute particulière pour le droit d'opposition et le retrait du consentement ;
- Les modalités pratiques pour exercer ces droits ;
- L'existence d'une prise de décision automatisée ou de profilage[189].

A titre complémentaire, une information doit être donnée dès lors que les données collectées sont utilisées pour une autre finalité que celle poursuivie initialement. Dans le cas de la propagande ciblée, cela ne devrait pas se produire puisque, rappelons-le, la CNIL et l'AEPD exige que ces données ne soient collectées et traitées qu'aux fins de mener les activités de propagande électorale et de communication politique. Néanmoins, nous pourrions envisager que les partis politiques emploient cette possibilité afin de conserver les données et de les utiliser ultérieurement.

Par ailleurs, si le parti politique ou candidat obtient les données personnelles de l'individu par une collecte indirecte, à savoir d'un tiers, il devra l'informer sur cette source[190] et mentionner si elle est accessible au public ou non. A rappeler que dans l'hypothèse où les données ne sont pas accessibles au public, le parti politique ou candidat ne peut traiter les données relatives aux opinions politiques. Cette information doit se faire dans un délai raisonnable après la collecte indirecte : au plus tard lors de la première communication ou lors du transfert à un destinataire, selon l'évènement qui se produit le premier[191]. Une fois de plus, nous constatons que le sous-traitant est totalement ignoré. Bien que le parti politique doive informer sur les transferts de données effectués hors de l'UE ou non, il n'a aucune obligation de mentionner l'identité de ce dernier et les actions qu'il effectue sur ces données, pourtant souvent délicates.

De plus, l'information n'est pas obligatoire si elle se révèle impossible, si elle suppose des efforts disproportionnés par rapport à l'intérêt de la démarche ou si la personne a déjà été informée[192]. Une telle exception soulève de nombreuses questions. La première est de savoir quand est-il considéré que la délivrance de cette information est impossible ou qu'elle suppose des efforts disproportionnés ? Le grand nombre d'électeurs concernés par un tel traitement

[189] MALLET-POUJOL, N. Protection des données personnelles et droit à l'information. *Victoire éditions,* 2016. LEGICOM, n°56.
[190] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[191] CNIL. « Les droits des électeurs ». 13 mai 2019.
[192] MALLET-POUJOL, N. Protection des données personnelles et droit à l'information. *op.cit.*

semble supposer un effort disproportionné, d'autant qu'il faut mettre en balance cette notion avec celle de l'intérêt de la démarche. Collecter les données des individus afin de mener une propagande ciblée présente-t-il un intérêt assez important pour effectuer cet effort disproportionné ? Il est difficile de se prononcer en l'état, la notion se voulant particulièrement imprécise. Néanmoins, il est facile d'imaginer que sur cette libre-interprétation de la notion, l'information des individus en la matière ne soit pas menée. Pourtant, des données dites sensibles sont traitées, et cela ne mériterait-il pas de mettre en œuvre l'effort disproportionné dont le RGPD fait mention ? De même, comment considérer que l'individu a déjà été informé ?

En résumé, le RGPD, bien qu'ayant renforcé le droit à l'information et le droit à la compréhension, se veut lui aussi insuffisant face aux enjeux que représente la propagande individualisée. Il ne parvient à donner une réponse aux problématiques, ou le fait de manière extrêmement floue.

Cependant, les droits à l'information et à la compréhension ne sont pas les principes que met en avant le RGPD. En effet, celui-ci doit répondre aux principes de licéité, loyauté et transparence, de finalité déterminée, explicite et légitime, de minimisation des données collectées, de données exactes et tenues à jour et de durée de conservation limitée.

Comme cela a déjà été vu, la durée de conservation est limitée à celle du processus électoral : les données ne peuvent jamais être conservées indéfiniment, sauf dans de rares exceptions et notamment celle où les données personnelles sont anonymisées pour être transformées en données statistiques.

Concernant le principe de finalité déterminée, explicite et légitime, la CNIL et l'AEPD précise que le fichier constitué à des fins de communication politique ne peut être utilisé à des fins autres que celles pour lesquelles les données ont été collectées[193]. Néanmoins, le RGPD précise seulement que les données ne peuvent pas être traitées ultérieurement si la finalité est incompatible avec celle premièrement définie. La notion d'incompatibilité soulève de nombreuses interrogations. En ces termes, rien n'empêche le parti politique de traiter ultérieurement les données de l'individu s'il définit une nouvelle finalité voisine à celle de la communication politique. L'article 6.4 du RGPD considère d'ailleurs que « le responsable de traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte (…) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère

[193] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*

personnel ont été collectées et les finalités du traitement ultérieur envisagé ». Dans cette hypothèse, il pourrait donc conserver les données et il est difficile de savoir s'il serait tenu à une obligation d'information envers la personne concernée.

La CNIL et l'AEPD précisent également que seules les données pertinentes et nécessaires au regard de la finalité poursuivie peuvent être collectées et traitées, et ce en vertu du principe de minimisation des données collectées[194]. L'ennui, dans le cadre de la propagande ciblée, est que toutes les données peuvent sembler strictement pertinentes et nécessaires aux yeux des partis politiques et candidats. Sans référentiel précis et concret, il sera difficile pour ces autorités de contrôle de sanctionner un parti politique parce qu'il a collecté plus de données qu'ils ne l'auraient dû. Dans un contexte où la propagande vise de plus en plus à persuader qu'à convaincre, tous les arguments sensationnels méritent d'être utilisés par les dirigeants d'Etats : l'aspect financier, l'inclusion et l'exclusion de minorités, les services de santé, les services de scolarité, etc. Un corollaire à ce principe de minimisation est que ces données ne doivent être accessibles qu'aux personnes habilitées. Néanmoins, comme cela a été vu, le panel d'individus ayant accès à ces données selon la CNIL et l'AEPD est véritablement conséquent, ce qui ne tend pas à sécuriser ces données. Pourtant, le RGPD met aussi en avant le principe de sécurité selon lequel les responsables de traitement doivent veiller à la sécurité et à la confidentialité des données vis-à-vis des tiers, y compris lorsqu'ils recourent à un prestataire externe[195].

Enfin la notion de sous-traitance au sens du RGPD est évoquée en matière de propagande électorale ! Cela laisse donc apparaître que cette notion n'est pas totalement étrangère aux autorités de contrôle française et espagnole. Néanmoins, seul l'aspect sécurité est pris en compte et cela se veut particulièrement insatisfaisant : ne serait-il pas plus judicieux d'adopter des mesures préventives en la matière ? D'autant plus qu'il faut rappeler qu'il est tout à fait possible de renseigner ses données personnelles dans une base de données établie par un prestataire à des fins commerciales ou politiques, lequel a pour mission de collecter ces données et de constituer un fichier à destination du parti politique auteur du message de propagande individualisée. Néanmoins, une telle pratique doit répondre à trois conditions :

- Au moment de la collecte initiale, les citoyens doivent être avertis de la réutilisation à des fins de communication politique ;

[194] *Ibid.*
[195] *Ibid.*

- Seuls peuvent être utilisés les fichiers du sous-traitant, et jamais un fichier de gestion des ressources humaines par exemple ;
- Aucun tri ne laissant apparaitre les origines ethniques n'est effectué[196].

La dernière condition retient particulièrement notre attention : certes les origines ethniques ne peuvent pas faire l'objet d'un traitement mais qu'advient-il de toutes les autres données sensibles ? Un traitement basé sur l'orientation sexuel ne serait-il pas tout aussi dangereux ? Le RGPD se veut donc, de manière générale, décevant par rapport aux engagements qu'il avait pris. Il reste à espérer que la protection qu'il apporte aux données relatives à l'opinion politique soit plus satisfaisante.

1.2. La protection spécifique apportée par le RGPD aux données relatives à l'opinion politique

En termes de protection des données personnelles, le RGPD distingue deux catégories : les données personnelles « classiques » et les données personnelles dites sensibles, évoquées à plusieurs reprises au cours de ce développement sans jamais avoir été réellement étudiées. L'article 9 du RGPD liste ces données sensibles. Il s'agit des données à caractère personne qui révèle :

- L'origine raciale ou ethnique ;
- Les opinions politiques ;
- Les convictions religieuses ou philosophiques ou l'appartenance syndicale ;
- Le traitement des données génétiques ;
- Les données biométriques aux fins d'identifier une personne physique de manière unique ;
- Les données concernant la santé ;
- Les données concernant la vie sexuelle ou l'orientation sexuelle.

Les données personnelles « classiques » présentent, certes, tout leur intérêt mais les données sensibles, et notamment les opinions politiques, représentent un véritable enjeu pour les candidats et partis politiques. Se les procurer leur permet de mener une propagande électorale individualisée d'une très grande efficacité et c'est pour cette raison – pour l'influence qu'elles peuvent avoir dans le processus de choix de l'électeur – ainsi que pour l'intrusion dans l'intimité et la vie privée des individus, qu'elles font l'objet d'une protection accrue de la part du RGPD.

[196] CNIL. « La communication politique par courrier électronique ». 13 mai 2019.

En effet, les mesures de protection évoquées plus tôt sont génériques et s'appliquent à toute catégorie de données, ce qui peut justifier en quelques sorte leur insuffisance.

Il faut noter que pour la France, les données relatives aux opinions politiques, qui ont tout notre intérêt comme données sensibles utilisées à des fins de propagande ciblée, n'entrent pas dans le champ de l'interdiction de traitement dès lors qu'elles sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la LIL par la CNIL. Néanmoins, la notion de bref délai reste à interpréter, le temps d'une campagne électorale pouvant finalement être très court… De la même manière, ne sont pas considérées comme des données révélatrices d'opinions politiques les informations relatives à la participation électorale ou à l'abstention dans différents scrutins, telles que collectées dans le cadre d'une étude statistique conduite par l'INSEE ; ainsi que les informations relatives aux activités publiques, comportement et déplacements, blogs et réseaux sociaux, en lien avec les groupes supporters d'appartenance traitées dans le cadre du fichier STADE[197].

En ce qui concerne les données relatives aux opinions politiques qui restent considérées comme des données sensibles, l'article 9 du RGPD prohibe le traitement de ces dernières. Néanmoins, ce n'est pas sans une certaine souplesse que l'on connaît déjà à ce règlement. Ainsi, il prévoit que dans certaines exceptions, le traitement de ces données est possible. C'est notamment le cas lorsque :

- La personne concernée a consenti expressément au traitement de ces données pour une ou plusieurs finalités spécifiques ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- Le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique (…), à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données ne soient pas communiquées en dehors de cet organisme ;
- Le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

[197] BENEZETH, B., DELLEVOY, V., FAVERO, E., GHANTY, A., TAMBA, J. et VILLEDIEU, A-L. *Protection des données personnelles*. Paris : Francis Lefebvre, 2018. 297 p.

- Le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'UE ou d'un Etat membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;
- (…).

Toutes les exceptions prévues par le RGPD ne sont pas citées, seules ont été retenues celles que la CNIL et l'AEPD acceptent de recevoir dans les cas du recueil et du traitement des données relatives aux opinions politiques afin de mener une propagande électorale ciblée. En ce qui concerne l'exception du consentement exprès, toutes deux précisent que celui-ci doit être impérativement actif, explicite et écrit. De plus, il doit être libre, spécifique et informé. De la même manière, elles précisent que lorsque l'exception est celle des motifs d'intérêt public important, elles doivent préalablement avoir autorisé ce traitement[198]. En effet, les autorités de contrôle française et espagnole admettent cette exception comme étant une base légale justifiant le traitement des opinions politiques à des fins de propagande, dès lors que les partis politiques et candidats proposent des mesures adéquates et spécifiques afin de protéger les intérêts et les droits fondamentaux des personnes concernées. A ce titre, l'AEPD recommande d'avoir recours aux procédés de pseudonymisation, d'agrégation ou d'anonymisation[199]. De plus, elle et la CNIL imposent aux partis politiques et candidats d'effectuer une analyse d'impact sur la protection des données et de les consulter, munis de ce document, au moins 14 semaines avant le début de la période électorale[200]. Néanmoins, le fondement et les limites de l'exception des motifs d'intérêt public restent à déterminer précisément, l'imprécision actuelle laissant place à de nombreux abus.

Au même titre que la CNIL et l'AEPD, la Commission Européenne s'est prononcée sur le sujet. Elle reconnaît que les données sensibles collectées dans un contexte électoral peuvent l'être sur la base de l'intérêt légitime du responsable de traitement, seulement si cet intérêt n'est pas supplanté par les intérêts et les libertés et droits fondamentaux des individus concernés. Néanmoins, cette exception ne tend pas à s'appliquer puisqu'il paraît indéniable que le droit fondamental à la vie privée des individus supplante cet intérêt légitime. Cependant, la

[198] CNIL. *Définition* : « Donnée sensible ».
[199] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[200] *Ibid.*

Commission Européenne admet aussi que les autorités publiques agissant dans le contexte électoral peuvent faire valoir une obligation légale ou l'exercice d'une tâche publique[201].

Face à tant d'exceptions, les données sensibles sont-elles encore réellement protégées ? Une fois de plus, le RGPD ne semble pas accomplir son devoir. Les exceptions qu'ils prévoient sont bien trop nombreuses et les plus laxistes, comme celles de l'intérêt public ou de l'intérêt légitime, portent à bien trop d'interprétation. De prime abord, elles paraissent limitatives mais les Etats membres sont invités à en définir la substance, sous réserve de prévoir des garanties appropriées pour les droits fondamentaux et les intérêts des personnes concernées[202]. L'ennui est que cela n'a pas été fait. De cette manière, les partis politiques peuvent collecter et traiter les données relatives aux opinions politiques comme ils l'entendent, sans même nécessiter le consentement des personnes concernées : à défaut de remplir les conditions d'une exception, ils peuvent en remplir d'autres. La directive de 1995, qui a été abrogée par le RGPD, était finalement peut être plus protectrice puisqu'elle ne prévoyait de contourner l'interdiction de traitement des données sensibles que dans les cas où cela était prévu par la loi et nécessaire dans une société démocratique[203]. Mener une propagande politique individualisée ne semble pas tout particulièrement nécessaire dans une société démocratique, en tout cas, ce ne l'était pas avant que les moyens techniques ne le permettent.

En 2001, Latarya Sweerey, doctorante au MIT, avait pourtant prévenu les gouvernements en démontrant que garantir la confidentialité des données sensibles n'est pas chose aisée. En effet, en croisant les listes électorales avec une base de données médicales pseudonymisée, elle était parvenue à réidentifier 90% des individus. Ainsi, s'il est impossible techniquement de mettre en œuvre une protection satisfaisante des données sensibles, tel devrait être le cas sur le plan juridique.

Afin de palier cette insuffisance très certainement constatée par la CNIL et l'AEPD, celles-ci ont mis un point d'honneur à ce que soit mis en avant le droit d'opposition dont dispose l'électeur. Ce droit, qui existe pour tout individu faisant l'objet d'un traitement de ses données personnelles, est défini par la CNIL comme la possibilité pour toute personne physique de s'opposer à ce que ses données à caractère personnel soient utilisées à des fins de prospection

[201] COMMISSION EUROPEENNE. *Commission guidance* : « The application of Union data protection law in the electoral context ». *op.cit.*
[202] BENEZETH, B., DELLEVOY, V., FAVERO, E., GHANTY, A., TAMBA, J. et VILLEDIEU, A-L. *Protection des données personnelles*. *op.cit.*
[203] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *op.cit.*

commerciale. Bien que la propagande politique ne soit pas soumise aux règles de cette prospection commerciale, les autorités de contrôle française et espagnole ont mis un point d'honneur à ce que soit garanti ce droit auprès des électeurs. Malgré son premier alinéa déclaré inconstitutionnel, l'article 58 bis de la LOREG a d'ailleurs consacré ce droit de façon stricte en exigeant des partis politiques qu'ils en garantissent l'exercice simple et gratuit[204].

L'AEPD a, de son côté, rappelé ces critères de simplicité et de gratuité à plusieurs reprises. La CNIL, quant à elle, a ajouté que le droit d'opposition pouvait s'exercer même si les données provenaient de sources ouvertes comme internet, même si elles n'avaient pas été collectées directement auprès de la personne concernée et même si cette dernière avait elle-même rendu ses données publiques[205].

Le fait que la propagande électorale réponde aux exigences de la prospection commerciale concernant l'exercice du droit d'opposition présente un véritable atout pour les électeurs : ceux-ci n'ont nullement besoin de justifier l'exercice de ce droit. Ainsi, le responsable de traitement doit faciliter l'exercice de ce droit et le traiter dans un délai d'un mois maximum. De plus, il doit faire répercuter l'opposition au traitement sur les autres partis s'il existe une base de données commune à plusieurs candidats[206]. Néanmoins, le délai d'un mois semble particulièrement long en ce qui concerne la propagande politique. La LOREG, par exemple, prévoit dans son article 51 que la campagne électorale dure 15 jours. A ce titre, la durée d'un mois permet aux partis politiques et candidats de traiter les données et de terminer leurs actions de propagande individualisée avant d'avoir à répondre à l'exercice du droit d'opposition. A ce titre, le droit de limitation du traitement, qui permet de geler temporairement l'utilisation des données personnelles durant cette période d'un mois, semble être une bonne option pour la personne concernée. En ce sens, l'AEPD exige des partis politiques et candidats qu'ils facilitent, d'un moyen facile et gratuit, l'exercice du droit d'accès, de rectification, de suppression et de limitation du traitement au même titre que l'exercice du droit d'opposition[207].

Néanmoins, ce droit d'opposition n'est pas une nouveauté puisqu'il avait déjà été accordé par la directive de 1995. Le RGPD ne fait finalement que lui apporter de la souplesse en ce qu'il donne la possibilité au responsable de traitement de démontrer l'existence de motifs légitimes et impérieux de nature à prévaloir sur ce droit. Les dispositions de la LIL modifiées se

[204] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[205] CNIL. *Délibération n°2014-041*, 29 janvier 2014.
[206] CNIL. « La communication politique par courrier électronique ». *op.cit.*
[207] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*

rapprochent d'ailleurs davantage de celles de la directive de 1995 puisqu'elle permet à la personne concernée de s'opposer à ce que ses données personnelles fassent l'objet d'un traitement pour des « motifs légitimes » et ne prévoit pas de capacité de refus en faveur du responsable de traitement. Cependant, d'autres exceptions existent au sens du RGPD : le droit d'opposition n'est pas opérant lorsqu'il a été écarté par une disposition expresse de l'acte autorisant le traitement et il doit également être écarté lorsque ce dernier répond à une obligation légale[208]. Une fois encore, tant d'exceptions tendent à fragiliser les droits offerts par le RGPD.

Face aux nombreuses lacunes du RGPD qui, de manière générale ou spécifique ne parvient pas à protéger les données personnelles et les données sensibles des individus, comment faire face à des pratiques encore plus intrusives que la propagande individualisée ? La naissance du micro-targeting et du profilage en est la meilleure expression : la souplesse des législations a permis leur arrivée et il est aujourd'hui difficile d'y faire face, ces concepts étant en perpétuelle évolution.

[208] BENEZETH, B., DELLEVOY, V., FAVERO, E., GHANTY, A., TAMBA, J. et VILLEDIEU, A-L. *Protection des données personnelles*. *op.cit.*

Chapitre 2. Le profilage et le micro-targeting : vers une intrusion dans la vie privée des électeurs

Comme cela a été vu, la propagande individualisée présente un danger non négligeable d'atteinte aux droits à l'intimité et à la vie privée de l'électeur. Néanmoins, ce n'est pas par le seul traitement des données personnelles et la personnalisation des e-mails par les noms et prénoms des électeurs qu'elle est la plus néfaste. En effet, elle prend sa forme la plus poussée dès lors qu'elle s'adapte aux besoins et envies de ceux-ci. Ainsi, le micro-targeting, pratique particulièrement aboutie de propagande ciblée, est interdit afin de protéger ce droit à la vie privée (**2.1**). Contre toute attente, il n'en va pas de même du profilage, dont la différence avec le premier est contestable, qui lui aussi met en péril le droit fondamental suscité (**2.2**). Pour cette raison, les autorités de contrôle, et notamment la CNIL, font preuve d'une grande vigilance.

2.1. L'interdiction du micro-targeting aux fins de protéger le droit à la vie privée

Lorsque Barack Obama a, lors de sa candidature aux élections de 2008, utilisé pour la première fois les données personnelles aux fins d'adresser à chaque citoyen américain une propagande individualisée, les auteurs et journalistes ont d'abord relevé la pratique extrêmement novatrice. Il avait utilisé, avec beaucoup d'audace et de perspicacité, les évolutions techniques et technologiques qui lui étaient offertes. Néanmoins, l'opinion publique n'avait pas encore eu connaissance des révélations d'Edward Snowden, et elle n'avait pas conscience des dangers que représentaient de telles pratiques pour le droit à la vie privée, ainsi que pour le libre-choix de l'électeur. La pratique du micro-targeting mise au point par Barack Obama, qui est une technique de propagande individualisée particulièrement ciblée, a permis en France d'augmenter la participation de presque 20% et a fait gagner 10 points de vote pour François Fillon dans les zones qu'il avait ciblé lors des élections de 2017[209]. Quoi de plus intrusif que d'avoir accès aux pensées des individus et de pouvoir les manipuler ?

La propagande individualisée, dans son aspect le plus poussé, met en péril de nombreux droits et libertés, qui vont bien au-delà du seul droit à la vie privée. Cela explique d'ailleurs très certainement que la référence au droit à la vie privée soit moins explicite dans le RGPD. A la différence de la directive de 1995, le droit à la vie privée ne fait pas l'objet d'une réception distincte des autres droits et libertés fondamentaux. L'objectif du RGPD n'est plus la protection

[209] THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *op.cit.*

« des droits et libertés fondamentaux des personnes physiques et notamment de la vie privée », mais « la protection des libertés et droits fondamentaux des personnes physiques et en particulier leur droit à la protection des données à caractère personnel » [210]. Cette nouvelle approche plus large des droits et libertés fondamentaux, en mettant à l'honneur le droit à la protection des données personnelles, prend tout son sens dans un contexte où ce dernier droit est finalement le garant de tous les autres droits : la pratique du micro-targeting ne peut exister si les partis politiques et candidats n'ont pas la possibilité de traiter les données personnelles comme ils l'entendent. Néanmoins, la pratique existe, et il faut mettre en cause l'insuffisance des législations nationales ainsi que la souplesse du RGPD.

Pourtant, l'UE tire la sonnette d'alarme – sans pour autant apporter de véritables solutions de son côté – et considère que le micro-targeting change les normes du discours politique, réduisant l'espace pour le débat et l'échange d'idées. On en revient au phénomène de bulle filtrant qui enferme l'électeur dans les conceptions personnelles qu'il se fait du monde et ses préjugés, ce qui tend à rendre les discussions entre les individus impossibles. Pour cette raison, il est nécessaire, et de façon urgente, d'initier un débat démocratique sur l'utilisation et l'exploitation des données pour l'organisation des campagnes électorales et la prise de décisions politiques[211]. Les autorités de contrôle française et espagnole ont déjà tenté de réguler la propagande ciblée, toujours de manière insatisfaisante. Le problème réside peut-être en ce que les mesures prises l'ont toujours été de façon totalement unilatérale et qu'elles n'ont jamais l'objet d'une discussion avec les citoyens français et espagnols.

Le grand problème du micro-targeting est qu'il repose finalement sur une décision automatisée : un message est envoyé à cet individu parce que, selon l'algorithme, il répond aux critères de sa programmation mathématique. C'est ce qu'on appelle le « data-driver decision-making » qui est un modèle de décision fondé sur des données chiffrées[212]. Les algorithmes sont d'indispensables instruments pour personnaliser les affichages publicitaires et recommander[213]. Cependant, le fait que l'humain n'ait pas le regard sur ces décisions algorithmiques inquiète : comment contredire une décision, en principe, totalement objective ? Il faut rappeler tout de même que les algorithmes ne sont pas neutres, mais loyaux et qu'il existe souvent des biais algorithmiques qui sont, justement, des erreurs du fait de la saisie humaine. Néanmoins, certains

[210] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *op.cit.*
[211] SUPERVISOR EUROPEO DE PROTECCION DE DATOS. *Dictamen 3/2018. op.cit.*
[212] BILLE, J. Marketing politique et Big Data. *op.cit.*
[213] CARDON, D. Le pouvoir des algorithmes. *Le Seuil*, 2018. Pouvoirs, n°164.

auteurs sont convaincus que ces calculs mathématiques peuvent protéger la démocratie. Il permettrait de faire face à la modification du paysage des circonscriptions électorales, ce qui est certes impossible pour l'Espagne mais qui pourrait tout à fait l'être pour la France, et éviter de procurer un avantage politique à certains partis. Les mathématiques pourraient protéger la démocratique contre cette fraude, grâce notamment à des algorithmes d'échantillonnage statistique[214].

Cependant, c'est le seul avantage que l'opinion publique trouve actuellement au micro-targeting et à ses décisions algorithmiques. Ainsi, l'UE continue d'interdire strictement cette pratique et elle est suivie par les autorités de contrôle française et espagnole. Dans un premier temps, elle interdit le traitement massif de données – ce qui est pourtant le cas finalement – et l'utilisation de l'IA car cela peut mener à modifier l'idéologie politique d'une personne. *A priori*, ce n'est pas donc pas tant le droit à la vie privée qui la préoccupe, sinon davantage la liberté d'opinion et d'expression de cette opinion : c'est la manipulation de l'électeur qui inquiète et, à ce titre, le Comité Européen de Protection des Données (ci-après dénommé le CEPD) prohibe aux partis la micro-personnalisation de leurs messages[215].

L'AEPD, de son côté, ajoute que l'activité de traitement du parti politique doit être proportionnelle à l'objectif poursuivi, à savoir mener sa campagne électorale et convaincre les électeurs. De son point de vue, le micro-targeting n'est pas un traitement proportionnel, ni tous ceux qui ont pour objectif de forcer ou dévier la volonté des électeurs. Elle considère d'ailleurs qu'il est contraire aux principes de transparence et de libre-participation qui sont les pierres angulaires d'un système démocratique[216]. En résumé, les individus ont le droit de ne pas faire l'objet d'une décision basée seulement sur un processus automatique produisant des effets le concernant : le micro-targeting entre dans cette catégorie dès lors qu'il affecte les circonstances, le comportement ou les choix des individus, ou dès lors qu'il a un impact prolongé ou permanent sur l'individu[217].

Comme énoncé plus tôt, cette décision automatisée n'est possible que grâce aux algorithmes. Il faut rappeler que les décisions algorithmiques sont procédurales et non substantielles, elles

[214] JOSE MARIN, J. y RUIZ GUEVERA, P. "Matemáticas para proteger la democracia". *El país*, 19 de diciembre de 2018.
[215] GALDON CLAVELL, G. "Los partidos quieren tus datos". *op.cit.*
[216] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[217] COMMISSION EUROPEENNE. *Commission guidance* : « The application of Union data protection law in the electoral context ». *op.cit.*

n'ont pas d'accès sémantiques aux informations qu'elles manipulent et elles apprennent des biais qui existent dans les données. A ce titre, ces dernières doivent répondre à plusieurs règles :

- Transparence : leurs calculs doivent être vérifiés par l'humain ;
- Loyauté : les services doivent expliquer à l'utilisateur les priorités qui président aux décisions de leurs algorithmes et que puisse être vérifié, en tout indépendance, que des intérêts cachés, des déformations clandestines ou des favoritismes cachés n'altèrent pas le service rendu.

Ainsi, si l'effet de l'algorithme est anticipé par la plateforme mais n'est pas identifiable par l'utilisateur, il existe déloyauté et donc manipulation. Néanmoins, la vigilance doit s'exercer davantage sur les données plutôt que sur les algorithmes car ce sont dans ces dernières qu'il existe des failles[218].

En conclusion, le micro-targeting est une pratique condamnée aussi bien par l'UE que ses Etats-membres. Cependant, et de manière assez surprenante, elle ne se prononce pas en matière de profilage, pourtant tout aussi dangereux que le micro-targeting. La différence entre les deux est d'ailleurs presque imperceptible et son acceptation est assez troublante.

2.2. La mise en péril du droit à la vie privée par le profilage

Tout ce que la CNIL et l'AEPD s'évertuent à interdire est finalement autorisée par une autre norme. C'est notamment le cas des opinions déduites par le croisement des données personnelles et le profilage qui, nécessairement, en découle. L'article 22 du RGPD les autorise d'ailleurs, non pas sans quelques restrictions.

L'AEPD distingue le micro-targeting de l'élaboration de profils. Elle accepte uniquement l'élaboration de profils généraux et par catégories génériques desquels il est possible de déduire des conduites générales de la population de forme agrégée. En résumé, le profilage se cantonne à une description générale de l'individu[219]. Cependant, l'autorité de contrôle espagnole ne donne aucune indication sur le niveau de généralité que doit respecter ce profilage, ni aucun référentiel permettant de cerner précisément sa définition. Si on le compare au micro-targeting, ce dernier se définit de la manière suivante : il est le croisement de données personnelles afin de déterminer des profils psychologiques individuels précis afin de faire du ciblage d'électeurs. En résumé, le micro-targeting ne se cantonne, quant à lui, à rien : plus il peut être précis, mieux

[218] CARDON, D. Le pouvoir des algorithmes. *Le Seuil*, 2018. Pouvoirs, n°164.
[219] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*

c'est[220]. Ainsi, la différence entre les deux notions se limite à une perception tout à fait subjective de l'imprécision ou de la précision de l'un et l'autre. Il apparaît ainsi particulièrement difficile de les distinguer car, d'un individu à l'autre, d'une autorité de contrôle à l'autre, une pratique sera permise ou condamnée.

Ainsi, les autorités de contrôle française et espagnol se détourne de cette distinction bancale et difficile à effectuer. La CNIL se concentre donc sur le croisement des données personnelles – ce qui ne semble pas être une mauvaise chose en soit puisque, de cette manière, le problème est solutionné à sa source – et fait preuve d'une grande vigilance en la matière. Le problème soulevé par les logiciels de stratégie électorale concerne, certes, le ciblage des électeurs, mais surtout les conséquences pratiques qui peuvent découler de leur présence dans ces bases de données. Ces dernières permettent en effet de croiser de nombreuses catégories d'informations provenant de sources diverses :

- Les informations de profils des réseaux autres que les seules données de contacts ;
- Les données de navigations collectées via des cookies ;
- Les données transmises par des tiers et collectées dans un contexte sans rapport avec la prospection politique.

Ainsi, les nouveaux outils de prospection électorale peuvent permettre de collecter non seulement les données déclaratives des profils (nom, prénom, profession, etc.) mais aussi des données d'usage (quand, avec quelle fréquence la personne interagit avec le candidat, les pages qu'elle visite, etc.). Il parait donc indispensable d'apporter des limites à la combinaison de ces données et notamment à l'exploitation de données relatives aux comportements, aux goûts et aux interactions sociales en ligne des personnes, ainsi qu'aux conséquences de ces opérations sur les personnes concernées.

A ce titre, la CNIL considère que la combinaison de données personnelles des utilisateurs d'un réseau social, en l'absence d'outils de contrôle suffisants à leur disposition et de possibilité de s'opposer au profilage, ne peut jamais se fonder sur le seul intérêt légitime du responsable de traitement puisqu'il n'existe pas un juste équilibre avec ls droits et libertés des personnes concernées : en ce sens, le consentement des internautes est donc indispensable. De cette manière, en l'absence de consentement, seuls des portes à portes ciblés, à l'échelle d'une circonscription, d'un quartier ou d'une rue, peuvent être réalisés sur la base des données traitées par ces logiciels, et non des portes à portes personnalisés, comme cela est le cas avec le micro-

[220] CHAVALARIAS, D. « Fake news : l'arbre qui cache la forêt ». *op.cit.*

targeting[221]. En résumé, la CNIL résume ainsi les conditions de croisement des données personnelles des individus :

- L'individu doit être informé à chaque collecte de données sur son profil de réseau social ;
- Son consentement doit être recueilli quant à l'ensemble des conditions de mise en œuvre du traitement de données ainsi agrégées.

Concernant la seconde condition, il faut noter que le consentement doit s'exprimer par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant. Ce consentement doit également pouvoir être retiré à tout moment. Par exemple, une case à cocher pourrait être proposée. Attention également, le croisement des données personnelles ne peut concerner que les contacts réguliers. En effet, les conditions d'information et de recueil du consentement peuvent difficilement être satisfaites pour les contacts occasionnels.

Ainsi, en France, étant donné que les personnes concernées doivent avoir consenti afin que les bases de données commerciales soient utilisées, l'élaboration de profils obtenus par croisement de fichiers multiples devient finalement un parcours complexe au regard de la vigilance exercée par la CNIL[222]. Reste à l'Espagne et à l'AEPD d'en faire de même…

[221] CNIL. « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ». *op.cit.*
[222] *Ibid.*

CONCLUSIONS

Au-delà de toutes les critiques qui ont été formulées dans cette étude, à l'égard de la régulation en vigueur, aussi bien européenne que nationale, il faut noter que des efforts sont fournis aussi bien par les autorités publiques que par les entreprises privées, et notamment celles mettant à disposition les plateformes de réseaux sociaux. En effet, l'UE a salué les efforts fournis par Facebook, Twitter et Google dans la lutte contre les Fake-news. Un taux de participation record a été enregistré lors des élections au Parlement Européen de 2019.

Grâce aux réseaux sociaux suscités, l'UE a renforcé ses capacités d'identification de la désinformation et de lutte contre celle-ci, notamment par l'intermédiaire du système d'alerte rapide qu'elle a créé et qui s'est révélé particulièrement efficace. Par ailleurs, le Code de bonnes pratiques, bien que non contraignant, a permis d'augmenter la sensibilisation de la société au phénomène de Fake-news et sa résilience face à ce dernier[223].

Néanmoins, les autorités publiques peinent à réagir et cela est un véritable frein aux initiatives d'ordre privé. Face aux évolutions technologiques constatées tout au long de ce développement, un retard considérable a déjà été pris, retard dont profitent des pratiques abusives comme le sont celles de l'astroturfing ou du deep-fake. Bien que la France ait adopté sa Loi Fake-news, le concept est de plus en plus difficile à cerner en raison de la rapidité à laquelle évolue le phénomène de désinformation qui menace dangereusement les droits à la liberté d'expression et à l'information. C'est d'ailleurs très certainement ce qui empêche l'Espagne d'agir en la matière.

Une première solution qui pourrait être proposée, au-delà de définir précisément la Fake-news et ainsi d'adapter le champ d'application de la loi, serait de sanctionner davantage le producteur de la fausse information plutôt que celui qui la diffuse. Une autre serait de rendre le Code de bonnes pratiques déployé par la Commission Européenne plus contraignant, en l'imposant par exemple à toute plateforme de réseau social offrant ces services au sein de l'UE. Celui-ci devrait, par la même occasion, être complété afin de contraindre les géants du web à mettre fin aux algorithmes de recommandations et, de la même manière, au phénomène de bulle filtrante particulièrement propice à la prolifération de la fausse information.

[223] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE fait rapport sur les progrès réalisés dans la lutte contre la désinformation en vue du Conseil européen ». 14 juin 2019.

Directement lié à l'utilisation des données personnelles par les réseaux sociaux, mettre fin au phénomène de bulle filtrante rendrait par ailleurs cette utilisation moins récurrente, et surtout moins dangereuse pour le droit à la vie privée. Son caractère utile a été démontré en matière de publicité commerciale, mais il n'en est rien pour ce qui est de la propagande politique : les algorithmes de recommandations nuisent gravement au pluralisme politique et au pluralisme médiatique.

Ainsi, du côté de la propagande individualisée, de nombreux efforts restent à fournir : la régulation doit se montrer plus stricte et précise, aussi bien du côté de l'UE que des Etats membres. L'article 9 du RGPD se veut extrêmement décevant en ce qui concerne la protection des données sensibles et notamment des opinions politiques, mais également en ce qui concerne la protection plus générale des données personnelles de l'individu et donc de sa vie privée. De cette manière, il est apparu tout au long de cette réflexion que les autorités de contrôle, tout autant que les gouvernements, ne disposent pas des outils nécessaires afin de contrôler et sanctionner les pratiques peu éthiques en matière de propagande électorale ciblée.

La meilleure solution serait sans doute de proposer une loi, ou un autre règlement, directement destinés à réguler cette propagande qui s'articule principalement sur les réseaux sociaux. Au-delà d'un seul cadre théorique, il faudrait également songer aux aspects pratiques et techniques qui sont peu pris en compte à l'heure actuelle et qui, souvent, rendent la législation en vigueur inapplicable. De la même manière, une démarche relative à la distinction entre le micro-targeting et le profilage ne serait pas négligeable.

Néanmoins, une augmentation de la sensibilisation des citoyens européens est tout de même à noter puisque les réactions face à l'entrée en vigueur de l'article 58 bis de la LOREG se sont montrées vives. Ce dernier a d'ailleurs été reconnu partiellement inconstitutionnel en raison des dangers qu'il représentait pour les droits fondamentaux à l'intimité et à la vie privée, ainsi qu'au droit à la protection des données personnelles qui se porte garant de ces deux derniers. Le fait qu'une telle loi ait pu être adoptée au niveau constitutionnel traduit bien l'incertitude des gouvernements et la difficulté pour ces derniers à s'adapter à un contexte en perpétuelle évolution technologique.

En conclusion, la législation continue de faire ce qu'elle a toujours fait, à savoir agir après que l'évolution sociale ne se soit déjà produite…

BIBLIOGRAPHIE

Ouvrages

BENEZETH, B., DELLEVOY, V., FAVERO, E., GHANTY, A., TAMBA, J. et VILLEDIEU, A-L. *Protection des données personnelles*. Paris : Francis Lefebvre, 2018. 297 p.

BERNAYS, E. *Propaganda : comment manipuler l'opinion en démocratie*. New York : Zones, 1928. 144 p.

BRAUD, P. *La science politique*. 11ème édition. Paris : Que sais-je, 2017. 128 p.

CHOMSKY N. et HERMAN, E. *Manufacturing consent : the political economy of the mass media*. New York : Pantheon Books, 1988.

DOSQUET, F. (dir.). *Marketing politique et communication politique*. 2ème édition. Paris : EMS Management et Société, 2017. 302 p.

RIUTORT, P. *Sociologie de la communication politique*. Paris : La Découverte, collection « Repères », 2007, 121 p.

Articles de revues

BERGUIG, M. et COUPEZ, F. Faut-il réellement craindre l'open data pour la protection de nos données personnelles ? *Victoires éditions*, 2016. LEGICOM, n°56.

BILLE, J. Marketing politique et Big Data. *Commentaire SA*, 2015. Commentaire, n°150.

BOTCHORICHVILI, N. Transferts de données personnelles hors de l'Union Européenne : quelles nouveautés avec la RGPD ? *Victoires éditions*, 2016. LEGICOM, n°56.

CARDON, D. Le pouvoir des algorithmes. *Le Seuil*, 2018. Pouvoirs, n°164.

CHAVALARIAS, D. Au-delà des « fake news » : à l'ère numérique, nos démocraties doivent évoluer pour ne pas mourir. *HAL*, 2018.

CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *Victoires éditions*, 2016. LEGICOM, n°56.

DUBOIS, L. et GAULLIER, F. Publicité ciblée en ligne, protection des données à caractère personnel et Eprivacy : un ménage à trois délicat. *Victoires éditions*¸ 2016. LEGICOM, n°56.

DUDEZERT, A. et KAROUI, M. Capital social et enjeux de pouvoir : une perspective socio-politique de l'appropriation d'une technologie de réseaux sociaux au sein d'une collectivité territoriale. *Systèmes d'information et management,* 2012. Volume 17.

ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *Análisis.* Quaderns de Comunicacio i Cultura, n°56.

JAYSON, H. (trad : RICHET, I.). Un guide critique des fake-news : de la comédie à la tragédie. *Le Seuil*, 2018. Pouvoirs, n°164.

KRZATALA-JAWORSKA, E. Internet : complément ou alternative à la démocratie représentative ? *Boeck Supérieur*, 2012. Participations, n°2.

LEHMANS, A. Les réinventions de la démocratie à l'aune de l'ouverture des données : du discours de la participation aux contraintes de la gouvernance. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

LOBO, S. Como influyen las redes sociales en las elecciones. *Nueva Sociedad,* 2017. n°269.

MALLET-POUJOL, N. Protection des données personnelles et droit à l'information. *Victoire éditions*, 2016. LEGICOM, n°56.

MERCANTI-GUERIN, M. Facebook, un nouvel outil de campagne : analyse des réseaux sociaux et marketing politique. *Direction et Gestion*, 2010. La Revue des Sciences de Gestion, n°242.

NICKERSON, D-W. and ROGERS, T. Political campaigns and Big Data. *Journal of Economic Perspectives, 2014*. Volume 28, n°2.

PIEDRA CARDOSO, J. Democracia y redes sociales. *Universidad Verdad*, 2017. 1(72).

THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *Quaderni*, 2018. N°96.

Articles de presse

ABELLAN, L. “El Gobierno activa una unidad contra la desinformación ante las elecciones”. *El país*, 11 de marzo de 2019.

CARDON, D. « Pourquoi avons-nous si peur des fake-news ? ». *AOC Media*, 20 juin 2019.

CHAVALARIAS, D. « Fake news : l’arbre qui cache la forêt ». *AOC media*, 7 novembre 2018.

DARMANIN, J., FERRAN, B. et RONFAUT L. « Minute par minute, le récit de la nuit de 13 novembre sur les réseaux sociaux ». *Le Figaro*, 25 novembre 2015.

DEL CASTILLO, C. y SARABIA, D. “Aprobada la ley que permitirá a los partidos hacer spam electoral y propaganda personalizada en internet”. *El diario*, 21 de noviembre de 2018.

DE MIGUEL, B. “La UE señala a Rusia como la mayor amenaza de interferencia para las elecciones europeas de Mayo”. *El país*, 20 de febrero de 2019.

“El Constitucional anula la reforma de la ley que permitía a los partidos recopilar datos de votantes”. *El Mundo*, 22 de mayo de 2019.

« Elections : à la fête du client ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c’est terminé, N°149.

« Elysée : des données pas données ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c’est terminé, N°149.

“Fake news: contra las falsedades”. *El país*, 12 de marzo de 2019.

GALDON CLAVELL, G. “Los partidos quieren tus datos”. *El país*, 24 de marzo de 2019.

GAYA, V. “Clases contra las “fake-news” ¿Son los universitarios analfabetos mediáticos?”. *El mundo*, 10 de abril de 2019.

GIREL, M. « De quoi parle le projet de loi sur les Fake News ? » *AOC media*, 04 juin 2018.

GOMEZ, R-G. “Privacidad: Los partidos suspenden en la protección de datos”. *El país*, 12 de marzo de 2019.

GOMEZ, R-G. “Protección de Datos limita el acceso de los partidos a información personal”. *El país*, 11 de marzo de 2019.

HERRAIZ, P. “Deep fake: así será la manipulación del futuro”. *El mundo*, 8 de mayo de 2019.

JOSE MARIN, J. y RUIZ GUEVERA, P. “Matemáticas para proteger la democracia”. *El país*, 19 de diciembre de 2018.

LAUSSON, J. « Facebook pourrait menacer la démocratie, selon un ex-patron des renseignements britanniques ». *Numerama*, 8 décembre 2018.

« Les Fake-news partagées sur Facebook par les « gilets jaunes » visionnées plus de 105 millions de fois ». *Le Nouvel Obs*, 13 mars 2019.

PEREZ-LANZAC, C. “No les pongas el trabajo fácil”. *El país*, 24 de marzo de 2019.

SIGNORET, P. « Wanted : une communauté Facebook de 800 000 membres et pas un rond ». *Le Monde*, 5 mai 2018.

TORRES DEL CERRO, A. “La lucha contra las “fake news” es un “talón de Aquiles” de las democracias”. *El confidencial*, 20 de septiembre de 2018.

VENTURA, B. “La fábrica de líderes: así contribuyen medios y redes sociales a elegir a los políticos”. *Yorokubu*, 22 de noviembre de 2018.

Ouvrages universitaires

BOULAY, S. *Usurpation de l’identité citoyenne dans l’espace public : astroturfing et communication politique*. Montréal : Doctorat en Communication, Université du Québec à Montréal, 2012. 359 p.

GALLARDO PAULS, B. y ENGUIX OLIVER, S. *Pseudopolítica: el discurso político en las redes sociales*. Valencia: Departamento de Teoría de los Lenguajes y Ciencias de la Comunicación, Universitat de València, 2016. 207 p.

Décrets, lois, circulaires, jurisprudences

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019 sobre el tratamiento de datos personales relativos a opiniones políticas y envió de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del articulo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general*, 7 de marzo de 2019.

CONSEIL CONSTITUTIONNEL. *Décision n° 2018-773 DC*, 20 décembre 2018.

CONSTITUTION FRANCAISE, 4 octobre 1958.

CONSTITUCION ESPAÑOLA, 6 de diciembre de 1978.

COUR DE JUSTICE DE L'UNION EUROPENNE. *Affaire 362/14 dite « Safe Harbor »*, 6 octobre 2015.

DECRET n° 2019-297 *relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général*, 10 avril 2019.

LEY ORGANICA 5/1985 *del régimen electoral general*, 19 de junio de 1985.

LEY ORGANICA 3/2018 *de protección de datos personales y garantía de los derechos digitales*, 5 de diciembre de 2018.

LOI ORGANIQUE n°2018-1201 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

LOI ORGANIQUE n°2019-221 *relative au renforcement de l'organisation des juridictions*, 23 mars 2019.

LOI n°62-1292 *relative à l'élection du Président de la République au suffrage universel*, 6 novembre 1962.

LOI n°78-17 *relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978.

LOI n°86-1067 *relative à la liberté de communication*, 30 septembre 1986.

LOI n°2016-1321 *pour une république numérique*, 7 octobre 2016.

LOI n°2018-1202 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

PARLEMENT EUROPEEN ET CONSEIL. *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995.

PARLEMENT EUROPEEN ET CONSEIL. *Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*, 12 juillet 2002.

PARLEMENT EUROPEEN ET CONSEIL. *Directive 2003/98/CE sur la réutilisation des informations du secteur public*, 17 novembre 2003.

PARLEMENT EUROPEEN ET CONSEIL. *Règlement (UE) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 27 avril 2016.

Déclarations officielles

CNIL. « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ». 8 novembre 2016.

CNIL. *Déclaration NS34* : « Communication politique ». 29 mars 2019.

CNIL. *Définition* : « Donnée sensible ».

CNIL. *Délibération n°2014-041*, 29 janvier 2014.

CNIL. « Election 2016/2017 : quelles règles doivent respecter les candidats et partis ? ». 8 novembre 2016.

CNIL. « La communication politique par courrier électronique ». 13 mai 2019.

CNIL. « Les droits des électeurs ». 13 mai 2019.

CNIL. « Les fichiers constitués dans le cadre des primaires ouvertes ». 8 novembre 2016.

CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». 2018.

COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». 26 et 27 novembre 2018.

- Resilient and inclusive democratic societies : supporting broad participation and representation ;
- Ensuring fair elections, pluralistic political debate and online and offline freedom of expression ;
- Sound and transparent information for an informed and pluralistic democratic debate : practical steps to ensure the support of the online world.

COMMISSION EUROPEENNE. *Commission guidance* : « The application of Union data protection law in the electoral context ». 12 septembre 2018.

COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions* : « Lutter contre la désinformation en ligne, une approche européenne ». 26 avril 2018.

COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE fait rapport sur les progrès réalisés dans la lutte contre la désinformation en vue du Conseil européen ». 14 juin 2019.

COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». 5 décembre 2018.

COMMISSION EUROPEENNE. *Déclaration relative au code de bonnes pratiques contre la désinformation* : « la Commission invite les plateformes en ligne à fournir davantage de précisions sur les progrès réalisés ». 28 février 2019.

COMMISSION EUROPEENNE. *Final report of the High Level Expert Group on Fake News and Online Disinformation*. 12 mars 2018.

COMMISSION EUROPEENNE. *First monthly intermediate results of the EU Code or Practice against disinformation*. 28 février 2019.

COMMISSION EUROPEENNE. *Last intermediate results of the EU Code of Practice against disinformation*. 14 juin 2019.

COMMISSION EUROPEENNE. *Report of the Independent High Level Group on Fake-news and online disinformation* : « a multi-dimensional approach to disinformation ». 2018.

EUROPEAN DATA PROTECTION BOARD. *Statement 2/2019 on the use of personal data in the course of political campaigns*. 13 mars 2019.

SUPERVISOR EUROPEO DE PROTECCION DE DATOS. *Dictamen 3/2018 sobre la manipulación en línea y los datos personales*. 18 de marzo de 2018.

Sites Internet

www.blogdumoderateur.com (consulté le 21 décembre 2018)

Vidéos

HUCHON, T. Comment Trump a manipulé l'Amérique ? *Arte*, 2018. Disponible sur : www.arte.fr (consulté le 13 octobre 2018)

BRANCHU EMILIE

2018/2019

Fake-news y propaganda individualizada: la puesta en peligro de los conceptos democráticos por las redes sociales.

Trabajo de fin de Máster

Doble título de Máster Hispano-Francés: Derecho de las Nuevas Tecnologías y Bio-derecho.

Bajo la dirección de: Sra. María Magnolia Pardo López

Sr. Marcel Moritz

Universidad de Murcia / Universidad de Lille

INDICE

AGRADECIMIENTOS

Este trabajo terminado, quisiera ante todo dar las gracias a mis dos profesores y directores de Trabajo de Fin de Máster, el Sr. Marcel Moritz y la Sra. María Magnolia Pardo López, que han demostrado una gran disponibilidad para asesorarme y acompañarme en la redacción de este.

También quiero dar las gracias al personal de las Universidades de Lille y Murcia, especialmente a los bibliotecarios, que han podido informarme con relevancia sobre las obras y artículos de revistas que podrían alimentar mi reflexión.

También quisiera expresar mi más sincero agradecimiento a los miembros del jurado por su cuidadoso examen y juicio de este trabajo.

Mis agradecimientos también van a Virginie Morgny y Maximilien Desmarais, que amablemente accedieron a corregir este TFM, y que lo hicieron con gran objetividad y perspicacia.

Además, me gustaría agradecer a mis padres y a mi hermano, Jacques, Corinne y Pierre Branchu, así como a mi compañero de vida, Victor Sponga, por el apoyo que me dieron tanto durante este escrito como a lo largo de mis estudios y por haber siempre creído en mis habilidades.

Del mismo modo, dirijo mis más sinceros agradecimientos a mis amigos cercanos, Dylan Lacoustasse, Romain Nave, AlexVercampt, Elies Adjem y Clément Prévost por haberme permitido desarrollar mis capacidades de curiosidad, reflexión espontánea y cuestionamiento perpetuo.

Por último, me gustaría agradecerme personalmente por el rigor y la tenacidad que he demostrado a lo largo de mis estudios y por terminarlos, así como por aprender de los obstáculos y dificultades que he encontrado.

ABREVIACIONES

ABBRE : Abreviaciones.

AEPD: Agencia Española de Protección de Datos.

CEDH: Convenio Europeo de los Derechos Humanos.

CEPD: Comité Europeo de Protección des Datos.

CNIL : Commission Nationale de l'Information et des Libertés.

CRT: Comisión de Radio y Televisión.

CSA : Conseil Supérieur de l'Audiovisuel.

CSDHLF: Convenio de Salvaguardia de los Derechos Humanos y de las Libertades Fundamentales.

DUDH: Declaración Universal de los Derechos Humanos.

EE. UU.: Estados Unidos.

GT29: Grupo de Trabajo del Artículo 29.

IA: Inteligencia Artificial.

INE: Instituto Nacional de Estadística.

LIL : Loi Informatique et Libertés.

LOPD: Ley Orgánica de Protección de Datos.

LOREG: Ley Orgánica del Régimen Electoral General.

RGPD Reglamento General de Protección de Datos.

TFUE: Tratado de Funcionamiento de la Unión Europea.

UE: Unión Europea.

INTRODUCCION

De la informática a las redes sociales

Desde los años 1960, la informática forma parte integrante de nuestra vida cotidiana y no cesa de perfeccionarse para facilitar las comunicaciones entre los individuos. La Academia francesa, en 1966, la define como "la ciencia del tratamiento racional, por maquinas automáticas, de la información considerada como el soporte de los conocimientos humanos y de las comunicaciones en los ámbitos técnicos, económicos y sociales". Esta definición deja pensar que la informática solo se basa en la repartición de los conocimientos adquiridos, pero de verdad es una herramienta peligrosa usada para recoger y tratar informaciones personales sobre los individuos.

De hecho, con la llegada de internet en el hogar de cada persona, el vínculo con la informática se acelera. A partir de este momento, el individuo contribuye a crear la información – ya no se conforma con consultarla –, incluyendo la información personal, y la desinformación. Así, las comunicaciones están intensificadas y las relaciones entre los individuos simplificadas, para no decir demultiplicadas con la llegada de las redes sociales en los años 2000 (Facebook, Twitter, Google+, etc.). Una red social se define tradicionalmente como un conjunto de individuos, organizaciones o entidades manteniendo relaciones sociales, basadas en la amistad, el trabajo colaborativo o el intercambio de informaciones[1]. Sin embargo, tal definición no puede aplicarse a las redes sociales informáticas. La enumeración de los fundamentos sobre los cuales se supone que se basen las relaciones entre los individuos es demasiada exhaustiva ya que no se interesa a la política, aún más presente en el mundo virtual que en la vida real.

Hoy en día, más populares que los periódicos o la radio, los autores llaman las redes sociales "los nuevos medios de comunicación", plataformas en las cuales las informaciones, verdaderas o falsas, están conocidas de todos en un segundo. De esta innovación tecnológica nacieron practicas mal intencionadas como la de la desinformación. De hecho, es muy peligrosa ya que 20% de la población usa las redes sociales como única fuente de información, subiendo hacia 65% para la población joven (18-24)[2].

[1] MERCANTI-GUERIN, M. Facebook, un nouvel outil de campagne : analyse des réseaux sociaux et marketing politique. *Direction et Gestion*, 2010. La Revue des Sciences de Gestion, n°242.
[2] TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *Quaderni*, 2018. N°96.

Más allá de la información, y de la desinformación, el volumen de los datos personales acumulado a nivel mundial dobla cada ano gracia – o por culpa – a las redes sociales. De tal manera, 67% de los usuarios de internet y de las redes sociales estarían interesados por el uso de sus datos personales con fines de propaganda electoral individualizada. Así, las redes sociales se presentan como una gran oportunidad para los políticos, que sea para difundir una propaganda generalizada o para dirigir una propaganda personalizada[3].

Orígenes del uso de las redes sociales en la vida política

Hoy en día, los políticos son muy presentes en las redes sociales, sobre todo durante el proceso electoral. De hecho, las redes sociales se presentan como una herramienta de propaganda muy útil. Aunque la apelación de "propaganda" mantenga una connotación bastante negativa debido a su uso durante la Primera Guerra Mundial, solo se define como la acción ejercida en la opinión para que tenga y sostenga ciertas ideas políticas. Edward Luis Bernays, en su obra *Propaganda* (1928), ya quería devolverle su acepción neutral y por esta razón, en lugar de "comunicación política", se usará exclusivamente ese término en este desarrollo[4].

En 2008, Barack Obama, futuro presidente de los Estados Unidos (denominados los "EE. UU." más adelante), es el primero a usar las redes sociales y a aprovechar los datos personales que contienen para llevar a cabo su propaganda. Igualmente, en 2012, los consultantes de Blue State Digital le acompañan y le permiten de cruzar datos políticos con datos comerciales para obtener informaciones normalmente inaccesibles sobre el comportamiento cotidiano de los ciudadanos estadunidenses[5].

En fin, todas esas informaciones colectadas permiten de elaborar perfiles muy precisos, después usados para dirigir una propaganda totalmente personalizada según las necesidades y deseos de cada individuo. Esta técnica se llama el "micro-targeting"[6]. Desde el éxito de las dos campañas electorales de Barack Obama, el recurso a la analítica de los datos personales se ha convertido en un pilar logístico del convencimiento político. No obstante, no es Barack Obama quien, de verdad, ha hecho del micro-targeting una práctica famosa, sino su predecesor Donald Trump.

---

[3] COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». Sound and transparent information for an informed and pluralistic democratic debate : practical steps to ensure the support of the online world. 26 et 27 novembre 2018.
[4] BERNAYS, E. *Propaganda : comment manipuler l'opinion en démocratie*. New York : Zones, 1928. 144 p.
[5] « Elections : à la fête du client ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c'est terminé, N°149.
[6] THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

El escándalo Cambridge Analytica y la elección de Donald Trump como presidente de los EE. UU.

"Como Trump manipuló América?"[7], es el título que dio *Arte*[8] a su reportaje sobre la elección de Donald Trump, actual presidente de los EE. UU., y el escándalo que tocó Facebook. Especializada en la influencia de opinión, la sociedad Cambridge Analytica habría colectado los datos personales detenidos por la red social con fines políticas y habría contribuido a que sea elegido Donald Trump como presidente de los EE. UU. Ese reportaje da continuación a las revelaciones de Christopher Wylie, exempleado de Cambridge Analytica, quien, después de haber denunciado el hackeo de los datos personales de 87 millones de usuarios de Facebook, explicó como estos datos robados fueron usados para influir en la elección de Donald Trump.

De hecho, Cambridge Analytica permitió la identificación de individuos haciendo perfilado psicológico, que la sociedad llama "micro identificación comportamental". Aunque lo llame de manera diferente, solo aplica la técnica del micro-targeting inventada por Barack Obama, que consiste en combinar los datos personales de los individuos con fines de determinar sus miedos y preocupaciones, datos personales comprados a Facebook. En fin, el micro-targeting puesto en marcha por Cambridge Analytica permitió a Donald Trump de orientar sus intervenciones públicas y, sobre todo, de centrarlas en los estados donde tenía más suerte de convencer nuevos simpatizantes. Como tal, el eslogan de la sociedad es muy alusivo: "Dirige el mensaje correcto, a la persona correcta, al momento correcto".

Por otra parte, los "news junkies" ("los adictos a la información" en español) aumentan considerablemente el uso de las redes sociales por parte de los políticos[9]. De hecho, el corolario directo a la creación de la información política es la desinformación, también conocida como la "Fake-news". Se define como una información voluntariamente engañosa, inexacta o falsificada. Se trata de un artículo de prensa falso publicado en un sitio de actualidad, falso o no, destinado a abusar o manipular el elector. *A contrario* del micro-targeting, la Fake-news es una herramienta potente pero poco onerosa y muy rentable[10]. Aunque no sepamos si Donald

[7] HUCHON, T. Comment Trump a manipulé l'Amérique ? *Arte*, 2018.
[8] Canal de información francés
[9] GALLARDO PAULS, B. y ENGUIX OLIVER, S. *Pseudopolítica: el discurso político en las redes sociales*. Valencia: Departamento de Teoría de los Lenguajes y Ciencias de la Comunicación, Universitat de València, 2016. 207 p.
[10] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions* : « Lutter contre la désinformation en ligne, une approche européenne ». 26 avril 2018.

Trump usó personalmente esta técnica para convencer la opinión pública, es irrefutable que las Fake-news influenciaron los votos en su favor – o no[11].

Hay que constatar que la vida política ha sido significativamente modernizada por las practicas estadunidenses y ya se han desplegadas en Europa. El caso Cambridge Analytica demostró la importancia de luchar contra la opacidad de la información hacia las personas tratando del uso de sus datos personales. Además, afectó gravemente las libertades de opinión y de expresión, así que la posibilidad de pensar libremente sin manipulaciones. Por lo tanto, el público europeo se preocupa de la llegada de esas prácticas, y sobre todo de la protección de sus derechos y libertades fundamentales.

Uso de las redes sociales en propaganda francesa y española

En este desarrollo, no parece oportuno interesarse en la Unión Europea (denominada la "UE" más adelante) en su globalidad. De hecho, aunque el Reglamento General de Protección de Datos[12] (denominado el "RGPD" más adelante), adoptado por la UE en 2016, tenga por objetivo uniformizar la legislación sobre la protección de los datos personales a nivel europeo y que la Comisión Europea tomase medidas relativas al fenómeno de Fake-news, parece mas pertinente interesarse a la legislación que los Estados miembros adoptan para sancionar los usos abusivos de tal propaganda en sus territorios.

Para ello, nuestra reflexión se interesará solamente a España y Francia, países vecinos a la legislación bastante similar, ya que España se inspiró mucho de lo que existía en Francia para editar sur normas. Asimismo, ambos países han recientemente sido interesados por procesos electorales: las elecciones presidenciales de 2017 para Francia y las elecciones generales de 2019 para España. Además, como países Estados miembros de la UE, también han sido interesados por las elecciones europeas de 2019. Así, se presentan como los candidatos ideales para nuestro estudio.

Esas tres elecciones han sido muy mediatizadas y, sobre todo, han sido el objeto de una propaganda digital importante. El partido "Vox", por ejemplo, es el partido español que cuenta lo más importante número de "followers"[13] en Instagram, la red social que lo más se ha desarrollado en 2018 y la más usada por los individuos entre 16 y 30 años, según un informe

[11] "Fake news: contra las falsedades". *El país*, 12 de marzo de 2019
[12] PARLEMENT EUROPEEN ET CONSEIL. *Règlement (UE) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 27 avril 2016.
[13] Las personas que siguen una cuenta en una red social.

de la Asociación de Comunicación Digital española. Como ocurrió por los partidos "Podemos" y "Ciudadanos", "Vox" logró una cierta presencia parlamentaria gracia a la propaganda digital que llevó a cabo[14].

En Francia, el partido "En Marche!" de Emmanuel Macron, actual presidente francés, es el mejor ejemplo de la ventaja que representan las redes sociales en cuanto se sabe usarlas hábilmente. El partido emergente supo imponerse frente a partidos más antiguos gracia a un programa de estrategia electoral desarrollado por la sociedad Big Data. Tal programa permite optimizar la gestión de varios datos personales recogidos por el candidato, cuales permiten animar y movilizar las comunidades perfeccionando la comunicación política según los perfiles de los diferentes contactos[15].

Desde unos años, la creación y el desarrollo de esas tecnologías son posibles gracia al "Big data". Desde que aparecieron internet y las redes sociales, aproximadamente 2,5 trillones de octetos de datos personales son producidos cada día. El conjunto de estos datos responde a las características de volumen, velocidad y variedad correspondiendo a la definición del Big data. Este ultimo permite a los jefes de Estados de responder a sus dos necesidades principales:

- La creación de una lista de ciudadanos, voluntarios y donadores a contactar;
- La construcción de modelos predictivos para hacer campañas de propaganda individualizada más potentes[16].

El Big data se alimenta principalmente del "Open data", que muchas veces se omite de mencionar. El Open data es el conjunto de datos personales colectados por las entidades publicas o privadas encargadas de un servicio público. Esos datos están puestos a disposición en formato digital en plataformas nacionales, lo que permite su libre acceso y su reutilización por los ciudadanos y organizaciones, incluso los partidos políticos[17]. Sin embargo, el RGPD prevé que la recogida de datos debe respetar finalidades y que otro tratamiento ulterior no puede ser incompatible con estas finalidades. Así, se plantea una pregunta: ¿puede ser considerado que los datos reutilizados por una propaganda electoral respetan la noción de finalidades incompatibles mientras han sido recogidos para una finalidad totalmente diferente por los

[14] VENTURA, B. "La fábrica de líderes: así contribuyen medios y redes sociales a elegir a los políticos". *Yorokubu*, 22 de noviembre de 2018
[15] THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *op.cit.*
[16] NICKERSON, D-W. and ROGERS, T. Political campaigns and Big Data. *Journal of Economic Perspectives*, 2014. Volume 28, n°2.
[17] LEHMANS, A. Les réinventions de la démocratie à l'aune de l'ouverture des données : du discours de la participation aux contraintes de la gouvernance. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

servicios públicos? La pregunta se plantea aún más cuando un programa de estrategia electoral implica *de facto* el uso de algoritmos. Estos últimos son unos procesos constituidos por un conjunto de operaciones y reglas operacionales dadas por un calculo. Generan necesariamente una decisión automatizada, la cual es el resultado de los cálculos programados.

Por lo tanto, parece ser indispensable regular todas esas prácticas para no causar los mismos escándalos que lo hicieron los EE. UU. Además, aunque el fenómeno de Fake-news no haya sido evocado en esta parte, Francia y España también han sido sus víctimas. Sin embargo, este fenómeno solo es peligroso para los derechos fundamentales, sobre todo el derecho a la información y el derecho a la vida privada los cuales están en el centro de nuestro desarrollo, cuando es objeto de individualización gracia al uso de los datos personales. Por tal razón nuestra reflexión se interesó principalmente a este último, pero el fenómeno de Fake-news no está excluido de una necesidad legislativa.

Insuficiencia de las regulaciones española y francesa en la materia

Frente a los cambios societales – en los cuales están incluidas las evoluciones tecnológicas – la legislación suele intervenir después que ocurrió el cambio. Tal es el caso para España y Francia, ya que no han hecho ningún cambio a nivel constitucional para permitir una adaptación jurídica al contexto actual. De hecho, la propaganda sigue definida como la acción ejercida sobre la opinión mediante folletos, radio y televisión para que tenga y sostenga ciertas ideas políticas.

Por dicho motivo, España intentó reaccionar, como consecuencia a la adopción en noviembre de 2018 de la Ley Orgánica de Protección de Datos[18] (denominada la "LOPD" más adelante), modificando su Ley Orgánica del Régimen Electoral General[19] (denominada la "LOREG más adelante) y especialmente con la inserción del artículo 58 bis previendo un principio que permite a los partidos políticos hacer SPAM electoral y propaganda personalizada en internet. El termino de propaganda es voluntariamente genérico y que permite integrar la noción de micro-targeting y la de Fake-news personalizada[20]. Esta última, que sea personalizada o no, no es objeto de una regulación constitucional más importante. Finalmente, las Fake-news

[18] LEY ORGANICA 3/2018 *de protección de datos personales y garantía de los derechos digitales*, 5 de diciembre de 2018.
[19] LEY ORGANICA 5/1985 *del régimen electoral general*, 19 de junio de 1985.
[20] DEL CASTILLO, C. y SARABIA, D. "Aprobada la ley que permitirá a los partidos hacer spam electoral y propaganda personalizada en internet". *El diario*, 21 de noviembre de 2018

diseminadas a todos los individuos parecen más peligrosas ya que no son objetas de una regulación relativa al uso de los datos personales, como lo hace el RGPD.

Esa regulación más importante pretende luchar, de manera específica, contra el fenómeno de "filtro burbuja". De hecho, perjudica gravemente al principio fundamental de pluralismo político, lo cual se basa en la existencia de varios partidos políticos, permitiendo a los electores de tener varias opciones y entonces, la libertad de elegir. El filtro burbuja tiene por efecto, gracia a los algoritmos de recomendaciones, de individualizar para cada individuo los contenidos publicados en su cuenta de red social según sus preferencias deducidas de sus datos personales recogidos. Igualmente, muchos principios fundamentales y democráticos están en peligro por culpa del uso de los datos personales con fines políticas. Por esta razón, un recurso de inconstitucionalidad en contra del artículo 58 bis de la LOREG ha sido ejercito ante el Defensor del Pueblo al principio de marzo de 2019.

Tratando del uso de los datos personales, hay que constatar que solo la LOPD y la "Loi Informatique et Libertés"[21] (denominada la "LIL" más adelante) garantizan la protección de estos datos. Siendo finalmente unas transposiciones bastante fieles del RGPD, ambas normas tienen varias carencias que serán el objeto de un desarrollo ulterior. De la misma manera, Francia hizo el intento de adoptar una ley[22] para regular el fenómeno de Fake-news. Es cierto que sanciona las acciones de desinformación, pero tampoco es convincente. *A contrario*, España no tomó ninguna medida para controlar las Fake-news, igual que no lo hizo Francia para el uso de los datos personales con fines políticas.

¿Frente a tal insuficiencia legislativa, como garantizar la perennidad de nuestros principios democráticos que enmarcan las campañas electorales y la elección de los jefes de Estados francés y español?

Sin tener la pretensión de proponer una regulación a la propaganda electoral actual, que se ejerce principalmente por y gracia a las redes sociales, este desarrollo analizará las carencias de las regulaciones en vigor, que sean europeas, constitucionales o legislativas, y los intentos que hacen para canalizar estas practicas peligrosas para los derechos y libertades fundamentales. Por lo tanto, es conveniente interesarse a la propaganda electoral generalizada, mediante las Fake-news, y más aún al peligro que representa para el derecho fundamental a la información (**PRIMERA PARTE**), primer derecho esencial al buen funcionamiento de nuestros procesos

[21] LOI n°78-17 *relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978.
[22] LOI n°2018-1202 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

democráticos. Luego, cabe interrogarse sobre la propaganda electoral personalizada. De hecho, como los datos personales están usados con fines políticas, tal propaganda perjudica gravemente al derecho fundamental a la protección de estos últimos (**SEGUNDA PARTE**), lo cual es el garante de los demás derechos fundamentales que, también, van a ser objeto de nuestra reflexión.

PARTE 1. Propaganda electoral generalizada: la puesta en peligro del derecho fundamental a la información por el fenómeno de Fake-news

Antes de que podamos analizar las lagunas legales y hacer propuestas regulatorias para evitar un desbordamiento del fenómeno de Fake-news (**TITULO 2**) – suponiendo que esto no haya ocurrido ya – debemos considerar como se inscribe este último en nuestra noción actual de propaganda electoral (**TITULO 1).** De hecho, la propaganda electoral está sujeta principalmente a una regulación constitucional. Sin embargo, es particularmente obsoleta en y no es adecuada para un fenómeno tan reciente conocido como el de las Fake-news.

TITULO 1. Inscripción del fenómeno de Fake-news en nuestra noción actual de propaganda electoral

El fenómeno de las Fake-news es motivo de preocupación porque es una herramienta temible para manipular la opinión, pero sobre todo porque infringe directamente el derecho a la información, así como otros principios democráticos franceses y españoles (**Capítulo 2**). Muy lejos de las concepciones actuales que tengan los derechos francés y español de la propaganda (**Capítulo 1**), la Fake-news es un concepto difícilmente "domesticable" debido a las varias formas que puede adoptar.

Capítulo 1. Las nociones actuales de propaganda en derecho francés y español

En el imaginario colectivo, la propaganda política es un proceso perjudicial para la democracia que pretende manipular el consentimiento del elector **(1.2)** y que sólo se aplica en los países dictatoriales. Sin embargo, no es más que un intento de convencer a los votantes y, como tal, se presenta como una forma normal de organización de la vida política. Así, una vez que se le restablece su significado neutro, nos damos cuenta de que existe en nuestras democracias francesas y españolas que intentan regularlo constitucionalmente (**1.1**).

1.1. Regulación constitucional de la propaganda electoral

Cuando un país elige a un nuevo jefe de Estado, se lleva a cabo sistemáticamente una campaña electoral *a priori.* El artículo 50 de la LOREG define la campaña electoral como el conjunto de actividades legales llevadas a cabo por candidatos, partidos, federaciones,

coaliciones y grupos políticos con el fin de captar los votos del electorado. Sobre la base de la comunicación política, que es el conjunto de procesos de comunicación que apoyan una democracia, la campaña electoral -o propaganda electoral como preferimos llamarla- trata así de guiar el voto del votante que se presenta como el proceso político necesario para mantener la democracia.[23]

Las informaciones transmitidas por televisión tienen la capacidad de alterar los índices de valoración pública de los votantes y los gobiernos. Sin embargo, la televisión sólo emite imágenes para un espectador pasivo que las está viendo, mientras que el ciberespacio es un mundo interactivo con usuarios dinámicos[24]. Por lo tanto, las redes sociales permiten el ejercicio efectivo de la democracia inclusiva, la participación y la representación de todos los ciudadanos (la participación equitativa de los jóvenes, las mujeres y otras minorías no suelen representados). Así, cada uno, en las redes sociales, puede producir su propia propaganda, una propaganda que obviamente no cumple con las reglas constitucionales establecido por los gobiernos.

De tal manera, existen muchos abusos, especialmente porque las normas aplicables a la propaganda electoral no se aplican a la que se lleva a cabo en las redes sociales. De hecho, desde el punto de vista constitucional, la regulación en este ámbito, que sea en Francia o en España, es particularmente obsoleta.

En Francia, el artículo 1 de la ley "Léotard" del 30 de septiembre de 1986[25] garantiza el respeto del carácter pluralista de la expresión de los corrientes de pensamiento y de opinión. Para ello, asegura la expresión más diversa posible de los partidos políticos con un tiempo de conversación equilibrado entre ellos. Aunque esta ley no tenga valor constitucional, el Consejo Constitucional francés estimó en 1986 y en 1989 que "el respeto del pluralismo es una de las condiciones de la democracia" y más ampliamente que "constituye el fundamento de la democracia"[26].

La ley francesa sobre la elección del Presidente de la República del 6 de noviembre de 1962[27], que tiene valor constitucional, también examina el principio del pluralismo político. En el apartado I bis de su artículo 3, garantiza que "los editores de servicios de comunicación

[23] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. Montréal : Doctorat en Communication, Université du Québec à Montréal, 2012. 359 p.
[24] PIEDRA CARDOSO, J. Democracia y redes sociales. *Universidad Verdad*, 2017. 1(72).
[25] LOI n°86-1067 *relative à la liberté de communication*, 30 septembre 1986.
[26] CNIL ET CSA. Guide : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». *op.cit.*
[27] LOI n°62-1292 *relative à l'élection du Président de la République au suffrage universel*, 6 novembre 1962.

audiovisual respeten, bajo el control del Conseil Supérieur de l'Audiovisuel ("Consejo Superior del Audiovisual" en español, llamado el "CSA" más adelante) el principio de equidad con respecto a reproducción y comentarios de las declaraciones y escritos de los candidatos y la presentación de su persona".

Del mismo modo, en España, los artículos 60 y 61 de la LOREG establecen que los partidos, federaciones, coaliciones y grupos políticos tienen derecho a espacios de propaganda libres en programas de radio y televisión de propiedad pública durante la campaña. El respeto del pluralismo está garantizado por la Comisión de Radio y Televisión (llamado el "CRT" más adelante).

Si nos vemos obligados a mirar las leyes orgánicas en lugar de las propias constituciones francesa[28] y española[29], es porque están totalmente desinteresadas de la propaganda necesariamente llevada a cabo en paralelo a las elecciones. De hecho, sólo se preocupan de las elecciones del jefe de Estado en sus aspectos procesales.

Por lo que se refiere a Francia, su ley de 1962 ha sido objeto de muchas reformas. De hecho, unos artículos del Código Electoral se han incluido en su artículo 3. Sin embargo, se ocupa principalmente de la propaganda tradicional – a saber, propaganda impresa, televisiva o radiofónica – pero menciona varias veces (en sus artículos L48-1 y L49, por ejemplo) "la propaganda electoral difundida por cualquier medio de comunicación electrónico al público". Del mismo modo, en el artículo L49-1, se interesa en los sistemas automatizados de llamadas telefónicas. Esto refleja la voluntad de adaptarse a las nuevas tecnologías y a las nuevas prácticas políticas que resultan de ellas. Sin embargo, cuando se examina la parte reglamentaria adjunta a esta parte legislativa, se da cuenta de que no existe ningún marco con respecto al uso de estas nuevas tecnologías y, aún peor, sólo se trata de la propaganda impresa que parece ser totalmente obsoleta hoy en día.

Por otra parte, Francia adoptó la ley "Fake-news" en dos textos. Su segundo texto, que no tiene valor constitucional, muestra más interés en las redes sociales ya que las aborda por primera vez en su concepción actual y también porque permitió la modificación de varios artículos del Código Electoral.

Por lo que se refiere a España, la LOREG afirma en su artículo 50 que la campaña institucional pretende informar a los ciudadanos sobre la fecha de votación, así como sobre el procedimiento

[28] CONSTITUTION FRANCAISE, 4 octobre 1958.
[29] CONSTITUCION ESPAÑOLA, 6 de diciembre de 1978.

de votación, sin influir en la dirección del voto de los electores. Sin embargo, esta es sólo la campaña institucional y una vez que la LOREG se interesa a la campaña electoral, la noción de influencia de los votantes desaparece. A primera vista, esto parece bastante lógico, ya que el propósito mismo de la propaganda no es más que convencer al votante. Sin embargo, al igual que la legislación francesa, debe establecerse un marco en este ámbito para evitar abusos.

Esto es particularmente lo que sucedió con el artículo 58 bis que, sin duda, tiene el mérito de mencionar las redes sociales y el uso de datos personales con fines de propaganda electoral dirigida, pero que también fue rápidamente objeto de indignación pública en vista a la violación del derecho a la privacidad y a la protección de los datos personales. Desde entonces, su primer párrafo ha sido anulado, y aunque insuficiente, volveremos a la decisión adoptada por el Tribunal Constitucional más adelante en el desarrollo.

1.2. Manipulación del consentimiento de los votantes y expansión del espacio público "digital"

Cuando hablamos de propaganda política en los medios de comunicación, y esto también se refiere a las redes sociales conocidas como "nuevos medios de comunicación", inmediatamente nos viene a la mente países como Corea del Norte, Irán o Kazajistán. Sin embargo, el ejemplo de la elección de Donald Trump y la estrategia que ha empleado para que su campaña electoral sea un éxito nos enseña que también existe en nuestros países de América y Europa.

De hecho, si la misión de los medios de comunicación es proporcionar información objetiva y completa al público para que pueda participar de manera informada en el proceso político, Noam Chomsky y Edward Herman demuestran que este no es el caso en su libro *Manufacturing consent* (1988)[30]. Por transposición de este libro al contexto actual, es posible identificar las cuatro funciones de manipulación que las redes sociales ofrecen a los partidos políticos:

- Crear “trending topics” (“temas de tendencia” en espanol) utilizando hashtags[31] que luego son amplificados por cuentas de robots;
- Identificar hashtags reales y anticipar ataques por cuentas de afiliados, sean falsas o no;
- Identificar los "trolls"[32] o cuentas de oponentes;

[30] CHOMSKY N. et HERMAN, E. *Manufacturing consent : the political economy of the mass media*. New York : Pantheon Books, 1988.
[31] Utilización del símbolo "#" antes de una palabra para acceder a un enlace donde se agrupan todos los mensajes a los que se hace referencia en esa palabra.
[32] Persona que publica mensajes negativos en Internet con el fin de alimentar las controversias.

- Aumentar artificialmente los "me gusta" en la cuenta de un político[33].

Además de estas nuevas funciones manipuladoras que ofrecen las redes sociales, cabe destacar también que han ampliado considerablemente el espacio público. Utilizado como referencia normativa para la comunicación en democracia, los autores hablan ahora de un espacio público "digital". Legislar en un ámbito tan amplio no es tan fácil para los gobiernos.

El filósofo alemán Jurgen Habermas define el espacio público como el proceso en el que el público, formado por individuos que hacen uso de su razón, se apropia la esfera pública controlada por la autoridad y la transforma en una esfera en la que se ejercen críticas contra el poder del Estado. Es, en definitivo, un lugar situado entre el Estado y la sociedad civil donde se reúnen los ciudadanos privados, formando así una audiencia que puede discutir libre y racionalmente[34].

De tal forma, las redes sociales parecen fortalecer la democracia porque permiten la comunicación entre los ciudadanos y entre los partidos políticos y los ciudadanos[35]. Desde el punto de vista de los políticos, la participación ciudadana en las redes sociales también tiene la gran ventaja de alimentar el Open data – y también ocurre lo contrario: el Open data alimenta la participación ciudadana[36] –.

En resumen, el espacio público "digital" sólo se está expandiendo a medida que el Open data, el Big data, los datos detenidos por empresas y los datos personales de las personas están entrelazados... Esto explica por qué el concepto es vago y que, como referencia normativa, no es fácil para los gobiernos dominarlo. Así, sin poder proponer una regulación satisfactoria, y debido a que los ciudadanos contribuyen a ampliar este espacio público un poco más cada día, nacen los abusos. La primera es la desinformación, que perjudica gravemente la participación ciudadana, la democracia y ciertos derechos y libertades fundamentales.

[33] GALLARDO PAULS, B. y ENGUIX OLIVER, S. *Pseudopolítica: el discurso político en las redes sociales*. *Op.cit.*
[34] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. *op.cit.*
[35] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *Op.cit.*
[36] LEHMANS, A. Les réinventions de la démocratie à l'aune de l'ouverture des données : du discours de la participation aux contraintes de la gouvernance. *op.cit.*

Capítulo 2. El puesta en peligro del derecho fundamental a la información y de los principios democráticos franceses y españoles por el fenómeno de Fake-news

Antes de que podamos constatar la insuficiencia de las normativas francesa y española (**2.3**) con respecto al fenómeno de Fake-news, es necesario en primer lugar interesarse a este complejo fenómeno y tratar de darle la definición más precisa que pueda (**2.1**). A estudiarlo, el peligro que representa para el derecho fundamental a la información, piedra angular de la democracia, así como para los principios esenciales de la democracia, aparece (**2.2**).

2.1. Presentación y análisis del fenómeno de Fake-news

Sin una definición precisa del fenómeno de Fake-news y un conocimiento sólido de sus orígenes e impactos, parece difícil comprenderlo. Nacido en 1999 del programa satírico y parodia estadounidense "The Daily Show", la Fake-news es una información intencionalmente engañosa, inexacta, falsa o falsificada. Este artículo de prensa falso, publicado en un sitio web falso o no de noticias, está destinado a abusar o manipular el votante[37]. Con esta definición, es fácil notar que la Fake-news nace de una intención deliberada de engañar que pueda tener une motivo político o de lucro, y no de torpeza.

Tratando de torpeza, cabe señalar que puede existir cuando los periodistas difunden una Fake-news sin comprobarla. Así es como puede llegar a ser publicada en un sitio web de noticias reales. Aquí es donde se presenta el verdadero peligro de las Fake-news: los ciudadanos pueden engañar a otros ciudadanos, pero ahora también son capaces de engañar a los propios periodistas.

En este sentido, las redes sociales tienen mucho que ver con ello. La rapidez con la que reaccionan los usuarios hace que los periodistas reaccionen de la misma manera y sean más laxos tratando de verificar la información que transmiten: en estas circunstancias, incluso hablamos de "instants articles" ("artículos instantáneos" en español) tanta la difusión de la información es rápida. Esto no es realmente sorprendente ya que un estudio realizado por la Universidad de Stanford demostró que las Fake-news generan más "me gusta" que la información real (9 millones frente a 7 millones)[38]. Por lo tanto, más allá de la mera torpeza, también se plantea la cuestión de saber si el beneficio no tendría prioridad hoy en día sobre la ética periodística en las redes sociales.

[37] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[38] JAYSON, H. (trad : RICHET, I.). Un guide critique des fake-news : de la comédie à la tragédie. *op.cit.*

De hecho, cabe señalar que las redes sociales son intermediarios formidables de las Fake-news: una vez producidas, son responsables de difundirlas y financiarlas[39]. El método de financiación es particularmente proporcional a la popularidad de las Fake-news compartidas y, por lo tanto, al número de "me gusta" que generan. Así, en comparación con la información verdadera, los beneficios aumentan de casi un 30% – si tenemos en cuenta las cifras propuestas por el estudio de Stanford – y esto tanto para el productor de la Fake-news como para la red social que la difunde.

Más allá del interés lucrativo, si las redes sociales no fueran vectores de desinformación y promovieran un fácil acceso a informaciones diversas de calidad, ayudarían a hacer que los procesos democráticos sean más inclusivos[40]. Ahora mismo, con las Fake-news, alimentan el odio, la división y la desconfianza hacia la democracia[41], que ya se sienten en las comunidades "desatendidas", a saber, las minorías.

Las Fake-news son similares a una marca de pertenencia a un grupo o una ideología. Como se ha visto anteriormente, crean sistemáticamente división y hostilidad entre las comunidades políticas. De esta manera, si el impacto creado por estas últimas es tal que hace imposible votar por el candidato primeramente elegido (que sea por una pérdida de confianza o simplemente porque no llegó a la segunda ronda, o porque sólo un voto "útil" podría ser exprimido con fin de evitar lo peor), el elector se abstiene. Como resultado, es más probable que el candidato "manipulador" sea invertido.

Sin embargo, el fenómeno de Fake-news, gravemente acentuado por los instants articles, no es el único que pesa en las elecciones y la manipulación de los votantes. El concepto de "post-truth" caracteriza las circunstancias en las que los hechos objetivos tienen menos influencia en la opinión pública que los llamamientos a las emociones[42]. "Post-truth" se refiere a una cultura política en la que los jefes de Estados dirigen los debates hacia emoción mediante el uso de elementos de lenguaje e ignorando los hechos y la necesidad de presentarles sus argumentos, esto siempre con fines electorales.

[39] *Ibid.*
[40] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[41] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». *op.cit.*
[42] TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *op.cit.*

2.2. Peligros existentes para el derecho fundamental a la información y los principios democráticos

La causa principal de amplificación del fenómeno de Fake-news es la ausencia de reglas y ética periodística en las redes sociales. De hecho, los medios tradicionales (es decir, la radio, la televisión o los periódicos) responden a un Código de ética. Como resultado, están sujetos a ciertas reglas incluyendo imparcialidad, pluralismo, diversidad cultural, contenido perjudicable, publicidad y contenido patrocinado[43] Estas reglas surgen de muchas responsabilidades relacionadas con su función de información:

- Deben proporcionar a las personas un relato veraz, completo e inteligible de los acontecimientos en un contexto que les dé sentido;
- Deben proporcionar a las personas un foro de intercambio para informar y responder a varias preguntas;
- Deben dar una imagen representativa de los grupos constituyendo la sociedad;
- Deben respetar, además de representar, los objetivos y valores de la sociedad;
- Deben proporcionar a las personas un acceso completo a la información del día[44].

Más allá de estas reglas y responsabilidades, hay que tener en cuenta que los medios tradicionales son libres e independientes. Lejos de ser su única diferencia con las redes sociales, es sin embargo importante porque, impulsadas por un fuerte objetivo lucrativo, las redes sociales responden a un modelo económico que no corresponde a la obligación de proporcionar información. Como se ha visto anteriormente, la popularidad de la información tiene prioridad sobre la calidad de la información para estas últimas. Por ejemplo, la Comisión Europea ha constatado que el 55 % de los europeos se ven afectados por las restricciones y la censura del debate político sobre las redes sociales[45].

Por lo tanto, se plantea la cuestión de saber si las redes sociales son actores políticos, al igual que los periodistas tradicionales y los medios de comunicación. Como respuesta, digamos que más que un actor político, las redes sociales se presentan mejor como una herramienta política porque no generan su propio contenido informativo, sólo lo difunden a gran escala.

[43] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[44] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. *op.cit.*
[45] COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». Sound and transparent information for an informed and pluralistic democratic debate : practical steps to ensure the support of the online world. *op.cit.*

Los políticos han tomado esta nueva herramienta porque les permite evitar la intervención de empresas periodísticas. La falta de ética y los criterios periodísticos mínimos para verificar o validar fuentes en las redes sociales les permite recurrir a discursos sensacionales, a saber, la técnica de post-truth[46].

El 43% de los usuarios se enteran de las informaciones en las redes sociales sin comprobar la fuente y es en este ámbito que los periodistas deben intervenir. Un estudio español sobre el impacto de las Fake-news ha demostrado que sólo el 14% de la población puede identificarlas. Como tal, la falta de educación en vista de estas últimas es la segunda causa principal de la amplificación del fenómeno[47].

En respuesta, se han establecido cursos específicos sobre las Fake-news en varias universidades[48]. Sin embargo, estos últimos sólo están dirigidos a los futuros periodistas, que representan la población más informada en cuanto a su identificación. Con el fin de combatir estas, sería apropiado proponer estos cursos a otros estudiantes, o incluso a profesores. ¿Pero qué hacemos con los ciudadanos que no cursan estudios universitarios? Se debe llevar a cabo una educación a las Fake-news antes de que se alcance la edad de 16 años, edad hacia la que el alumno debe asistir a clases. Los impactos de estas últimas no deben ser descuidados por ningún ciudadano que, tarde o temprano, también se convierte en un votante.

Por otra parte, los defectos de los métodos de elección de nuestras democracias contemporáneas se multiplican en gran medida por las operaciones de manipulación de opinión. De hecho, muchos autores señalan que las Fake-news tienden a aumentar el número de corrientes políticas, lo que llaman división. Si bien esto puede parecer algo bueno a primera vista, ya que tiende a intensificar el pluralismo político y la representación de todas las comunidades, incluidas las minorías, en la práctica reduce el porcentaje de votos a alcanzar para que el candidato pueda acceder al segundo turno de las elecciones. Es en esta fase que entra en juego la polarización, a saber, el aumento de la incompatibilidad y de los conflictos entre los corrientes políticos. Como se dijo anteriormente en el desarrollo, es en estas circunstancias, donde prevalece la hostilidad, que los votos "útiles" aumentan para evitar lo peor o simplemente la abstención. De tal manera, las Fake-news aumentarían el ascenso al poder de los candidatos perjudiciales para la

[46] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*
[47] *Ibid.*
[48] GAYA, V. “Clases contra las “fake-news” ¿Son los universitarios analfabetos mediáticos?”. *op.cit.*

democracia. Hay que recordar que, en general, las Fake-news apoyan posiciones o actividades extremas[49].

Sin embargo, hay que atemperar el peligro de la desinformación. Según el estudio realizado por el Politoscopio – un proyecto francés destinado a analizar los usos de Twitter por los políticos – sólo el 0,1% de los mensajes de Twitter contendrían una Fake-news. Además, por lo general se dirigen sólo a comunidades específicas que son, como era de esperar, los partidos políticos "extremistas".[50]

2.3. Regulación actual insuficiente en Francia y España

Los periodistas alertan y estiman que en 2022 – en sólo 3 años – el público consumirá más noticias falsas que información probada[51]. Entonces, ¿cómo explicar que los gobiernos no actúan?

El mayor temor en este ámbito se debe al riesgo de interferir con el derecho a la libertad de expresión. El artículo 10 del Convenio Europeo de Derechos Humanos (llamado el "CEDH" más adelante) establece que "toda persona tiene derecho a la libertad de expresión. Este derecho incluye la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin interferencia de las autoridades públicas y sin tener en cuenta las fronteras"[52]. Además, el Consejo Constitucional reconoció en 1994 que la libertad de expresión es una "libertad fundamental aún más valiosa porque su existencia es una de las garantías esenciales del respeto de otros derechos y libertades".

Sin embargo, hay que recordar que muchos usuarios de las redes sociales han sido víctimas de censura de los debates políticos, debido a algoritmos de recomendación que filtran el contenido al que tienen acceso. Por lo tanto, es difícil decir que las redes sociales promueven fuertemente la democracia tal como la conocemos en nuestras sociedades. De hecho, la desinformación que transmiten en respuesta a su modelo económico perjudica gravemente a la libertad de expresión, que incluye:

- El respeto de la libertad de los medios de comunicación y del pluralismo: si el único objetivo lucrativo de las redes sociales se propagaría, los medios tradicionales ya no

[49] CHAVALARIAS, D. Au-delà des « fake news » : à l'ère numérique, nos démocraties doivent évoluer pour ne pas mourir. *HAL*, 2018.
[50] TORRES DEL CERRO, A. "La lucha contra las "fake news" es un "talón de Aquiles" de las democracias". *El confidencial*, 20 de septiembre de 2018.
[51] GAYA, V. "Clases contra las "fake-news" ¿Son los universitarios analfabetos mediáticos?". *op.cit.*
[52] COMMISSION EUROPEENNE. *Report of the Independent High Level Group on Fake-news and online disinformation* : « a multi-dimensional approach to disinformation ». 2018.

serían libres e independientes como lo son ahora, y las redes sociales se convertirían en los únicos medios de comunicación, lo que perjudicaría directamente al respeto del pluralismo.

- El derecho de los ciudadanos a expresar opiniones y a recibir o comunicar informaciones e ideas: si los medios tradicionales desaparecerían en favor de los algoritmos de recomendación, las opiniones de los ciudadanos serian distorsionadas, especialmente porque estos también incluirían Fake-news.

Así, se ha propuesto una solución técnica: utilizar la inteligencia artificial (llamada "IA" más adelante) para erradicar las Fake-news de las redes sociales. Sin embargo, surge un problema: ¿qué pasaría con los errores de citas, la crítica, la sátira, la parodia, los discursos disidentes u ofensivos, las informaciones y comentarios partidarios[53]? Si la IA no es capaz de diferenciarlos de las Fake-news y eliminaría todo este contenido, esto constituiría claramente un abuso y, por lo tanto, una violación de la libertad de expresión.

En fin, para evitar tal infracción, la Comisión Europea recomienda la lucha contra las Fake-news sólo si se demuestra que la difusión de dicha información es el resultado de una mala fe y de una intención deliberada de dañar[54]. Sin embargo, tal recomendación es inviable en la práctica, en particular debido a su vaguedad conceptual: ¿cómo demostrar la intención de manipular en relación con el comportamiento normal y cómo atribuir el acto de desinformación a un individuo o grupo?

[53] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions. op. cit.*
[54] GIREL, M. « De quoi parle le projet de loi sur les Fake News ? » *AOC media*, 04 juin 2018.

TITULO 2. Propuestas regulatorias para evitar un desbordamiento del fenómeno de Fake-news

Si, a primera vista, parece posible limitar el fenómeno de Fake-news mediante una reglamentación legislativa más adecuada (**Capítulo 1**), la tarea no es tan fácil. De hecho, la noción de Fake-news es difícil de definir. Además, este fenómeno está en constante evolución y, desde su creación relativamente reciente, han surgido prácticas que tienden a manipular aún más la opinión de los votantes: el astroturfing y las noticias falsas dirigidas (**Capítulo 2**).

Capítulo 1. La posible limitación del fenómeno de Fake-news a través de la regulación legislativa y de cambios sociales

A pesar de la voluntad europea de combatir el fenómeno de la Fake-news animando los intentos de regulación en Francia y España (**1.1**), los esfuerzos de estos Estados miembros siguen siendo extremadamente insuficientes, para no decir decepcionantes. Sin embargo, con la llegada del Código de Buenas Prácticas propuesto por la Comisión Europea, algunas redes sociales están tratando de involucrarse en esta lucha que es el combate de todos (**1.2**).

1.1. Impulso europeo e intentos de regulación francesa y española

Ante las numerosas cuestiones planteadas por la insuficiencia de la regulación constitucional y el alcance del fenómeno de Fake-news, la UE ha tomado la iniciativa de crear el proyecto "EUvsDisinfo" que forma parte de la campaña “Task Force East Stratcom”, nacido en 2015, que tiene por objetivo luchar contra la desinformación de los activistas pro-Kemlin[55]. También, ha tomado muchas recomendaciones, la primera listando las mejores prácticas que se deben adoptar para combatir la desinformación:

- Transparencia de las fuentes de información;
- Educación de las personas destinada a enseñarles a leer, pero sobre todo a descifrar e interpretar los medios de comunicación y la información;
- Valorar los usuarios y periodistas, por ejemplo, permitiéndoles debatir y asignarles una "puntuación" de fiabilidad;
- Diversidad y sostenibilidad del ecosistema europeo de medios de información, garantizando varias fuentes de información;

[55] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l’UE renforce son action contre la désinformation ». *op.cit.*

- Investigación y participación de los investigadores en la identificación de fuentes de información poco fiables[56].

Sin embargo, sin la ayuda de las plataformas de redes sociales, la Comisión Europea sola no puede garantizar el buen funcionamiento de estas misiones. Por eso, a finales de 2018, la Comisión Europea adoptó un Código de Buenas Prácticas contra la desinformación. Ya ha sido firmado por las redes sociales más influyentes de Internet, a saber, Facebook, Twitter y Google. No obstante, su alcance sigue siendo limitado, ya que sólo se impone a los signatarios, no a todas las redes sociales. Se presenta como una garantía de fiabilidad y confianza para los usuarios, pero ¿qué sucede con otras redes sociales? De hecho, las redes sociales que son signatarias son objeto de un estrecho seguimiento por parte de la Comisión Europea. Como tal, le deben dar un informe mensual sobre los progresos realizados en la lucha contra el fenómeno de las Fake-news hasta las elecciones europeas de mayo de 2019. El objetivo de estos informes es establecer una evaluación global después de 12 meses[57], que permitirá a la Comisión Europea adoptar diversas medidas, posiblemente reglamentarias, así como proponer directivas anti-desinformación.

Más allá de las medidas tomadas por la UE, los Estados miembros adoptaron también unas normas en contra del fenómeno de Fake-news. Este es el caso de Francia con la adopción de su ley Fake-news. Presentada como un complemento de la Loi sur la liberté de la presse[58] ("Ley sobre la libertad de la prensa" en español) de julio de 1881, tiene como objetivo suprimir la circulación de información falsa, especialmente si perturba el orden público durante una consulta electoral.

Por lo tanto, su alcance es relativamente limitado, ya que impone como condiciones una consecuencia y un marco temporal: se dedica únicamente a las noticias falsas que tienen como consecuencia perjudicar el orden público, así como a las que se inscriben en un contexto electoral. De este modo, parece que la cuestión de la verdad y la calidad de la información sólo se aborda en la superficie y que esta ley está más interesada en la cuestión de la manipulación. Esto explica por qué tres criterios acumulativos presiden la aplicación de la ley Fake-news: el contenido de la información debe ser manifiestamente falso, viral y artificialmente amplificado.

[56] COMMISSION EUROPEENNE. *Final report of the High Level Expert Group on Fake News and Online Disinformation*. 12 mars 2018
[57] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». *op.cit.*
[58] GIREL, M. « De quoi parle le projet de loi sur les Fake News ? ». *op.cit.*

Esto reduce aún más el alcance de esta ley, ya que el hecho de que las noticias falsas se amplifican artificialmente implica que la producción es de naturaleza intencional.

La ley Fake-news ha hecho algunos cambios en el Código Electoral, ya que está dentro de su ámbito de aplicación, y en particular para hacerlo un poco más adaptado al contexto actual. El artículo L163-1 se refiere a las redes sociales como "plataformas en línea" y considera que se tienen, "en vista del interés general unido a la información de los ciudadanos durante las elecciones y la sinceridad de las elecciones", ciertas obligaciones de divulgación siempre y cuando su "actividad supere un umbral de conexiones en el territorio francés" (5 millones de visitantes al mes)[59]. Por lo tanto, deben proporcionar al usuario información justa, clara y transparente sobre la identidad de la persona o moral que le paga la remuneración "a cambio de la promoción de contenidos informativos relacionados con un debate interés público." Si los importes recaudados por la plataforma de redes sociales superan un determinado umbral (100 euros libres de impuestos), éstos deben hacerse públicos. En vista de los umbrales establecidos por el decreto de aplicación de la ley de Fake-news, debe señalarse la voluntad de la legislación francesa de controlar todas las plataformas de redes sociales y los partidos políticos que acuden a estas últimas.

El artículo L163-2 del Código Electoral se centra en el uso abusivo de la desinformación y de las redes sociales por parte de cualquier persona física o moral. La decisión del Consejo Constitucional, del 20 de diciembre de 2018[60], reconoce la conformidad de este artículo, así como de "un procedimiento que puede tener el efecto de parar la difusión de determinados contenidos de información" a la Constitución y a la libertad de expresión.

El artículo L112 del Código Electoral castiga la difusión masiva de noticias falsas con un año de prisión y una multa de 75.000 euros. Es una multa importante, pero debe ser atemperada por varios elementos: más allá de la prisión, la multa es "ridícula" para redes sociales como Facebook; la sanción sólo puede imponerse si el carácter inexacto o engañoso de la información es evidente y el riesgo de alteración de la sinceridad de la votación también debe ser manifiesto. Además del alcance relativamente estrecho de la ley Fake-news y de los artículos modificados del Código Electoral, existen muchas condiciones para sancionar. En fin, la ley Fake-news no es muy eficaz en la erradicación del fenómeno de desinformación. Sin embargo, Francia al menos tiene el mérito de haber legislado en este ámbito, lo que no sucede en España. Hasta

[59] DECRET n° 2019-297 *relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général*, 10 avril 2019.
[60] CONSEIL CONSTITUTIONNEL. *Décision n° 2018-773 DC*, 20 décembre 2018.

ahora, la única medida que España ha tomado es la creación de una "Unidad contra la desinformación".

1.2. Participación de las redes sociales

Las redes sociales son la piedra angular del fenómeno de las noticias falsas: dan a todos la oportunidad de ejercer su derecho a la libertad de expresión, pero sobre todo facilitan la propagación de la desinformación, hasta que la hagan incontrolable. La Comisión Europea adoptó el Código de Buenas Prácticas para combatir la opacidad y la renuencia de las redes sociales a combatir las noticias falsas.

Los primeros informes sobre las medidas adoptadas durante el mes de enero de 2019 emitidos a la Comisión Europea por Facebook, Twitter y Google fueron decepcionantes. En particular, se distinguieron por una gran falta de detalles y no demuestran que las nuevas medidas adoptadas por las tres redes sociales se desplegarían a tiempo y con recursos suficientes. Además, los resultados de las medidas ya adoptadas tampoco fueron objeto de un análisis más detallado[61]. Por lo tanto, cabe señalar que estas tres redes sociales, a pesar de la firma de este Código de Buenas Prácticas, siguen siendo timoratas a la transparencia. Así, el compromiso asumido por estas últimas parece haberlo sido a mitad, o sin ninguna consideración de la meta real.

No obstante, la Comisión Europea, en una de sus declaraciones, apoyó las medidas policiales desarrolladas por estas tres plataformas. De hecho, aunque poco demostrado en sus informes, Facebook, Twitter y Google han adoptado medidas relativas al seguimiento y control de las valuaciones publicitarias, al cierre de cuentas falsas y a sistemas de marcación de cuentas robots. Con respecto a la transparencia de los anuncios políticos, sólo Facebook declaró que había desarrollado e implementado medidas para detectar publicaciones peligrosas y garantizar la transparencia de los anuncios. Google y Twitter han fracasado en este ámbito y esto plantea un verdadero problema, ya que los debates públicos divisivos son propicios a la desinformación.

La Comisión Europea parece ser laxista – o pedagoga – y, además, el Código de Buenas Prácticas no es vinculante para las plataformas de redes sociales que son signatarias. Como tal, Francia ha decidido actuar al mismo tiempo mediante la adopción de su ley Fake-news, la cual es más estricta.

[61] COMMISSION EUROPEENNE. *First monthly intermediate results of the EU Code or Practice against disinformation*. 28 février 2019.

El artículo 11 de esta ley, que complementa el artículo L163-1 del Código Electoral, señala que los "operadores de plataformas en línea", sin distinción, están obligados a tomar "medidas para combatir la difusión de información falsa que pueda perturbar el orden público o alterar la sinceridad de las elecciones". Desafortunadamente, una vez más, este artículo sólo se refiere a las noticias falsas transmitidas en un contexto electoral y no en ningún momento. Entre las medidas que las redes sociales deben adoptar, la ley Fake-news exige que toman medidas que incluyan:

- La transparencia de sus algoritmos, incluidos los de recomendación;
- La promoción de contenidos de empresas y agencias de noticias y servicios de comunicación audiovisual, los cuales son una garantía de fiabilidad;
- La lucha contra las cuentas robots que propagan masivamente información falsa;
- Información de los usuarios sobre la identidad del partido político que les paga a cambio de la promoción de contenidos informativos relacionados con un debate de interés general;
- Información de los usuarios sobre la naturaleza, el origen y los métodos de difusión de contenidos, un punto en el que las redes sociales son particularmente opacas;
- Medios de comunicación y educación sobre la información.

Las redes sociales deberán hacer públicas estas medidas, así como los recursos que les dediquen. Como tal, tendrán que enviar una declaración a la CSA cada año indicando cómo se implementarán. Tratando de la noción de educación a los medios de comunicación para la que la ley que las redes sociales adopten medidas, se plantea una pregunta: ¿realmente depende de las redes sociales hacer esta educación? ¿No es parte de las prerrogativas del Estado? Parece exonerarse de ciertas responsabilidades que son suya delegándola a las plataformas de redes sociales, las cuales, técnicamente, no tienen forma de educar a millones de usuarios.

Al mismo tiempo, debemos señalar la idea particularmente interesante evocada por el artículo 11 de la ley Fake-news, que quiere hacer del usuario de las redes sociales un actor proactivo de la lucha contra las Fake-news. De hecho, menciona que las plataformas en línea tienen la obligación de "poner en marcha un dispositivo de fácil acceso y visible que permita a sus usuarios señalar [las informaciones falsas], especialmente cuando provienen de un contenido publicado en nombre de un tercero". Este párrafo del artículo 11 refleja la idea según la cual las redes sociales, aunque obligadas por la ley a combatir el fenómeno de Fake-news, no son los únicos actores en su difusión, dado que sus usuarios son también los mayores responsables. Por

lo tanto, tal legislación no puede aplicarse de manera sostenible sin una conciencia pública y colectiva, de ahí el interés para el Estado de invertir en la educación de la población.

Capítulo 2. Astroturfing y Fake-news individualizada: hacia una manipulación de la opinión de los votantes

Es a través del matrimonio de todos los avances tecnológicos y los contextos permisivos actuales que han nacido prácticas particularmente peligrosas. El astroturfing, que literalmente usurpa la identidad ciudadana en el espacio público digital (**2.1**) es el primer ejemplo. Sin embargo, no es el único y, cuando el uso de los datos personales se combina con estas evoluciones tecnológicas y lagunas legales, nace las Fake-news individualizidas. Esta peligrosa arma utilizada contra la democracia amenaza seriamente con destruir los principios electorales democráticos (**2.2**).

2.1. Astroturfing o la usurpación de la identidad ciudadana en las redes sociales

El astroturfing, que a primera vista se presenta como una evolución técnica y tecnológica de las Fake-news, no es un concepto tan fácil de definir. De hecho, pretende simular la existencia de un grupo de usuarios de Internet que se unan espontáneamente a una causa para influir en los ciudadanos reales[62]. Las cuentas robots, o "bots", han permitido el surgimiento de esta práctica y es por esta razón que la Comisión Europea hace un punto de honor a que las redes sociales los mencionan o eliminan.

Gracia a técnicas manuales o algorítmicas, pero sobre todo gracias al Big data que se alimenta del Open data, estos bots pueden enviar mensajes dirigidos usuarios elegidos según ciertas características[63]. De esta manera, el astroturfing permite una difusión más rápida de las noticias falsas ya que se dirigen "a las personas adecuadas, en el momento adecuado" para volver a utilizar el eslogan de Cambridge Analytica. Por lo tanto, más que una evolución, el astroturfing es una herramienta de desinformación.

El hecho de que una estrategia tan engañosa, modificando su fuente real y mintiendo sobre su origen, haya nacido refleja perfectamente la falta de regulación en este ámbito. Como tal, el astroturfing, sobre la base de esta comunicación falsa y engañosa en relación con su fuente, hace imposible la auténtica intersubjetividad, que sin embargo es la condición *sine qua non* de

[62] CHAVALARIAS, D. « Fake news : l'arbre qui cache la forêt ». *op.cit.*
[63] BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. *op.cit.*

la comunicación y de una ética de discusión, a su vez guardián de une sana comunicación democrática.

En resumen, existe astroturfing cuando se cumplen las dos siguientes características:

- La fuente de la comunicación se esconde a sabiendas y se ejecuta sin que la persona se entere;
- Aún sin saberlo, el productor del astroturfing se apropia ilegítimamente y estratégicamente la identidad del ciudadano para mejorar la credibilidad de la supuesta fuente y de la información difundida al público objetivo[64].

En conclusión, el astroturfing se aprovecha de todas las tecnologías evocadas (Big data, Open data, algoritmos) así como del contexto legislativo actual casi inexistente y la creciente difusión de Fake-news. De este modo, reúne todas las innovaciones posibles y se presenta como un arma temible para los principios democráticos actuales. Otra práctica, menos aterradora a primera vista pero igualmente peligrosa, es la de las Fake-news individualizadas que ponen en serio peligro la libre voluntad del electorado.

2.2. Hacia la aniquilación de los principios electorales democráticos

La Fake-news individualizada no usurpa de la identidad ciudadana, como lo hace el astroturfing. Solo aprovecha los avances tecnológicos y los progresos en la individualizacion algorítmica para dirigirse a un panel más estrecho de individuos, en lugar de dirigirse a toda la población antes de quedar rápidamente olvidada.

Por lo tanto, que sea astroturfing o Fake-news individualizadas, está claro que ambas prácticas perjudican seriamente al libre albedrio y a la libre elección del votante. Del mismo modo, es un primer paso hacia una intrusión en la intimidad ya que es alimentándose del Big data, y de los datos personales de los usuarios, que tal fenómeno pueda existir. Parece que las revelaciones de Edward Snowden en 2013 sobre el uso de los datos personales detenidos por las plataformas de internet no les impidieron seguir compartiéndolos.

La segmentación se basa en el contenido que busca el individuo, la ubicación del usuario y/o el momento de la navegación. Como tal, los perfiles se pueden elaborar en función de:

- El comportamiento de los usuarios de internet;
- La información proporcionada por los afectados ellos-mismos;

[64] *Ibid.*

- La acción del usuario.

Así, existe dos prácticas. Una es la recopilación “activa” de datos que solo es la recuperación de la información proporcionada por los propios usuarios de internet, a diferencia de la recogida "pasiva" que se lleva a cabo sobre los datos del individuo sin su conocimiento, sin que él pueda consentir. Así es como el usuario de las redes sociales se encuentra atrapado en una situación de confinamiento algorítmico, también llamado "gobernanza algorítmica"[65].

No obstante, el Grupo de Trabajo del artículo 29 formado por la UE (llamado el “GT29” más adelante), aconseja no recopilar los datos personales de manera pasiva a la luz del "grave riesgo de dañar los datos personales si este tipo de información se utiliza con el fin de difundir publicidad comportamental" y recomienda pedir el consentimiento de interesado[66].

En el transcurso de la primera parte de este desarrollo, se señaló que las prácticas de propaganda actuales eran particularmente peligrosas para la democracia. Ya sea libertad de expresión, libertad de comunicación, derecho a la información, libre albedrio que tantos otros, las redes sociales perjudican todos los derechos y son, como tales, una parte verdaderamente integral de nuestra vida cotidiana. Sin embargo, el fenómeno de Fake-news, del astroturfing y de las Fake-news individualizadas representan únicamente la faceta visible del peligro y otras prácticas, en particular basadas en el uso de datos personales, como el micro-targeting son igualmente peligrosas, para no decir que lo son aún más.

[65] DUBOIS, L. et GAULLIER, F. Publicité ciblée en ligne, protection des données à caractère personnel et Eprivacy : un ménage à trois délicat. *Victoires éditions*¸ 2016. LEGICOM, n°56.
[66] *Ibid.*

PARTE 2. Propaganda electoral individualizada: poner en peligro el derecho fundamental a la protección de datos personales a través de su uso político

Al igual que el fenómeno de Fake-news, la propaganda electoral individualizada gracia a los datos personales amenaza con perjudicar nuestros principios democráticos más antiguos y esenciales. Antes de que podamos analizar los intentos de regulación con el fin de proteger los derechos y libertades fundamentales, incluido el derecho a la privacidad, frente al uso de los datos personales con fines políticos e identificar las carencias de esta regulación (**TITULO 2**), debemos materializar los peligros existentes para los principios democráticos franceses y españoles (**TITULO 1**).

TITULO 1. Materialización de los peligros para los principios democráticos franceses y españoles de una propaganda electoral individualizada

El primer peligro que existe cuando la reglamentación nacional es insatisfactoria en el ámbito de la propaganda individualizada es el que pesa directamente sobre el derecho fundamental a la protección de datos personales (**Capítulo 2**)**.** Sin embargo, muchos otros derechos fundamentales están en riesgo frente a esta propaganda individualizada (**Capítulo 1**).

Capítulo 1. Los riesgos actuales de la propaganda individualizada sobre los derechos fundamentales de los electores

La propaganda en sí misma no es un peligro para nuestras democracias, ni para los derechos fundamentales de los votantes. Es cuando se añaden los desarrollos tecnológicos y sus usos mal intencionados que se vuelve peligrosas para nuestros procesos electorales. Así, la propaganda individualizada presenta un primer riesgo significativo de aniquilación del libre albedrio del votante (**1.1**). Del mismo modo, el uso de datos personales con fines políticas es una verdadera intrusión en la vida privada (**1.2**), aunque presente un desafío importante para los jefes de Estados.

1.1. Aniquilación del libre albedrio del votante

Mas allá de la propaganda mediante Fake-news, la propaganda basada en hechos verdaderos pero dirigida es igualmente peligrosa. Cuando las publicaciones políticas en las redes sociales se difunden a un panel estrecho de personas, elegidas según un perfil ideológico elaborado sobre sus datos personales, hablamos del filtro burbuja. Para decirlo más "técnicamente", los bots capaces de automatizar la publicación de contenidos responden a la programación de un conjunto de algoritmos llamados " de recomendaciones"[67].

En este caso, el filtro burbuja y sus algoritmos de recomendaciones proporcionan al usuario una vista del mundo distorsionada[68]. El individuo se encuentra encerrado en un espacio digital conforme a sus prejuicios y que refuerza su sesgo de confirmación[69]. Como tal, las redes sociales refuerzan seriamente el empobrecimiento de la pluralidad de la información – ya perjudicada por el fenómeno de Fake-news – y de la democracia.

El fenómeno de filtro burbuja, ya que reduce *de facto* la información y las opiniones de los votantes, aumenta en gran medida el riesgo de polarización política e ideológica, El peligro que representan las redes sociales para la democracia es, como tal, muy importante. De hecho, el CEO de Facebook, Mark Zuckerberg, fue multado con 45.000.000 dólares por el daño irreparable que causó "al debate democrático y al debate civilizado en el mundo"[70]. Desde entonces, su equipo se ha esforzado por mitigar este fenómeno de filtro burbuja, en vano[71].

De tal manera, el fenómeno de filtro burbuja sigue siendo el muy peligroso ya que internet ha hecho perfectamente incontrolable e impredecible el encuentro de individuos y mensajes. Esto no está exento de consecuencias:

- La información ya no tiene ningún vínculo, excepto el de las intenciones e intereses ideológicos de sus productores;
- Sobre los individuos "fuertes" de la sociedad conectada, los efectos son pequeños, pero *a contrario* para los individuos "débiles" con atención cautiva, los efectos son fuertes[72].

---

[67] TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *op.cit.*
[68] LAUSSON, J. « Facebook pourrait menacer la démocratie, selon un ex-patron des renseignements britanniques ». *Numerama*, 8 décembre 2018.
[69] ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *op.cit.*
[70] *Ibid.*
[71] LAUSSON, J. « Facebook pourrait menacer la démocratie, selon un ex-patron des renseignements britanniques ». *op.cit.*
[72] CARDON, D. « Pourquoi avons-nous si peur des fake-news ? ». *AOC Media*, 20 juin 2019.

En resumen, las redes sociales son vectores de (des)información con alta precisión de individualización[73].

1.2. Aniquilación del derecho a la vida privada del votante

El artículo 12 de la Declaración Universal de los Derechos Humanos (llamada la "DUDH" más adelante) consagra la vida privada como un derecho fundamental. Afirma que "nadie será objeto de interferencias arbitrarias en su vida privada, familiar, en su hogar o en sus correspondencias, ni será objeto de vulneración de su honor o de su reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o infracciones". Del mismo modo, el artículo 8 de la Convención de Salvaguardia de los Derechos Humanos y de las Libertades Fundamentales (llamada la "CSDHLF" más adelente) consagra también este derecho, pero añade que "no puede haber injerencias de una autoridad pública en el ejercicio de ese derecho". En vista de lo que se desarrolló anteriormente, está claro que, irónicamente, la autoridad pública es ahora una de las mayores amenazas a este derecho a la vida privada. De hecho, en el contexto actual de propaganda virtual, los mensajes personalizados e información personalizada basados en intereses personales, estilo de vida, hábitos y valores presentan una grave intrusión en la vida privada y, por lo tanto, un grave riesgo para la confianza y la integridad del proceso democrático[74].

Frente a estos peligros, el derecho a la protección de datos debe intervenir para proteger el derecho a la vida privada. La unión de ambos derechos da la luz al "derecho al olvido", lo cual permite a cualquier persona de pedir la supresión de sus datos personales que detenga una organización. Se presenta como un medio para garantizar la protección de la vida privada, sin embargo, surge una pregunta: ¿es excesiva o indispensable? De hecho, existe en detrimento de la libertad de expresión y del derecho a la información y, por lo tanto, es necesario equilibrar estos dos principios fundamentales con el derecho a la intimidad y la protección de los datos personales, lo que no consiguen hacer los gobiernos. Esto puede explicar la naturaleza obsoleta o inexistente de las regulaciones francesa y española sobre la propaganda individualizada...[75]

[73] COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions*. *op.cit.*
[74]. EUROPEAN DATA PROTECTION BOARD. *Statement 2/2019 on the use of personal data in the course of political campaigns*. 13 mars 2019.
[75] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *op.cit.*

Capítulo 2. La puesta en peligro del derecho fundamental a la vida privada por una regulación nacional obsoleta o inexistente

Del mismo modo que para el fenómeno de Fake-news, las normas constitucionales francesas y españolas son particularmente inadecuadas (**2.1**) al fenómeno de la propaganda individualizada. Si las medidas adoptadas a un nivel menor propuestas por estos dos países fueran más restrictivas, este fenómeno no sería de mucha preocupación. Desgraciadamente, son tan inadecuados como la actual regulación constitucional (**2.2**). Por lo tanto, tal vacío legal y reglamentario no está sin consecuencias (**2.3**) y se puede imaginar que los abusos surgen debido a la libre interpretación que hace posible.

2.1. La inexistencia de la regulación constitucional en Francia y en España

En Francia, más allá de las ya mencionadas normas constitucionales que incorporan vagamente el concepto de red social, no existe ningún artículo, en sentido estricto, directamente interesado en el uso de los datos personales con el fin de llevar a cabo una propaganda individualizada. Esta práctica está regulada únicamente por las leyes de derecho privado, incluyendo la LIL y el RGPD. Una vez más, esto refleja el carácter obsoleto del derecho constitucional francés, pero también las dificultades que se encuentran para adaptarlo.

A contrario, en España, se hizo un intento. Tras la adopción de la LOPD, se incorporó el artículo 58 bis a la LOREG en diciembre de 2018. Este nuevo artículo dice "la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas". Así permite a los partidos políticos utilizar datos personales, incluidos datos sensibles, para hacer propaganda individualizada. Les autoriza a recopilar, de páginas web y otras fuentes de acceso público, "datos personales relativos a las opiniones políticas de las personas en el curso de sus actividades electorales" sobre la base del interés público, a saber, el interés legítimo del responsable de tratamiento. Así, la recopilación y el tratamiento de datos sensibles, aunque están prohibidos en virtud del RGPD, está legitimados durante la campaña electoral y ya no requiere el consentimiento de las personas interesadas[76].

La unica “limitación” establecida en el artículo 58 bis al uso de los datos personales en el contexto de propaganda es muy permisiva, ya que dice que no se considerará comunicación

[76] GALDON CLAVELL, G. “Los partidos quieren tus datos”. *El país*, 24 de marzo de 2019.

comercial y, a este respecto, no estará sujeta a sus normas, a saber, la obligación de transparencia, información y consentimiento[77].

De hecho, ante el gran peligro para los derechos a la vida privada y a la protección de datos que representa este artículo, se hizo un recurso de inconstitucionalidad ante el Defensor del Pueblo. El primer párrafo del artículo 58 bis fue anulado ya que violaba al derecho a la libertad ideológica, así como al derecho a la protección de los datos personales, y a la libertad de expresión y participación política[78]. Sin embargo, no sabemos si su anulación es algo bueno, ya que, por lo tanto, existe un grave vacío jurídico y la falta de regulación sugiere que los partidos políticos pueden cometer nuevos abusos.

2.2. Medidas inadecuadas propuestas por Francia y España

Frente a la naturaleza inexistente u obsoleta de las regulaciones constitucionales francesa y española, se han adoptado medidas de iniciativa "privada", a menor escala. España, por su parte, ofrece varias opciones a sus ciudadanos para oponerse al envío de propaganda electoral, individualizada o no:

- La asociación de los usuarios de internet proporciona una forma de acceso y oposición al tratamiento de los datos personales;
- Los ciudadanos españoles pueden exprimir su deseo de no recibir publicidad política a través de SMS, WhatsApp o redes sociales en general;
- También pueden pedir al Instituto Nacional de Estadística (llamado el "INE" más adelante) que no divulgue sus datos personales a los partidos políticos cuando les facilite los censos;
- Pueden inscribirse en la "Lista viernes"[79].

La opción propuesta por el INE es, por su parte, algo sorprendente. La LOREG establece que los partidos políticos pueden tener acceso a los datos contenidos en el censo electoral, con el fin de llevar a cabo sus campañas institucionales y electorales y enviar un programa político a cada ciudadano español. Como tal, esta opción parece oponerse directamente a la ley orgánica, ya que tendería a limitar el acceso a estos datos a los partidos políticos. El INE también propone otra herramienta para oponerse al envío por correo de propaganda electoral[80]. Esta herramienta

[77] *Ibid.*
[78] "El Constitucional anula la reforma de la ley que permitía a los partidos recopilar datos de votantes". *El Mundo*, 22 de mayo de 2019.
[79] PEREZ-LANZAC, C. "No les pongas el trabajo fácil". *El país*, 24 de marzo de 2019.
[80] GALDON CLAVELL, G. "Los partidos quieren tus datos". *El país*, 24 de marzo de 2019.

fue ciertamente útil en el pasado, pero hoy en día se caracteriza sobre todo por su naturaleza obsoleta. La última opción ofrecida a los españoles complementa esta herramienta ofrecida por el INE. Registrarse en la Liste viernes, que es una lista disponible en Internet, permite a los ciudadanos oponerse a recibir propaganda electoral por teléfono o correo electrónico[81]. Aunque sea más apropiada, esta lista tampoco está interesada en las redes sociales y la propaganda que allí se lleva a cabo.

En resumen, todas las opciones que se ofrecen a los españoles parecen insuficientes o simplemente inviables. Por eso, la AEPD ha estado trabajando en este tema, con el objetivo de proporcionar un marco reglamentario a estas prácticas y abordar el vacío legal existente. Como tal, ha publicado dos circulares, que enumeran las garantías apropiadas y específicas que los partidos deben ofrecer si utilizan datos personales[82], incluidos datos sobre opiniones políticas que son considerados por el RGPD como datos sensibles.

La AEPD considera que sólo los partidos políticos, federaciones o coaliciones que presentan las candidaturas pueden ser responsables del tratamiento. Añade que, en ningún momento los datos recogidos con fines de propaganda política pueden ser compartidos o transferidos a terceros[83]. Aunque el alcance que ofrezca es amplio, la primera pregunta es ¿qué sucede con las empresas privadas que ofrecen servicios a los partidos políticos, como los programas de estrategia electoral? Si bien prohíbe la transferencia de los datos personales a terceros, sólo se interesa en ellos como destinatarios y no como subcontratistas. La AEPD también considera que el tratamiento sólo será lícito durante el período electoral, y sólo puede aplicarse a las actividades de propaganda electoral y a los actos de campaña electoral. Además, el responsable del tratamiento tendrá que determinar las finalidades perseguidas en relación con la actividad electoral[84]. Como tal, impone ciertas restricciones:

- Los partidos tendrán que consultarla 14 semanas antes del inicio de la campaña electoral sobre los datos que desean reunir (3 semanas para las elecciones de 2019): para ello, tendrán que facilitarle un documento en el que se detallen las medidas adoptadas para evaluar el impacto de la recopilación de datos personales y la minimización del riesgo.
- El uso del Big data y de la IA tendrá que ser estrictamente limitado;

[81] *Ibid.*
[82] *Ibid.*
[83] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[84] *Ibid.*

- La prohibición del micro-targeting y de cualquier sistema que tienda a "forzar o desviar la voluntad del votante";
- Los datos personales deben ser destruidos una vez que la campaña electoral haya terminado.

Además de estas restricciones, la AEPD ha prohibido la recopilación de datos para interpretar la opinión política. Sin embargo, es posible recoger los que se expresan públicamente[85]. Por lo tanto, los partidos políticos pueden recoger estas opiniones siempre que se expresen en páginas web y fuentes de acceso público. Por fuentes de acceso público, la AEPD se refiere a aquellas a las que puede acceder cualquier persona. Esto excluye a aquellas cuyo acceso está restringido a un círculo determinado de personas. En el caso de que el responsable del tratamiento desee obtener datos de un tercero, deberá asegurarse de que los datos se obtuvieron legalmente y de que dicho tercero tiene una legitimación específica para la obtención de los datos. Además, debe comprobar que ha informado expresamente a los interesados de las posibles finalidades políticas[86].

Así, la cuestión de por qué las circulares de la AEPD no son objeto de una ley, que se interesaría específicamente en la propaganda electoral individualizada y que sería más restrictiva, así como más disuasoria, sigue sin resolverse. Sin embargo, hay que recordar que este último tiene una capacidad de castigo, aunque muy poco utilizado en la práctica[87]. Por iniciativa propia o a petición de los ciudadanos, puede controlar y, si encuentra un incumplimiento al RGPD y a la LOPD, su sanción puede ascender hasta 20 millones de euros[88].

Por el lado francés, no se han adoptado medidas especiales para limitar la recopilación de datos personales, sensibles o no, con el fin de llevar a cabo propaganda individualizada. Como tal, la CNIL, que ha sido particularmente activa sobre el tema desde 2012, ha formulado varias recomendaciones. De la misma manera que la AEPD, ha impuesto algunas restricciones al responsable del tratamiento. Este último sólo puede ser el partido, la agrupación política, los funcionarios electos o los candidatos a cargos electos, así como cualquier persona o asociación que desarrolle operaciones de comunicación de carácter político[89]. Esta limitación, como en España, no es tan restrictiva y, lo que es aún peor, pretende ser aún más amplia en la medida en

[85] GOMEZ, R-G. "Protección de datos limita el acceso de los partidos a información personal". *El país*, 11 de marzo de 2019.
[86] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[87] GOMEZ, R-G. "Privacidad: Los partidos suspenden en la protección de datos". *El país*, 12 de marzo de 2019.
[88] GOMEZ, R-G. "Protección de datos limita el acceso de los partidos a información personal". *op.cit.*
[89] CNIL. *Déclaration NS34* « Communication politique ». 29 mars 2019.

que permite que "cualquier persona o asociación que desarrolle operaciones de comunicación política" sea responsable del tratamiento. Por lo tanto, se puede imaginar que las empresas privadas, como las que desarrollan programas de estrategia electoral, serán consideradas como responsables del tratamiento. Esta es excesivamente permisiva y permite que muchos sean considerados como responsables del tratamiento.

Con respecto al programa de estrategia electoral, la CNIL consideró que la recopilación masiva de datos de las redes sociales no es legal a falta de información de las personas interesadas que, en particular, serán informadas de la existencia del derecho de oposición. Además, añade que el uso de las redes sociales no debe llevar a los responsables del tratamiento a atribuir opiniones políticas a los usuarios de internet. Al igual que la AEPD, esto significa que la opinión política no puede deducirse de un conjunto de datos personales[90]. De hecho, la CNIL considera que los datos personales que muestran, directa o indirectamente, la opinión política real o supuesta de un individuo están excluidos de los datos que pueden ser utilizados por los partidos políticos en el contexto de su propaganda electoral individualizada. Sin embargo, permite a estos partidos recopilar estos datos confidenciales si:

- El procesamiento se limita a los datos sensibles correspondientes a la actividad del responsable del tratamiento;
- El tratamiento sólo se aplica a los miembros del partido o de la asociación, así como a los "contactos regulares", es decir, aquellos que han dado un paso positivo hacia el establecimiento de relaciones regulares con el partido y su acción política;
- Los datos no están transferidos a terceros, excepto cuando la persona haya expresamente consentido[91].

La primera limitación es, en este caso, totalmente innecesaria ya que las opiniones políticas son necesariamente vinculadas a la actividad del "partido, agrupación política, funcionarios electos o candidatos para cargos electivos y de cualquier persona o asociación que desarrolle operaciones de comunicaciones políticas". La segunda limitación plantea más cuestiones, en particular con respecto a los "contactos regulares". Aunque la CNIL especifica que se trata de aquellos que han dado un paso positivo hacia el establecimiento de relaciones regulares con el partido político, la definición pretende ser imprecisa, ya que no detalla cuándo se considera que existe un enfoque positivo o no.

[90] CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». 2018.
[91] *Ibid.*

De hecho, en sus recomendaciones de 2016 (no actualizadas desde entonces, así que se puede suponer que siguen siendo aplicables al contexto actual), la CNIL diferencia entre contactos regulares y ocasionales. Considera que los contactos regulares son "amigos" (para Facebook) o "seguidores" (para Twitter) y que los contactos ocasionales son aquellos a los que les gustan, comentan, comparten o “retwitean” publicaciones[92].

En cuanto a los contactos ocasionales, pueden convertirse en contactos regulares y este es el principal objetivo de los partidos políticos. Su información de contacto se puede utilizar por primera vez para ofrecerles contacto regular. Si el individuo está de acuerdo, se convierte en un contacto regular de los responsables del tratamiento. Si se niega o no responde, estos datos tendrán que ser eliminados. No obstante, la CNIL recuerda que la aceptación o la denegación no pueden utilizarse para inferir una sensibilidad u orientación política real o supuesta[93].

También, la CNIL ha creado desde 2012 un observatorio electoral con varias misiones:

- Informar a los votantes de sus derechos "Informática y Libertades";
- Reaccionar rápidamente a los vacíos de la LIL y llevar a cabo controles (también ha puesto a disposición de los votantes un formulario para que puedan reportar posibles violaciones);
- Acompañar a los partidos y candidatos en la implementación de su comunicación política de acuerdo con la LIL (lo que hizo, por ejemplo, Emmanuel Macron, el actual presidente francés)[94].

De hecho, los débiles esfuerzos actuales de las autoridades estatales para luchar contra el uso de los datos personales pueden eludirse mediante el uso de referenciales y bases de datos constituidas al vuelo. Con la creciente profesionalización de las prácticas digitales, estas tendencias se multiplicarán a corto plazo[95].

2.3. Los riesgos que plantea la falta de regulación

Este vacío legal derivado de la insuficiencia de la normativas francesa y española, así como de las medidas adoptadas, no está sin consecuencias. De hecho, los donantes de los partidos políticos se convierten en una base de datos de activistas comprometidos que puede ser utilizada: se consideran como contactos regulares[96]. La simple donación vale el

[92] CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». *op.cit.*
[93] CNIL. « Election 2016/2017 : quelles règles doivent respecter les candidats et partis ? ». *op.cit.*
[94] *Ibid.*
[95] DOSQUET, F. (dir.). *Marketing politique et communication politique. op.cit.*
[96] BILLE, J. Marketing politique et Big Data. *op.cit.*

consentimiento, consentimiento que normalmente es obligatorio para ser parte de la lista de comunicación política de un partido[97]. Esto se opone directamente a la idea de que cualquier afinidad con un partido político no puede inferirse cuando un contacto ocasional acepta o se niega a convertirse en un contacto regular. Al final, es la expresión más reveladora de los peligros de la inseguridad jurídica.

Además, es posible el uso de los censos para llevar a cabo una propaganda política, como ya se había enseñado gracia a la herramienta propuesta por el INE que permite oponerse al uso de los datos personales contenidos en estos censos. Esto tiene sentido ya que el acceso a estos últimos es libre y que los partidos políticos no tienen prohibido seleccionar en estas listas para "dirigirse a una categoría particular de votantes". Así aparece el fenómeno del micro-targeting.

Además, la hipótesis de la " revitalización de los abstencionistas" se está convirtiendo en una práctica común. De hecho, parece ser más eficaz “movilizar a los votantes de su propio campo arriesgando de abstenerse que tratar de convencer a los indecisos o a los votantes del campo adverso". Esto puede ser sólo el comienzo del micro-targeting pero ya es muy preocupante...

[97] CNIL. « Les fichiers constitués dans le cadre des primaires ouvertes ». *op.cit.*

TITULO 2. Intentos de regulación con fin de proteger el derecho fundamental a la vida privada

Sin proporcionar una regulación satisfactoria en la protección de datos personales, parece difícil combatir fenómenos que tienden a perjudicar directamente el derecho fundamental a la intimidad: este es el caso de la micro-targeting y del perfilado (**Capítulo 2**). Por lo tanto, es necesario prestar más atención a la regulación proporcionada por el RGPD y a la protección que ofrece a los datos relativos a las opiniones políticas (**Capítulo 1**).

Capítulo 1. La regulación proporcionada por el RGPD y la protección especial ofrecida a los datos políticos

Ante los muchos riesgos que la propaganda individualizada plantea para los derechos de intimidad y de vida privada, el derecho a la protección de datos es a primera vista un garante del respeto de estos últimos. Cuando se adoptó, el RGPD se presentó como la norma más adecuada para proteger estos derechos fundamentales y permitir el ejercicio efectivo del derecho a la intimidad. En general, tiene como objetivo proteger los datos personales a la hora de recopilarlos y tratarlos (**1.1**). Más concretamente, está interesado en los datos sensibles y, como tal, proporciona protección específica para los datos relativos a opiniones políticas (**1.2**).

1.1. La protección proporcionada por el RGPD al recopilar y tratar datos personales

Para proteger los datos personales, la UE adoptó el RGPD en 2016. Como ya se ha señalado, su objetivo era proporcionar un marco de protección para los datos personales de las personas y armonizar la legislación de los Estados miembros en este ámbito. Si se ha cumplido su misión de armonización, no es cierto por lo de proponer un marco suficiente para la protección de los datos personales.

No obstante, debe reconocerse que el derecho a la información, que planteaba muchas cuestiones anteriormente, se ha visto reforzado por el RGPD. Este último lo elevó entonces como uno de sus "pilares" y añadió la noción del derecho a la comprensión. Este último derecho implica que la información se adapta a todos, con el fin de garantizar que sea entendida por cualquier individuo. Por lo tanto, debe entregarse de forma concisa, transparente, inteligible y de fácil acceso, en un lenguaje sencillo. Si esto es imposible o requiere un esfuerzo desproporcionado, la información debe ser facilitada por un formulario electrónico en el sitio

web del responsable del tratamiento, en las redes sociales o cualquier servicio equivalente[98]. Sin embargo, surge la cuestión de cómo implementar técnicamente este derecho a la información y la comprensión en una red social[99].

También, la información debe facilitarse siempre que los datos recopilados se utilicen para un fin distinto al inicialmente perseguido. En el caso de la propaganda individualizada, esto no debería suceder ya que la CNIL y la AEPD exigen que estos datos sean recogidos y tratados únicamente con el fin de llevar a cabo actividades de propaganda electoral y comunicación política.

Sin embargo, los derechos a la información y a la comprensión no son los únicos principios expuestos por el RGPD. Debe responder a los principios de legalidad, lealtad y transparencia, de finalidad determinada, explícita y legítima, de minimizar los datos recopilados, de datos precisos y actualizados y de duración de conservación limitada. Esta última se limita a la del proceso electoral: los datos nunca se pueden conservar indefinidamente, excepto en raras excepciones, incluyendo una en la que los datos personales se anonimizan para convirtirse en datos estadísticos.

En cuanto al principio de finalidad determinada, explícita y legítima, la CNIL y la AEPD afirman que la base de datos constituida con finalidad de comunicación política no puede utilizarse para otras finalidades[100]. Sin embargo, el RGPD sólo especifica que los datos no pueden ser tratados en una fecha posterior si la finalidad es incompatible con la definida al principio. En estos términos, no hay nada que impida al partido político de tratar los datos personales en una fecha posterior si define una nueva finalidad similar a la de la comunicación política. El artículo 6.4 del RGPD también considera que "el responsable del tratamiento, para determinar si la nueva finalidad es compatible con la finalidad para la que se recopilaron originalmente los datos personales, tiene en cuenta (...) la posible relación entre los fines para los que se recopilaron los datos personales y las finalidades del tratamiento posterior previsto". Por lo tanto, en este caso, el partido podría conservar los datos y es difícil saber si estaría obligado a informar el interesado.

La CNIL y la AEPD también establecen que sólo se pueden recopilar y tratar los datos relevantes y necesarios en relación con la finalidad prevista, y esto bajo el principio de

[98] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[99] MALLET-POUJOL, N. Protection des données personnelles et droit à l'information. *Victoire éditions*, 2016. LEGICOM, n°56.
[100] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*

minimización de los datos[101]. El problema con la propaganda individualizada es que todos los datos pueden parecer estrictamente relevantes y necesarios para los partidos políticos y los candidatos. Un corolario a este principio de minimización es que estos datos sólo deben estar accesibles a personas autorizadas. Sin embargo, de acuerdo con la CNIL y la AEPD, el panel de personas que tienen acceso a estos datos es verdaderamente amplio, lo que no tiende a protegerlos.

1.2. La protección específica proporcionada por el RGPD a los datos de opinión política

El RGPD distingue entre los datos personales "clásicos" y los llamados datos personales sensibles. El artículo 9 del RGPD los enumera e incluye las opiniones políticas. Si bien los datos personales "clásicos" son de gran interés, las opiniones políticas son una meta real para los candidatos y los partidos políticos. Obtenerlas les permite llevar a cabo una propaganda electoral individualizada de gran eficiencia y es por esta razón, así como para la intrusión en la vida privada de las personas, que están sujetas a una mayor protección por parte del RGPD.

En Francia, los datos sobre opiniones políticas no están comprendidos en el ámbito de la prohibición del tratamiento, siempre y cuando sean sujetos, a corto plazo, a un proceso de anonimización previamente reconocido de conformidad con las disposiciones de la LIL por la CNIL[102]. Del mismo modo, las informaciones sobre la participación o abstención de votantes, cuando se recopilan como parte de un estudio conducto por el INSEE; así como informaciones sobre actividades públicas, comportamientos y viajes, blogs y redes sociales, en relación con los grupos de aficionados incluidos en el archivo STADE.

Con respecto a las opiniones políticas que siguen siendo consideradas como datos sensibles, el artículo 9 del RGPD prohíbe su tratamiento. Sin embargo, este Reglamento no está sin cierta flexibilidad. Por lo tanto, establece que, en algunas excepciones, el tratamiento de estos datos es posible:

- El tratamiento se lleva a cabo, como parte de sus actividades legítimas y con las garantías adecuadas, por una fundación, asociación u otra organización sin fines de lucro y persiguiendo una finalidad política (...), siempre que dicho tratamiento se refiere exclusivamente a miembros o ex miembros de esa organización o a personas que tienen contactos regulares con ella;

[101] *Ibid.*
[102] BENEZETH, B., DELLEVOY, V., FAVERO, E., GHANTY, A., TAMBA, J. et VILLEDIEU, A-L. *Protection des données personnelles*. Paris : Francis Lefebvre, 2018. 297 p.

- El tratamiento implica datos personales hechos públicos por el interesado;
- El tratamiento es necesario por motivos de interés público, sobre la base del derecho de la UE o de los Estados miembros que debe ser proporcional al objetivo, respetar la esencia del derecho a la protección de datos y proporcionar medidas adecuadas y salvaguardar los derechos e intereses fundamentales del interesado.

No se citan todas las excepciones previstas por el RGPD, sólo las que la CNIL y la AEPD reciben en el caso de la recopilación y tratamiento de datos relativos a opiniones políticas con el fin de llevar a cabo una propaganda electoral. Del mismo modo, afirman que, cuando la excepción es la de motivos de interés público, deben haber autorizado este tratamiento de antemano[103]. De hecho, las autoridades de control francesas y españolas aceptan esta excepción como base jurídica para el tratamiento de opiniones políticas, siempre y cuando los partidos políticos propongan medidas para proteger los intereses y derechos fundamentales de los afectados. Como tal, la AEPD recomienda el uso de procesos de seudonimización, agregación o anonimización[104]. No obstante, el fundamento y las limitaciones de la excepción de interés público siguen por determinarse con precisión, y la vaguedad actual da lugar a muchos abusos.

Ante esas excepciones, ¿siguen siendo protegido los datos sensibles? Una vez más, el RGPD no parece cumplir su misión. Las excepciones que proporciona son demasiado numerosas y muy laxistas, como el interés público o el interés legítimo. La directiva de 1995, derogada por el RGPD, fue quizás más protectora, ya que sólo preveía eludir la prohibición del tratamiento de datos sensibles en los casos previstos por la ley y necesarios en una sociedad democrática[105]. La propaganda política individualizada no parece particularmente necesaria en una sociedad democrática, en cualquier caso, no fue hasta que los medios técnicos lo permitieron.

Para superar esta insuficiencia, la CNIL y la AEPD garantizan de manera particularmente estricta el derecho de oposición del votante. Este derecho, que existe para cualquier persona que es objeto de un tratamiento de sus datos personales, es definido por la CNIL como la posibilidad de que cualquier persona física se oponga al uso de sus datos personales con el fin de publicidad comercial. Aunque la propaganda política no esté sometida a las reglas de esta publicidad comercial, las autoridades de control francesa y española han hecho un honor garantizar este derecho a los votantes. A pesar de que su primer párrafo haya sido declarado

[103] CNIL. *Définition* : « Donnée sensible ».
[104] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[105] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *op.cit.*

inconstitucional, el artículo 58 bis de la LOREG consagraba estrictamente este derecho al exigir a los partidos políticos que garantizaran su ejercicio sencillo y libre[106]. La AEPD, por su parte, ha recordado estos criterios de simplicidad y gratuidad[107]. La CNIL, en lugar de ello, añadió que el derecho de oposición podía ejercerse incluso si los datos procedían de fuentes abiertas como internet, aunque no se hubieran recogidos directamente al interesado e incluso hubiera el mismo hecho públicos sus datos.

El hecho de que la propaganda electoral cumpla con los requisitos de la publicidad comercial por el ejercicio del derecho de oposición es una ventaja real para los votantes: no necesitan justificar las razones del ejercicio de ese derecho y el partido deberá transmitir la oposición al tratamiento a los demás partidos si existe una base de datos común a varios candidatos[108]. Sin embargo, el plazo de un mes parece particularmente largo con respecto a la propaganda política. La LOREG, por ejemplo, establece en su artículo 51 que la campaña electoral dura 15 días. Como tal, el período de un mes permite a los partidos políticos y candidatos tratar los datos y hacer propaganda individualizada antes de tener que responder al ejercicio de tal derecho . Como tal, el derecho a limitar el tratamiento, que permite "congelar" temporalmente el uso de los datos personales durante este plazo de un mes, parece ser una buena opción para el interesado. En este sentido, la AEPD exige a los partidos políticos y candidatos que faciliten, de manera gratuita, el ejercicio del derecho de acceso, rectificación, supresión y limitación del tratamiento de la misma manera que por el derecho de oposición[109].

[106] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[107] CNIL. *Délibération n°2014-041*, 29 janvier 2014.
[108] CNIL. « La communication politique par courrier électronique ». 13 mai 2019.
[109] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*

Capítulo 2. Perfilado y micro-targeting: hacia una intrusión en la vida privada de los votantes

La propaganda individualizada toma su forma más avanzada tan pronto cuando se adapta a las necesidades y deseos de los votantes. Se llama el micro-targeting, una práctica particularmente exitosa de propaganda individualizada, que queda prohibida para proteger el derecho a la vida privada (**2.1**). Contra todo pronóstico, no ocurre lo mismo con el perfilado, lo cual también pone en peligro el derecho fundamental suscitado (**2.2**).

2.1. Prohibición del micro-targeting para proteger el derecho a la vida privada

La propaganda individualizada, en su aspecto más avanzado, pone en peligro muchos derechos y libertades, que van mucho más allá del derecho a la vida privada por sí sola. Esto explica sin duda por qué la referencia al derecho a la vida privada es menos explícita en el RGPD. A diferencia de la directiva de 1995, el derecho a la intimidad no se protege por separado a los otros derechos y libertades fundamentales. El objetivo del RGPD ya no es la protección de "los derechos y libertades fundamentales de las personas y, en particular, de la intimidad", sino "la protección de las libertades y derechos fundamentales de las personas y, en particular, su derecho a la protección de los datos personales". Este nuevo enfoque más amplio de los derechos y libertades fundamentales, al honrar el derecho a la protección de los datos personales, tiene sentido ya que este último es el garante de todos los demás derechos: la práctica de micro-targeting no puede existir si los partidos políticos y los candidatos no tienen la oportunidad de tratar los datos personales como consideren oportuno[110].

Sin embargo, la UE está dando la alarma – sin ofrecer soluciones reales– y considera que el micro-targeting está cambiando las normas del discurso político, reduciendo el espacio para el debate y el intercambio de ideas. Vuelve al fenómeno de filtro burbuja que encierra el votante en sus concepciones personales del mundo y sus prejuicios, y que tiende a hacer imposibles las discusiones entre individuos. Por esta razón, es urgente iniciar un debate democrático sobre el uso y la explotación de datos para la organización de campañas electorales y la toma de decisiones políticas[111]. Las autoridades de control francesa y española ya han tratado de regular la propaganda individualizada, siempre insatisfactoriamente. El problema puede estar en el caso

[110] CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *op.cit.*
[111] SUPERVISOR EUROPEO DE PROTECCION DE DATOS. *Dictamen 3/2018. op.cit.*

de que las medidas adoptadas siempre se hayan tomado de una manera totalmente unilateral y nunca se hayan discutido con los ciudadanos franceses y españoles.

El gran problema con el micro-targeting es que se basa en una decisión automatizada: se envía un mensaje a este individuo porque, según el algoritmo, cumple con los criterios de su programación matemática. Se debe recordar que los algoritmos no son neutrales, sino leales, y que a menudo hay sesgos algorítmicos que son, precisamente, errores debidos a la entrada humana. Sin embargo, algunos autores están convencidos de que estos cálculos matemáticos pueden proteger la democracia. Permitiría hacer frente a los cambios de panorama de los distritos electorales, que ciertamente es imposible para España pero que podría serlo para Francia, y evitar una ventaja política a ciertos partidos. Las matemáticas podrían proteger la democracia de este fraude, gracias en particular a los algoritmos de muestreo estadístico[112].

Por ahora, La UE sigue prohibiendo estrictamente esta práctica y está seguida por las autoridades de control francesa y española. Al principio, prohíbe el tratamiento masivo de datos y el uso de la IA porque puede conducir a cambios en la ideología política de una persona. *A priori*, no es tanto el derecho a la intimidad que le preocupa, si no más la libertad de opinión y la expresión de esta opinión: la manipulación del votante la preocupa y, como tal, el Comité Europeo de Protección de Datos (llamado "CEDP" más adelante) prohíbe a los partes la micro personalización de sus mensajes[113].

La AEPD añade que la actividad de tratamiento del partido político debe ser proporcional al objetivo perseguido, a saber, llevar a cabo su campaña electoral y convencer a los votantes. Desde su punto de vista, el micro-targeting no es un tratamiento proporcional, ni tampoco lo son aquellos que pretenden forzar o desviar la voluntad del votante. Considera que es contrario a los principios de transparencia y de libre participación, que son las piedras angulares de un sistema democrático[114]. En resumen, los individuos tienen derecho a no ser objeto de una decisión basada únicamente en un proceso automático que produzca efectos en ella: el micro-targeting entra en esta categoría siempre y cuando afecte circunstancias, comportamiento o elecciones de individuos, o si tiene un impacto prolongado o permanente en el individuo.[115]

[112] JOSE MARIN, J. y RUIZ GUEVERA, P. "Matemáticas para proteger la democracia". *El país*, 19 de diciembre de 2018.
[113] GALDON CLAVELL, G. "Los partidos quieren tus datos". *op.cit.*
[114] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019. op.cit.*
[115] COMMISSION EUROPEENNE. *Commission guidance* : « The application of Union data protection law in the electoral context ». *op.cit.*

Hay que recordar que las decisiones algorítmicas son procedurales y no sustanciales, no tienen acceso semántico a la información que manipulan y aprenden de los sesgos. Como tal, estas últimas deben cumplir varias reglas:

- Transparencia: sus cálculos deben ser verificados por los seres humanos;
- Lealtad: los servicios deben explicar al usuario las prioridades que presiden las decisiones de sus algoritmos y que los intereses ocultos, las distorsiones clandestinas o los favoritismos ocultos pueden verificarse de forma independiente.

Por lo tanto, si el efecto del algoritmo es anticipado por la plataforma, pero no es identificable por el usuario, hay deslealtad y entonces manipulación. Sin embargo, la vigilancia debe ejercerse más en los datos que en los algoritmos porque es en este último donde hay defectos[116].

2.2. La puesta en peligro del derecho a la vida privada a través de la elaboración de perfiles

Todo lo que la CNIL y la AEPD se esfuerzan por prohibir es finalmente permitido por otro estándar. Este es el caso, en particular, de las opiniones deducidas por un conjunto de datos personales y la elaboración de perfiles que necesariamente resultan de los mismos. El artículo 22 del RGPD les permite, no sin algunas restricciones.

La AEPD distingue el micro-targeting del perfilado. Sólo acepta la elaboración de perfiles generales y de categorías genéricas de las que es posible deducir conductas generales de la población agregada[117]. En resumen, la elaboración de perfiles se limita a una descripción general del individuo. En comparación, el micro-targeting se define como el cruzamiento de datos personales para determinar perfiles psicológicos individuales precisos y para dirigirse a los votantes[118]. Por lo tanto, la diferencia entre los dos conceptos se limita a una percepción completamente subjetiva de la inexactitud o precisión de ambos. Esto hace que sea particularmente difícil distinguirlos porque, de un individuo a otro, de una autoridad de control a otra, se permitirá o condenará una práctica.

Así, las autoridades de control francesa y española se están alejando de esta distinción coja. Por lo tanto, la CNIL se centra en el control del cruzamiento de los datos personales, lo que no parece ser malo ya que el problema se resuelve en su origen. El problema planteado por el programa de estrategia electoral es, por supuesto, la individualización de los votantes, pero sobre todo las consecuencias prácticas que pueden resultar de su presencia en estas bases de

[116] CARDON, D. Le pouvoir des algorithmes. *Le Seuil*, 2018. Pouvoirs, n°164.
[117] AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019*. *op.cit.*
[118] CHAVALARIAS, D. « Fake news : l'arbre qui cache la forêt ». *op.cit.*

datos. Estos últimos permiten que muchas categorías de información de una variedad de fuentes sean tratadas:

- Información de perfil distinta de los datos de contacto por sí solos;
- Datos de navegación recopilados a través de cookies;
- Datos transmitidos por terceros y recogidos en un contexto no relacionado con la propaganda política.

La CNIL considera que la combinación de datos personales de los usuarios de una red social, a falta de herramientas de control suficientes a su disposición y la posibilidad de oponerse a la elaboración de perfiles, nunca puede basarse en el único interés legítimo de la persona encargada del tratamiento, ya que no existe un equilibrio adecuado con los derechos y libertades de las personas afectadas: en este sentido, el consentimiento de los usuarios de internet es indispensable. En ausencia de consentimiento, sólo las acciones dirigidas, a nivel de distrito, barrio o calle, se pueden hacer sobre la base de los datos procesados por este programa, no acciones personalizadas, como este es el caso del micro-targeting[119]. En resumen, la CNIL resume las condiciones para el cruzamiento de los datos personales de las personas:

- El individuo debe ser informado en cada recopilación de datos en su perfil de red social;
- Debe obtenerse su consentimiento en cuanto a las condiciones de plena aplicación del tratamiento de los datos así agregados.

También, el cruzamiento de datos personales sólo puede referirse a los contactos regulares. De hecho, las condiciones de información y la recopilación de consentimiento difícilmente pueden difícilmente cumplirse para el contacto ocasional. Así, en Francia, dado que los interesados deben haber consentido para que los partidos puedan utilizar bases de datos comerciales, el desarrollo de perfiles obtenidos mediante el cruzamiento de múltiples datos se convierte finalmente en un complejo viaje al respecto de la vigilancia ejercida por la CNIL[120].

[119] CNIL. « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ». *op.cit.*
[120] *Ibid.*

CONCLUSIONES

Más allá de todas las críticas que se han formulado en este estudio, con respecto a la regulacion actual, tanta europea como nacional, cabe señalar que tanto las autoridades públicas como las empresas privadas están realizando esfuerzos, y incluyendo aquellos que hacen que las plataformas de redes sociales existan. De hecho, la UE ha elogiado los esfuerzos realizados por Facebook, Twitter y Google en la lucha contra las Fake-news. Una participación récord se registró en las elecciones del Parlamento europeo de 2019.

Gracia a las redes sociales suscitadas, la UE ha reforzado su capacidad a identificar y combatir la desinformación, incluso a través del sistema de alerta rápida que ha creado, la cual ha demostrado ser particularmente eficaz. Además, el Código de Buenas Prácticas, aunque no es vinculante, ha aumentado la conciencia de la sociedad sobre el fenómeno de Fake-news y su resiliencia ante él[121].

Por el lado de la propaganda individualizada, quedan muchos esfuerzos por hacer: la regulación debe ser más estricta y precisa, tanto por parte de la UE como por parte de los Estados miembros. Sin embargo, ha habido un aumento de la conciencia de los ciudadanos europeos, ya que las reacciones a la entrada en vigor del artículo 58 bis de la LOREG han sido contundentes. Este último fue declarado parcialmente inconstitucional.

En conclusión, la legislación sigue haciendo lo que siempre ha hecho, a saber, actuar después de que ya se haya producido el cambio social...

[121] COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE fait rapport sur les progrès réalisés dans la lutte contre la désinformation en vue du Conseil européen ». 14 juin 2019.

BIBLIOGRAFIA

Obras

BENEZETH, B., DELLEVOY, V., FAVERO, E., GHANTY, A., TAMBA, J. et VILLEDIEU, A-L. *Protection des données personnelles*. Paris : Francis Lefebvre, 2018. 297 p.

BERNAYS, E. *Propaganda : comment manipuler l'opinion en démocratie*. New York : Zones, 1928. 144 p.

BRAUD, P. *La science politique*. 11ème édition. Paris : Que sais-je, 2017. 128 p.

CHOMSKY N. et HERMAN, E. *Manufacturing consent : the political economy of the mass media*. New York : Pantheon Books, 1988.

DOSQUET, F. (dir.). *Marketing politique et communication politique*. 2ème édition. Paris : EMS Management et Société, 2017. 302 p.

RIUTORT, P. *Sociologie de la communication politique*. Paris : La Découverte, collection « Repères », 2007, 121 p.

Artículos de revistas

BERGUIG, M. et COUPEZ, F. Faut-il réellement craindre l'open data pour la protection de nos données personnelles ? *Victoires éditions*, 2016. LEGICOM, n°56.

BILLE, J. Marketing politique et Big Data. *Commentaire SA*, 2015. Commentaire, n°150.

BOTCHORICHVILI, N. Transferts de données personnelles hors de l'Union Européenne : quelles nouveautés avec la RGPD ? *Victoires éditions*, 2016. LEGICOM, n°56.

CARDON, D. Le pouvoir des algorithmes. *Le Seuil*, 2018. Pouvoirs, n°164.

CHAVALARIAS, D. Au-delà des « fake news » : à l'ère numérique, nos démocraties doivent évoluer pour ne pas mourir. *HAL*, 2018.

CLEMENT-FONTAINE, M. L'union du droit à la protection des données à caractère personnel et du droit à la vie privée. *Victoires éditions*, 2016. LEGICOM, n°56.

DUBOIS, L. et GAULLIER, F. Publicité ciblée en ligne, protection des données à caractère personnel et Eprivacy : un ménage à trois délicat. *Victoires éditions*¸ 2016. LEGICOM, n°56.

DUDEZERT, A. et KAROUI, M. Capital social et enjeux de pouvoir : une perspective socio-politique de l'appropriation d'une technologie de réseaux sociaux au sein d'une collectivité territoriale. *Systèmes d'information et management*, 2012. Volume 17.

ENGUIX OLIVER, S. Impacto político e informativo de las redes sociales: esferas de actuación y comparación con los medios. *Análisis.* Quaderns de Comunicacio i Cultura, n°56.

JAYSON, H. (trad : RICHET, I.). Un guide critique des fake-news : de la comédie à la tragédie. *Le Seuil*, 2018. Pouvoirs, n°164.

KRZATALA-JAWORSKA, E. Internet : complément ou alternative à la démocratie représentative ? *Boeck Supérieur*, 2012. Participations, n°2.

LEHMANS, A. Les réinventions de la démocratie à l'aune de l'ouverture des données : du discours de la participation aux contraintes de la gouvernance. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

LOBO, S. Como influyen las redes sociales en las elecciones. *Nueva Sociedad*, 2017. n°269.

MALLET-POUJOL, N. Protection des données personnelles et droit à l'information. *Victoire éditions*, 2016. LEGICOM, n°56.

MERCANTI-GUERIN, M. Facebook, un nouvel outil de campagne : analyse des réseaux sociaux et marketing politique. *Direction et Gestion*, 2010. La Revue des Sciences de Gestion, n°242.

NICKERSON, D-W. and ROGERS, T. Political campaigns and Big Data. *Journal of Economic Perspectives, 2014*. Volume 28, n°2.

PIEDRA CARDOSO, J. Democracia y redes sociales. *Universidad Verdad*, 2017. 1(72).

THEVIOT, A. Une économie de la promesse : mythes et croyances pour vendre du Big Data électoral. *GRESEC*, 2018. Les enjeux de l'information et de la communication, n°19/2.

TROUDE-CHASTENET, P. Fake news et post-vérité : de l'extension de la propagande au Royaume-Uni, aux Etats-Unis et en France. *Quaderni*, 2018. N°96.

Artículos de prensa

ABELLAN, L. "El Gobierno activa una unidad contra la desinformación ante las elecciones". *El país*, 11 de marzo de 2019.

CARDON, D. « Pourquoi avons-nous si peur des fake-news ? ». *AOC Media*, 20 juin 2019.

CHAVALARIAS, D. « Fake news : l'arbre qui cache la forêt ». *AOC media*, 7 novembre 2018.

DARMANIN, J., FERRAN, B. et RONFAUT L. « Minute par minute, le récit de la nuit de 13 novembre sur les réseaux sociaux ». *Le Figaro*, 25 novembre 2015.

DEL CASTILLO, C. y SARABIA, D. "Aprobada la ley que permitirá a los partidos hacer spam electoral y propaganda personalizada en internet". *El diario*, 21 de noviembre de 2018.

DE MIGUEL, B. "La UE señala a Rusia como la mayor amenaza de interferencia para las elecciones europeas de Mayo". *El país*, 20 de febrero de 2019.

"El Constitucional anula la reforma de la ley que permitía a los partidos recopilar datos de votantes". *El Mundo*, 22 de mayo de 2019.

« Elections : à la fête du client ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c'est terminé, N°149.

« Elysée : des données pas données ». *Les dossiers du canard enchainé*, octobre 2018. #Vie privée, c'est terminé, N°149.

"Fake news: contra las falsedades". *El país*, 12 de marzo de 2019.

GALDON CLAVELL, G. "Los partidos quieren tus datos". *El país*, 24 de marzo de 2019.

GAYA, V. "Clases contra las "fake-news" ¿Son los universitarios analfabetos mediáticos?". *El mundo*, 10 de abril de 2019.

GIREL, M. « De quoi parle le projet de loi sur les Fake News ? » *AOC media*, 04 juin 2018.

GOMEZ, R-G. "Privacidad: Los partidos suspenden en la protección de datos". *El país*, 12 de marzo de 2019.

GOMEZ, R-G. "Protección de Datos limita el acceso de los partidos a información personal". *El país*, 11 de marzo de 2019.

HERRAIZ, P. "Deep fake: así será la manipulación del futuro". *El mundo*, 8 de mayo de 2019.

JOSE MARIN, J. y RUIZ GUEVERA, P. "Matemáticas para proteger la democracia". *El país*, 19 de diciembre de 2018.

LAUSSON, J. « Facebook pourrait menacer la démocratie, selon un ex-patron des renseignements britanniques ». *Numerama*, 8 décembre 2018.

« Les Fake-news partagées sur Facebook par les « gilets jaunes » visionnées plus de 105 millions de fois ». *Le Nouvel Obs*, 13 mars 2019.

PEREZ-LANZAC, C. "No les pongas el trabajo fácil". *El país*, 24 de marzo de 2019.

SIGNORET, P. « Wanted : une communauté Facebook de 800 000 membres et pas un rond ». *Le Monde*, 5 mai 2018.

TORRES DEL CERRO, A. "La lucha contra las "fake news" es un "talón de Aquiles" de las democracias". *El confidencial*, 20 de septiembre de 2018.

VENTURA, B. "La fábrica de líderes: así contribuyen medios y redes sociales a elegir a los políticos". *Yorokubu*, 22 de noviembre de 2018.

Obras universitarias

BOULAY, S. *Usurpation de l'identité citoyenne dans l'espace public : astroturfing et communication politique*. Montréal : Doctorat en Communication, Université du Québec à Montréal, 2012. 359 p.

GALLARDO PAULS, B. y ENGUIX OLIVER, S. *Pseudopolítica: el discurso político en las redes sociales*. Valencia: Departamento de Teoría de los Lenguajes y Ciencias de la Comunicación, Universitat de València, 2016. 207 p.

Leyes, circulares, jurisprudencias

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. *Circular 1/2019 sobre el tratamiento de datos personales relativos a opiniones políticas y envió de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del articulo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general*, 7 de marzo de 2019.

CONSEIL CONSTITUTIONNEL. *Décision n° 2018-773 DC*, 20 décembre 2018.

CONSTITUTION FRANCAISE, 4 octobre 1958.

CONSTITUCION ESPAÑOLA, 6 de diciembre de 1978.

COUR DE JUSTICE DE L'UNION EUROPENNE. *Affaire 362/14 dite « Safe Harbor »*, 6 octobre 2015.

DECRET n° 2019-297 *relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général*, 10 avril 2019.

LEY ORGANICA 5/1985 *del régimen electoral general*, 19 de junio de 1985.

LEY ORGANICA 3/2018 *de protección de datos personales y garantía de los derechos digitales*, 5 de diciembre de 2018.

LOI ORGANIQUE n°2018-1201 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

LOI ORGANIQUE n°2019-221 *relative au renforcement de l'organisation des juridictions*, 23 mars 2019.

LOI n°62-1292 *relative à l'élection du Président de la République au suffrage universel*, 6 novembre 1962.

LOI n°78-17 *relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978.

LOI n°86-1067 *relative à la liberté de communication*, 30 septembre 1986.

LOI n°2016-1321 *pour une république numérique*, 7 octobre 2016.

LOI n°2018-1202 *relative à la lutte contre la manipulation de l'information*, 22 décembre 2018.

PARLEMENT EUROPEEN ET CONSEIL. *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995.

PARLEMENT EUROPEEN ET CONSEIL. *Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*, 12 juillet 2002.

PARLEMENT EUROPEEN ET CONSEIL. *Directive 2003/98/CE sur la réutilisation des informations du secteur public*, 17 novembre 2003.

PARLEMENT EUROPEEN ET CONSEIL. *Règlement (UE) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 27 avril 2016.

Declaraciones oficiales

CNIL. « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ». 8 novembre 2016.

CNIL. *Déclaration NS34* : « Communication politique ». 29 mars 2019.

CNIL. *Définition* : « Donnée sensible ».

CNIL. *Délibération n°2014-041*, 29 janvier 2014.

CNIL. « Election 2016/2017 : quelles règles doivent respecter les candidats et partis ? ». 8 novembre 2016.

CNIL. « La communication politique par courrier électronique ». 13 mai 2019.

CNIL. « Les droits des électeurs ». 13 mai 2019.

CNIL. « Les fichiers constitués dans le cadre des primaires ouvertes ». 8 novembre 2016.

CNIL ET CSA. *Guide* : « Campagnes électorales : tout savoir sur les règles CSA et CNIL ». 2018.

COMMISSION EUROPEENNE. *Colloque annuel sur les droits fondamentaux* : « la démocratie dans l'UE ». 26 et 27 novembre 2018.

- Resilient and inclusive democratic societies : supporting broad participation and representation ;
- Ensuring fair elections, pluralistic political debate and online and offline freedom of expression ;
- Sound and transparent information for an informed and pluralistic democratic debate : practical steps to ensure the support of the online world.

COMMISSION EUROPEENNE. *Commission guidance* : « The application of Union data protection law in the electoral context ». 12 septembre 2018.

COMMISSION EUROPEENNE. *Communication au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions* : « Lutter contre la désinformation en ligne, une approche européenne ». 26 avril 2018.

COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE fait rapport sur les progrès réalisés dans la lutte contre la désinformation en vue du Conseil européen ». 14 juin 2019.

COMMISSION EUROPEENNE. *Communiqué de presse* : « Une Europe qui protège : l'UE renforce son action contre la désinformation ». 5 décembre 2018.

COMMISSION EUROPEENNE. *Déclaration relative au code de bonnes pratiques contre la désinformation* : « la Commission invite les plateformes en ligne à fournir davantage de précisions sur les progrès réalisés ». 28 février 2019.

COMMISSION EUROPEENNE. *Final report of the High Level Expert Group on Fake News and Online Disinformation*. 12 mars 2018.

COMMISSION EUROPEENNE. *First monthly intermediate results of the EU Code or Practice against disinformation*. 28 février 2019.

COMMISSION EUROPEENNE. *Last intermediate results of the EU Code of Practice against disinformation*. 14 juin 2019.

COMMISSION EUROPEENNE. *Report of the Independent High Level Group on Fake-news and online disinformation* : « a multi-dimensional approach to disinformation ». 2018.

EUROPEAN DATA PROTECTION BOARD. *Statement 2/2019 on the use of personal data in the course of political campaigns*. 13 mars 2019.

SUPERVISOR EUROPEO DE PROTECCION DE DATOS. *Dictamen 3/2018 sobre la manipulación en línea y los datos personales*. 18 de marzo de 2018.

Sitios web

www.blogdumoderateur.com (consulté le 21 décembre 2018)

Videos

HUCHON, T. Comment Trump a manipulé l'Amérique ? *Arte*, 2018. Disponible sur : www.arte.fr (consulté le 13 octobre 2018)