Victor Cavalcante

LA PERSONNALISATION DE LA COMMUNICATION POLITIQUE : QUELLE PROTECTION AUX ÉLECTEURS FACE AU TRAITEMENT ALGORITHMIQUE DE LEURS DONNÉES PERSONNELLES ?

Sous la direction de Mme Névine LAHLOU

Master 2 droit des Données, des Administrations Numériques et des Gouvernements Ouverts

Année universitaire 2020 - 2021

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE
ÉCOLE DE DROIT
DE LA SORBONNE

L’université Paris 1 Panthéon-Sorbonne n’entend donner aucune approbation, ni improbation, aux opinions émises dans le présent mémoire de recherche. Ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

À ma famille, Deise SHIMIZU, Kazuyuki SHIMIZU et Mariana SHIMIZU, pour le soutien émotionnel inconditionnel, mon remerciement spécial.

Je tiens à remercier madame Névine LAHLOU, la directrice de ce mémoire de recherche, pour son engagement et présence constante dans l'orientation de mes travaux. Je lui suis reconnaissant pour son investissement personnel.

Je tiens à remercier également madame Irène BOUHADANA et monsieur William GILLES, qui m'ont permis de leur rejoindre sur ce projet réussi qui est le Master 2 Droit des données, des administrations numériques et des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne.

Je remercie encore Alan PAES et Vinícius GONZAGA, des amis qui j'ai eu la chance de connaître durant mon séjour à Paris.

Je remercie enfin Laetitia TAZIAUX, pour la bienveillance de m'accorder du temps à la relecture de ce mémoire.

SOMMAIRE

ABBRÉVIATIONS PRINCIPALES

CE	Conseil d'État
CEPD	Comité Européen de la Protection des Données
CJUE	Cour de Justice de l'Union Européenne
CNIL	Commission National de l'Informatique et des Libertés
Cons. const.	Conseil Constitutionnel
ICO	Information Commissioner's Office
PS	Parti Socialiste
RGPD	Règlement Général sur la Protection des Données
UMP	Union pour un Mouvement Populaire

INTRODUCTION

L'effort porté par les hommes d'état pour se faire entendre traverse largement l'histoire de l'organisation sociale dans l'occident. À la cité grecque, l'assemblée du peuple, censée guider les affaires de la ville, délibérait sur un éventail considérable de sujets, comme la politique interne et externe, l'élection des magistrats, la passation des lois et la création des ressources financières. Pour ce faire, elle se prévalait des apports concrets des citoyens, à la fois éditeurs et destinataires des délibérations[1].

Ce caractère de légitimation populaire de la volonté politique retrouve des échos partout où l'opinion des administrés a contribué à la mise en œuvre de l'idéal de démocratie consacré siècles plus tard par Abraham Lincoln. Le gouvernement du peuple, par le peuple et pour le peuple présuppose, de plus en plus, un niveau optimal d'entente entre les responsables politiques et les administrés.

Les technologies d'information et communication utilisées par ces responsables pour porter leur message connaissent des bouleversements importants au fil de années. Des changements qui, pour la plupart, étendent la portée non seulement géographique du message transmis, mais également de sa précision[2]. Les partis politiques, les élus et les candidats à des fonctions électives, sont très vite heurtés à l'inexorabilité de cette dynamique, et le besoin de voir délimités les contours de cette communication que l'on appellera *politique* s'imposera.

Avant de s'intéresser à la définition de ce terme, il convient de distinguer ce que la littérature spécialisée[3] appelle les trois périodes des campagnes électorales traversées par les organisations politiques. La prémoderne, allant du milieu du XIX^{e} siècle à 1950, se caractériserait par des relations d'interconnaissance entre les hommes politiques et les citoyens et un niveau d'organisation léger et éphémère des volontaires. Les moyens de communication

[1] « *L'Assemblée restait toujours maîtresse de son ordre du jour. Un évènement imprévu pouvait exiger une mesure urgente ; une délibération pouvait ne pas aboutir en une séance (…). Enfin, sous le coup d'un malheur public, quand on était pressé par la nécessité, les prytanes convoquaient une 'assemblée d'épouvante et tumulte', en y appelant les citoyens de la ville aux sons de la trompette et ceux de la compagne par un feu allumé sur l'agora* », *in* G. GLOTZ, « La cité grecque, *Albin Michel*, 1928, pp. 183-184.

[2] « Précision » en tant qu'acte approprié au geste, cf. définition proposée par le site internet officiel du Centre National de Ressources Textuelles et Lexicales, consulté en ligne le 29 mai 2021.

[3] P. NORRIS (2003), citée par J. GERSTLÉ ; C. PIAR, « La communication politique », *Armand Colin*, 2020, p. 108.

dont ceux-ci se prévalaient pour relayer le message politique étaient manifestement simples[4]. La moderne, débutant aux années 1960 et s'achevant à la fin des années 1980, voit la durée des campagnes s'allonger et augmenter le niveau de professionnalisation des bénévoles œuvrant pour les campagnes. Elle témoigne d'une accentuation sensible du dynamisme des campagnes, en vertu de la montée en importance des sondages politiques et leur effet *feedback* sur la communication politique[5]. Enfin, la période post-moderne, à partir des années 1990, expérimente l'intensification de la coordination centrale des campagnes et de la professionnalisation, au vu de la proéminence des « campagnes permanentes ». L'espace politique s'enrichit d'autres supports, tels que la télévision[6] et l'internet (avec les blogs et réseaux sociaux, groupes de discussions, podcasts, etc.).

L'internet jouera un rôle capital dans la compréhension des décisions des électeurs. Les partis politiques, élus et candidats à des fonctions électives l'utilisent à partir du début des années 2000, pour apprivoiser le potentiel insaisissable de la donnée, particulièrement des données personnelles des électeurs, afin de construire leur stratégie de communication politique.

Mais qu'est-ce que la communication politique ? Il faut premièrement savoir que ces acteurs politiques, c'est-à-dire, les partis politiques, les élus et candidats à des fonctions électives, recourent à des traitements de données à caractère personnel dans le cadre de leurs activités. Des fichiers sont ainsi mis en œuvre aux fins de gestion interne des affaires de ces acteurs, de la communication en direction des membres ou des contacts réguliers des partis, de prospection (recherche de nouveaux adhérents, de soutiens, de financements, etc.) ainsi que de propagande (en vue d'une élection particulière). Dans le cadre de ce mémoire de recherche, ces activités seront regroupées sous la rubrique de « *communication politique* »[7].

Alors que la communication politique fait l'objet de plus d'attention des grands médias durant la période électorale, le message dirigé aux membres d'un parti ou contacts des acteurs

[4] Notamment les affiches, tracts, libelles, les émissions de radio et les tournées des candidats.
[5] En France, cet effet, consistant à une épreuve presque instantanée de la force du message porté par les acteurs politiques, a été repéré depuis la « période moderne » d'organisation des campagnes, non seulement en vertu des sondages, mais aussi de l'introduction de la télévision dans le débat politique. Se référer à A. CHAUVEAU en « L'Homme Politique et la Télévision », *Presses de Sciences Po*, 2003, p. 91.
[6] La démocratisation de l'accès à la télévision, nous précisons.
[7] D'autres définitions, plus socio-politiques que proprement juridiques, mettent l'accent sur le côté informatif de la communication, en favorisant des débats horizontaux et verticaux, l'influence sur les délibérations, la participation aux décisions, tout en permettant l'évaluation des actions conduites par la municipalité. *In* G. LOISEAU, « La démocratie électronique municipale française : au-delà des parangons de vertu », *CNRS Éditions*, 2000, p. 216.

politiques à des fins politiques (en vue d'une élection particulière) peut tout à fait être véhiculé avant, voire assez à l'avance, de cette période. Cela fait que le phénomène de la communication politique n'est nullement cantonné aux seuls mois précédents à la tenue des élections.

Ainsi, la communication politique peut être entendue comme moyen de prospecter de nouveaux électeurs ou de s'adresser aux électeurs dits acquis (ou bien de « fidéliser » les électeurs). Or, les projets et les hommes politiques n'étant pas des marchandises, l'idée de « fidéliser » des électeurs serait normalement à bannir du vocabulaire de la communication politique[8]. Et pourtant, les pratiques modernes entourant l'application de techniques de vente de marchandises au contexte électoral, connues sous l'appellation de marketing politique, connaissent un rebond dans les années 1980 et 1990, alors même que sa genèse serait plus lointaine[9].

La campagne présidentielle de Bill Clinton aux élections de 1992 est l'un de ces premiers exemples. Essentiellement novatrice, la proposition d'un site Web pour le candidat à l'époque où l'internet comptait à peine une cinquantaine de sites au total n'a pas reçu beaucoup d'attention du public[10]. Aux présidentielles de 1996, les équipes de campagne mobilisent d'autres moyens d'utiliser l'internet, en y proposant des dossiers sur les enjeux de la campagne, des discours des candidats et des tentatives d'engager les électeurs en ligne et sur le terrain.

Si le concept de communication politique ne pose pas d'obstacles conséquents à sa compréhension, il est néanmoins nécessaire de la distinguer des autres approches voisines se prêtant peut-être à la confusion. Outre la communication assurée à des fins politiques (en vue d'une élection particulière), les élus sont souvent amenés à s'adresser à leurs administrés en tant que responsables politiques, de l'État ou collectivités territoriales. Cette communication, institutionnelle par essence, dépourvue de finalité électorale, ne devra être considérée comme communication politique à des fins de ce travail[11]. Ainsi, par exemple, la communication

[8] « *Deux stratégies de communication sont généralement mises en place par les hommes politiques en campagne (Maarek, 2001, p 66). La communication « de conquête » s'intéresse aux électeurs fragiles des concurrents et aux indécis. Dans la communication « de maintien » en revanche, le candidat cible principalement ses propres électeurs fragiles et ceux décrits comme 'acquis'* », *in* C. MAUNIER, « La Communication politique en France, un état des lieux », *Éditions ESKA*, avril 2006, p. 74.

[9] « *Né aux États-Unis dans les années 1950 (Albouy, 1994), le marketing politique ne s'est répandu que dix ans plus tard au continent européen et en France en particulier (Albouy, 1994 ; Thomas-Joyeux, 1980 ; Maarek, 2001)* », *Op cit.*, p. 70.

[10] E. BARQUISSAU ; L. SCHLENKER « Marketing et Communication Politique », *EMS Editions*, 2017, p. 260.

[11] Le partage entre communication politique et communication institutionnelle était déjà clair lors de l'édiction, par le Commission Nationale de l'Informatique et Libertés, de sa délibération 96-105, du 03 décembre 1996, portant

adressée par le maire aux administrés d'une commune pour gérer les affaires communales ne saurait être de la même nature que celle mise en œuvre par des candidats à l'élection et des partis politiques aux électeurs en vue d'une élection particulière.

En ce qui concerne les médias et les moyens techniques et communicationnels mobilisables par les acteurs politiques pour se faire entendre (ex. affiches, bouche-à-l'oreille, porte-à-porte, télévision, radio, réunions publiques, contacts téléphoniques, tracts, internet), les spécialistes de marketing et communication en ont proposé une typologie intéressante, qui essaie de décortiquer les fonctions de chacune, les types d'interaction envisageables entre les acteurs politiques et les électeurs, et la nature officielle ou optionnelle du média[12].

Le besoin de comprendre les motivations, envies, craintes et doutes des électeurs, afin de communiquer avec eux, sera rapidement saisi par les partis, élus et candidats à des fonctions électives. Cet impératif, de connaître pour comprendre – et convaincre –, témoigne d'un effort grandissant de personnalisation de la stratégie de communication politique de la part de ces acteurs politiques.

Certes, cette personnalisation traverse des moments historiques divers, en France et ailleurs, avec des degrés variables d'incidence sur les droits des électeurs. Néanmoins, un regard plus attentif sur la manière dont la communication politique a évolué en France amène à un constat : certains de ces droits, notamment ceux qui orbitent autour de la vie privée des électeurs, ont été davantage remis en cause avec la personnalisation de la communication politique.

L'encadrement juridique de la matière évolue pour rattraper le dynamisme implicite à la communication politique. Des textes ayant une incidence sur la protection des données personnelles des personnes sont mis en place au niveau national et européen. Les électeurs retrouvent ainsi, depuis la fin des années 1970, un dispositif juridique non négligeable pour faire valoir certains droits. La Commission Nationale de l'Informatique et Libertés prend le relais du législateur dans la matière en édictant, en 1985, l'une des premières délibérations

recommandation relative à l'utilisation de fichiers à des fins politiques. Le régime de déclarations des actes relevant des deux modalités de communications se distinguait sensiblement (se référer à la page 8 de ce document).

[12] C. MAUNIER, *Op cit.*, p. 78.

applicables à la communication politique, sur l'utilisation de fichiers publics et privés, « en vue de l'envoi de documents de propagande et de la recherche de financement »[13].

Au fil de la réflexion, il sera démontré que les stratégies traditionnelles d'approche des électeurs par les partis politiques, élus et candidats à des fonctions électives en France ont basculé de manière constante vers la personnalisation de la communication. À l'appui des nouvelles technologies d'information et communication, notamment l'internet, le degré de personnalisation du message s'accentue. Les *données personnelles* deviendront ainsi la matière première de cette personnalisation.

Celles-ci permettront, dans un deuxième temps, l'intensification, à un degré encore plus important, de la personnalisation de la communication politique avec les logiciels de stratégie électorale, objet d'analyse de la deuxième partie de ce travail.

Il emporte de préciser à ce stade que les cookies, autre moyen de personnalisation possible de la communication politique, ne seront pas étudiés dans ce mémoire. Le régime juridique et la réglementation de la matière par la CNIL méritent, il semble, une étude à part entière.

Eu égard à ce contexte particulier de l'approche des électeurs, il convient de vérifier dans quelle mesure la personnalisation de la communication politique implique des risques à la protection des données personnelles des électeurs. Pour cela, il faudra s'intéresser, dans une première partie, à la manière dont les stratégies traditionnelles de communication ont été mises en œuvre par les acteurs politiques, ainsi qu'à leurs effets, qui se sont avérés premièrement maîtrisés (**Partie 1**). Ensuite, dans une deuxième partie, il conviendra d'une part de s'attarder sur l'accentuation du degré de personnalisation de la communication politique et d'emblée aux effets décuplés et potentiellement délétères aux données personnelles des électeurs et droits qui s'y attachent (**Partie 2**).

[13] Délibération CNIL n° 85-60, du 05 novembre 1985.

PREMIÈRE PARTIE

LA COMMUNICATION POLITIQUE : UNE STRATÉGIE TRADITIONNELLE AUX EFFETS MAÎTRISÉS POUR LA PROTECTION DES DONNÉES PERSONNELLES DES ÉLECTEURS

Dans cette première partie, il sera analysé comment les efforts apportés par les acteurs politiques pour s'approcher et entretenir avec les électeurs un contact à des fins politiques ont été encadrés par les textes juridiques français et européens dès la fin du XX^{e} siècle. Dès le départ du mouvement de légiférération, le législateur repère des bases de licéité mobilisables pour mettre en œuvre la communication politique, ce qui consacre juridiquement un point d'interlocution possible entre ceux-ci et les électeurs. Les textes structurants comme la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, la « loi informatique et libertés », font l'objet de changements importants au début des années 2000, notamment par l'initiative du droit européen. Ces changements constituent, pour les électeurs, des garanties supplémentaires de respect aux droits inscrits auparavant dans l'ordonnancement juridique, et élargissement d'autres droits. Les prémices de la communication politique témoignent la pratique de prospection et fidélisation des électeurs à l'appui des techniques classiques d'approche des électeurs **(Chapitre 1)**. Ces techniques, de par leur nature, ne se sont pas avérées des menaces substantielles aux données à caractère personnel des électeurs **(Chapitre 2)**.

CHAPITRE 1 – UNE STRATÉGIE TRADITIONNELLE PRÉVUE PAR LE DROIT POSITIF

Les techniques classiques d'approche des électeurs, érigées en véritable stratégie de prospection et fidélisation des électeurs, n'ont pas été négligées par la première vague législative sur la protection des données à caractère personnel. Inaugurée en France par la loi informatique et libertés, cette vague, à la fois européenne et française, apportera de gages à la protection de certains droits fondamentaux des électeurs, comme la vie privée et le droit à l'information **(Section 1)**. À cette phase de positivation de droits s'est suivie une autre, d'élargissement de l'étendue des droits des électeurs **(Section 2)**.

Section 1 – L'encadrement juridique européen et national bienvenu de la communication politique

Si la communication politique en tant que phénomène social[14] remonte à des moments historiques anciens, ce n'est qu'à partir de la fin des années 1970 que le législateur européen et national se sont emparés du sujet pour en encadrer la pratique et fixer des limites. Cet encadrement juridique voit ainsi le jour à l'aube de l'activité informatique, où l'échange des informations entre les acteurs politiques et le grand public se caractérisait par sa verticalité – diffusion des informations de ces acteurs vers les électeurs (**Paragraphe 1**). Il s'est ensuite avéré que la protection des données personnelles des électeurs ne pouvait pas être assurée sans que les bases de licéité de leur traitement ne soient pas établies en amont (**Paragraphe 2**).

Paragraphe 1 – L'autonomisation du corpus juridique à l'heure de la société d'information, ou Web 1.0

Quelques théoriciens du marketing indiquent que c'était bien à la première partie du XX^{e} siècle que les entrepreneurs se sont heurtés à l'urgence de miser sur des techniques plus raffinées de communication avec le public-cible pour faire couler la production[15].

[14] En vertu de sa régularité dans l'organisation les sociétés modernes, la communication politique s'approcherait de l'idée durkheimienne de fait social, qui conditionnerait les décisions des électeurs en tant que participants du débat politique.

[15] « *L'entreprise sait produire, elle doit maintenant apprendre à vendre. C'est l'âge d'or de la 'réclame' et des techniques de vente développées aux États-Unis à partir des années trente* ». *In* S. MAYOL, « Le Marketing 3.0 », Chapitre 2, Marketing 1.0, 2.0 et 3.0, *Dunod*, 2011, p. 4.

L'arrivée de l'internet dans les années 1960 et la parution des premiers sites de commerce en ligne quelques décennies plus tard[16] ont ensuite fait migrer l'arsenal communicationnel développé jusqu'alors par les professionnels du marketing vers le réseau mondial d'ordinateurs. À ce moment, l'existence d'un web statique, figé, centré autour de la production et diffusion des informations par ceux qui détenaient les produits ou services à vendre sur le web, ne permettait l'intervention des utilisateurs ciblés (les consommateurs) qu'à la marge, pour des échanges et opinions ponctuels. Ce paysage de production de l'information en réseau, dont l'entrepreneur était l'axe principal à partir duquel le contenu émanait vers les consommateurs, règne jusqu'au début des années 2000[17].

Naturellement, les données personnelles, appelées alors « informations nominatives » par la loi informatique et libertés[18], des consommateurs ont fait l'objet de la convoitise de ces premiers entrepreneurs du web, autant que des partis politiques, élus et candidats à des fonctions électives.

Ces acteurs politiques se sont ainsi confrontés à des contraintes légales ayant vocation à encadrer la communication politique et protéger les données personnelles des électeurs. C'est avec la loi informatique et libertés – et, au niveau européen, avec la Convention du Conseil de l'Europe n° 108, du 28 janvier 1981, que sont posés les premiers standards de protection des données personnelles des électeurs.

La loyauté et licéité de la collecte des données personnelles ont été dans la première version de la loi informatique et libertés. Le droit d'accès – que, dans le contexte de la communication politique, se décline dans le droit des électeurs à la communication de leurs données personnelles, opposable aux partis politiques, élus et candidats à des fonctions électives – s'est vu accompagner d'un droit à la rectification des données personnelles, du droit à l'information et du droit à l'opposition au traitement des données personnelles. Pour ce qui est des opinions politiques, l'interdiction par principe de traiter des données qui les font apparaître

[16] « *At noon yesterday, Phil Brandenberger of Philadelphia went shopping for a compact audio disk, paid for it with his credit card and made history. (...) There, a team of young cyberspace entrepreneurs celebrated what was apparently the first retail transaction on the Internet using a readily available version of powerful data encryption software designed to guarantee privacy. », in «* Attention Shoppers, the internet is open », *New York Times*, 12 août 1994, consulté en ligne le 24 mars 2021, 13h20.
[17] « Du web 1.0 au web 4.0 », *Marketing*, sans date, consulté en ligne le 23 mars 2021, 16h45.
[18] L'expression « données à caractère personnel » a remplacée celle « d'informations nominatives » par la loi du 6 août 2004, que nous aborderons par la suite. La notion « d'informations nominatives » suggérait un rapport direct uniquement avec les éléments d'identification entretenant une proximité avec le nom de la personne concernée, alors que son périmètre d'application avait, depuis le départ, vocation à recouvrir beaucoup plus de données.

s'est inscrite dans la loi de 1978, qui pour autant pourrait être dérogée par l'accord des personnes concernées[19].

Contrairement à la tendance législative moderne, les premières versions de la loi de 1978 ne posaient pas l'obligation d'informer les personnes lorsque les données personnelles les concernant étaient collectées auprès de tiers[20]. Cela témoignait d'un premier décalage législatif à la réalité, où le partage des données personnelles en ligne à des fins de prospection commerciale et les activités de courtage de données prenaient déjà l'essor, comme il sera précisé dans les lignes qui suivent.

La Convention n° 108, en précisant son but de garantir le respect des droits et libertés des personnes dans les territoires des États signataires, notamment le droit à la vie privée, renverra à la loi nationale la tâche de poser les garanties appropriées au traitement des opinions politiques. Cette convention apportera pour la première fois au niveau européen le concept de « fichier automatisé », qu'elle définira comme tout ensemble d'informations faisant l'objet d'un traitement automatisé.

Plus tard, la Directive 95/46/CE du Parlement européen et du Conseil de l'Union européenne, du 24 octobre 1995, sur la protection des données personnelles, éclaircira les controverses autour de la base de licéité de la collecte des données relatives aux opinions politiques des personnes, en invitant, dans son considérant 36, les États membres à autoriser ce traitement sur la base de l'intérêt public poursuivi par le responsable de traitement. La Directive comblera par ailleurs un vide important de la loi nationale, en obligeant l'information de la personne concernée lorsque les données la concernant ne sont pas collectées directement auprès d'elle. La Directive entre en vigueur en France en 2004, avec la transposition en droit national opérée par la loi n° 2004-801, du 6 août 2004.

L'article L52-1 du Code électoral, dans sa rédaction fixée par la loi n° 90-55 du 15 janvier 1990, est venu encadrer la pratique de la propagande électorale pendant les trois mois avant le premier jour du mois d'une élection et jusqu'à la date du tour de scrutin, en interdisant

[19] Article 25 pour la loyauté et la licéité dans la collecte des données ; article 34 pour le droit d'accès aux données détenues à l'égard de la personne concernée ; article 36 pour le droit à la rectification des données ; article 26 pour le droit à l'opposition ; article 27 pour le droit à l'information ; et l'article 31 pour l'interdiction par principe de traiter des données relevant des opinions politiques.

[20] A. MOLE, « Protection des personnes sur internet : conditions posées par la CNIL », *Victoires Éditions*, 1995, p. 63.

tout procédé de publicité commerciale par la presse ou par tout moyen de communication audiovisuelle. Ce délai a ensuite été ramené à six mois par la loi n° 2011-412 du 14 avril 2011[21].

Cette loi n° 90-55 du 15 janvier 1990, relative à la limitation des dépenses électorales et à la clarification du financement des activités politiques, et celles du 11 mars 1988 et du 15 janvier 1990, sur la réforme des modalités de la propagande électorale et le financement des partis politiques, ont également joué un rôle stratégique pour la limitation de la portée de la communication politique durant la période électorale[22].

La CNIL s'est investi tôt de ces missions d'analyse, d'alerte et de recommandation pour réguler les activités relevant de la communication politique. La délibération de la CNIL n° 85-60, du 05 novembre 1985, mentionnée en introduction, rappelait l'applicabilité des droits informatique et libertés évoqués précédemment aux électeurs prospectés. Cette délibération, à valeur de recommandation[23], faisait aussi savoir que l'utilisation à des fins de propagande et de financement de certains fichiers informatisés collectés pour assurer une mission de service public était de nature à constituer un détournement de finalité de traitement.

Toujours en 1985, la CNIL soulignait dans son rapport d'activités que parmi les cas les plus récurrents de détournement de finalité de traitement, on retrouve l'utilisation des fichiers clients à des fins autres que celles pour lesquelles ils ont été constitués, en méconnaissance l'article 27 de la loi. Lors des demandes de soutien financier à l'occasion de la campagne pour les élections cantonales de 1985, il s'est avéré que la société Burberrys a commercialisé de nombreux fichiers clients avec le Rassemblement pour la République, en faisant appel à des sociétés mandatées spécifiquement pour le faire[24]. D'autres réclamations de même nature identifiées par l'autorité française illustraient alors les frontières des premières atteintes repérées aux droits à la vie privée des électeurs dans le paysage politique national. Dix ans

[21] En Cons. const., 2002-2690 AN, 20 janvier 2003, *A.N., Paris*, le Conseil Constitutionnel, visant l'article 49 du même code, qui pose l'interdiction de diffuser électroniquement, à la veille du scrutin, tout message ayant le caractère de propagande électorale, a pris position en ce que le maintien du message de propagande électronique jusqu'au jour du scrutin ne constitue pas une opération interdite dès lors qu'il n'y avait pas des modifications apportées au contenu de ce message pendant la période de silence.

[22] « *Compte tenu des limitations apportées par la loi du 15 janvier 1990, aux moyens de communication couramment utilisés en période électorale (affichage, publicité par voie de presse ou audiovisuelle et mise à disposition d'un numéro vert au public), les candidats et partis politiques seront vraisemblablement amenés à adresser davantage de courrier aux électeurs* », *in* 12e Rapport d'activité de la CNIL, 1991.

[23] Comme la plupart des délibérations évoquées par ce travail, celle-ci aura valeur de recommandation, n'ayant donc pas de force contraignante.

[24] 6e Rapport d'activités de la CNIL, 1985, pp. 55-56. Aujourd'hui encore (2021), aucune disposition législative n'interdit à un parti, un élu ou candidat de procéder à la location de fichiers auprès de sociétés spécialisées à des fins politiques, la pratique étant donc autorisée.

après, cette tendance ne s'était pas amoindrie, le marketing politique demeurant l'un des dix secteurs d'activité ayant suscité le nombre le plus important de plaintes à la CNIL[25].

La CNIL a ainsi consolidé au fil des années sa doctrine au sujet de la protection des données personnelles des électeurs, par le biais de ses délibérations, recommandations publiés sur le site officiel, ou dans ses rapports d'activités annuels, où les intéressés trouveront des informations sur le contexte d'élaboration des normes élaborés, sanctions, et statistiques des plaintes et saisines de la CNIL.

Enfin, la Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, la Directive *e-Privacy*, transposée en droit national par la loi pour la confiance dans l'économie numérique, n° 2004-575 du 21 juin 2004, a harmonisé les dispositions des États membres concernant la protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée dans le secteur des communications électroniques, ayant vocation à s'appliquer à la communication politique lorsqu'elle se déroule électroniquement[26].

Vu les premières règles dégagées sur la protection des données personnelles applicables à la communication politique, il conviendra, dans un deuxième temps, de s'intéresser aux bases de licéité du traitement des données des électeurs utilisées par les acteurs politiques. Pour cela, il faudra en outre apporter des précisions sur les fichiers utilisés pour assurer cette communication.

Paragraphe 2 – Les bases de licéité du traitement des données des électeurs prospectés

Les textes n'ayant pas abordé directement les fichiers dont pouvaient se prévaloir les acteurs politiques pour s'approcher des électeurs, la CNIL s'empare de la tâche d'en donner des précisions. Dès 1985[27], l'autorité de contrôle crée une grille de partage utile entre les fichiers susceptibles d'être utilisés à des fins de communication politique des autres fichiers, à bannir de cette activité. Il était alors envisagé de faire de la pédagogie auprès de ces acteurs afin de réitérer dans les esprits des acteurs politiques l'importance de distinguer la communication politique de la communication institutionnelle.

[25] 16e Rapport d'activités de la CNIL, 1995, pp. 18 et 164.
[26] L'un des objectifs de la Directive était de faire maîtriser l'utilisation des cookies à des fins de traçage du comportement des internautes.
[27] Délibération CNIL 85-60, du 05 novembre 1985.

C'est pourquoi l'utilisation de fichiers informatisés de gestion publics ou privés, comme les fichiers du personnel, de locataires, de bénéficiaires de l'aide sociale, de fichiers d'abonnés des régies communales d'eau, de gaz et d'électricité, parmi d'autres – dont la finalité serait d'assurer l'imposition des personnes –, était à ce moment, et demeure aujourd'hui, interdite. En effet, la finalité pour laquelle les fichiers ont été collectés n'était pas liée à la réalisation de la communication politique, mais à une mission ou service public spécifique. Dans le même registre, en application de l'article 31 des premières versions de la loi informatique et libertés, il était déjà interdit le traitement des données qui faisaient apparaître les origines raciales, sauf accord exprès de l'intéressé. La Directive 95/46/CE élargira la portée de ce dispositif en interdisant également les traitements des données relevant spécifiquement de l'ethnie des personnes concernées, en comblant un vide législatif important existant jusqu'alors[28].

À l'inverse, l'autorité de contrôle française estimera que les listes d'adresses extraites de fichiers commerciaux informatisés, les données figurant dans le fichier de l'annuaire du téléphone, en raison de son caractère public, de sa finalité de communication, de sa mise à jour régulière, ainsi que les listes électorales, communicables à tout électeur et aux candidats et partis politiques pendant toute la période de l'année, pouvaient être légitimement utilisées à des fins de communication politique[29].

Un peu avant, le Conseil constitutionnel, dans sa décision n° 82-148, du 14 décembre 1982, saisi par des sénateurs contestant la régularité de certaines dispositions de la loi n° 82-1061 du 17 de décembre de 1982, relative à la composition des conseils d'administration des organismes de sécurité sociale, a expressément posé le principe selon lequel « la publicité des

[28] « *En juin 1994, sous le titre 'Électoralisme et immigration', Plein droit (n° 24) s'est fait l'écho des plaintes déposées par une association de Colombes, Actions citoyennes, contre une pratique qui avait, aux dernières élections cantonales, permis à l'association France Plus d'adresser, sur Colombes et Bagneux, des courriers ciblés à destination de jeunes d'origine maghrébine les invitant à voter pour deux candidats du RPR. Si ces plaintes n'ont pas abouti, elles ont révélé une faille importante dans notre système légal de protection des données nominatives* ». C. DAADOUCH, « Listes électorales, une exploitation contestable », *in Plein droit*, n° 28, septembre 1995. Le traitement des données concernant les origines raciales et ethniques fera ainsi objet d'interdiction (avec exceptions) par la loi française à partir de la loi de 06 août 2004.

[29] Aujourd'hui, c'est l'article L 330-4 du Code électoral qui donne le périmètre de consultation de la liste électorale par ces acteurs sociaux. En outre, une innovation récente dans la gestion des listes électorales a été instituée par la loi n. 2016-1048 du 1er août 2016, sur la rénovation des modalités d'inscription des électeurs sur ces listes. Le dispositif créera le répertoire électoral unique (REU), faisant office d'une « liste globale » des listes électorales sous contrôle de l'INSEE. On y retrouve, parmi d'autres, des données personnelles comme le nom, prénom, date et lieu de naissance, domicile ou lieu de résidence des électeurs. De manière assez surprenante, le Décret n. 2018-343 du 9 mai 2018, pris en application de quelques articles de cette loi, va créer la sous-catégorie « informations complémentaires » du répertoire électoral unique, pour y ajouter expressément l'adresse de messagerie électronique et le numéro de téléphone des électeurs, innovant sensiblement le dispositif juridique en vigueur.

listes électorales existe en toutes matières », de telles listes ayant ainsi vocation à être utilisées dans à des fins de communication politique.

La littérature juridique de l'époque témoignait des difficultés spécifiques rencontrées par certains départements français concernant la gestion des fichiers électoraux, en rappelant qu'il était déjà question d'assurer le fonctionnement régulier des mécanismes démocratiques[30], eu égard au besoin de prendre en compte les données des nouveaux électeurs, de radier celles des anciens électeurs, et cela annuellement.

A la suite de l'intervention des lois du 11 mars 1988 et du 15 janvier 1990, la recommandation de 1985 de la CNIL a été abrogée et remplacée par une autre, inscrite dans la délibération n° 91-115 du 3 décembre 1991, sur l'utilisation de fichiers à des fins politiques au regard de la loi informatique et libertés[31]. Comme les précédentes, la nouvelle recommandation mettra à jour les conditions de création et d'utilisation des fichiers crées par les partis politiques, élus et candidats durant la période électorale[32].

Plus récemment, le sujet a fait l'objet de nouvelles recommandations CNIL, pour tenir compte des avancées technologiques et de la complexification des pratiques communicationnelles en ligne qui se sont suivies depuis lors. La recommandation CNIL 2012-020, du 26 janvier 2012, dernière publié au sujet de la communication politique consolidant la doctrine de l'autorité de contrôle, actualise celle du 5 octobre 2006 (2006-228), et crée une typologie de fichiers qui est en partie reprise par d'autres recommandations plus récentes[33]. Parmi les fichiers utilisables, se retrouvent l'annuaire des abonnées des compagnies téléphoniques, les listes électorales, le répertoire national des élus, les fichiers de contacts occasionnels ou réguliers constitués par des candidats, élus ou partis politiques, les fichiers

[30] J. FRAYSSINET, « La communication et l'utilisation des listes électorales : de l'organisation du scrutin à la communication politique », *La Semaine Juridique Edition Générale*, 1989, p. 1.

[31] Sur le caractère non contraignant des recommandations de la CNIL, la 17e chambre correctionnelle du TGI de Paris a estimé, le 17 octobre 1994, dans un jugement non frappé d'appel, que la recommandation 89-13 du 14 février 1989 de la CNIL n'avait aucune portée à propos de l'exigence de déclaration préalable à la CNIL, si le législateur n'a pas entendu exiger de l'utilisateur de la liste électorale une déclaration préalable à la CNIL.

[32] Par une autre délibération parue de la même année (91-118), la CNIL adopte la norme simplifiée n° 34, destinée à faciliter les formalités préalables que devaient être accomplies par les partis, les élus ou les candidats à des fonctions électives. Cette logique des formalités préalables, il y a lieu de rappeler, a été abrogée par le Règlement UE 2016/679 du Parlement européen et du Conseil de l'Union européenne, au profit d'une logique de responsabilisation des acteurs par défaut.

[33] « Quels fichiers peuvent être utilisés à fins de communication politique », page web CNIL du 27 novembre 2019, consulté en ligne le 25 mars 2021, 21h20.

constitués lors des élections primaires ou pour organiser ou gérer un référendum local, données publiques issues des documents administratifs et certains fichiers du secteur privé[34].

Il semble ainsi que l'utilisation des techniques classiques d'approche des électeurs, menées par ces acteurs politiques à l'appui des fichiers énoncés, n'entraînait pas d'atteintes considérables aux droits et libertés des électeurs, comme le témoignent les premières décisions de justice et la doctrine spécialisée de l'époque.

Pour ce qui est des bases de licéité du traitement des données des électeurs, il a été précédemment souligné que la Directive 95/46/CE avait amorcé, dans son considérant 36, la possibilité de collecter des données concernant les opinions politiques des électeurs sur la base de l'intérêt public[35]. Le Règlement UE 2016/679 du Parlement européen et du Conseil, le RGPD, reprendra plus récemment le même ordre d'idées dans le considérant 56. L'article 7 de la Directive 95/46/CE et puis du RGPD inscriront effectivement dans le marbre cette possibilité.

La loi n° 2004-801, du 6 août 2004, en reprenant l'article 7, alinéa « a », de la Directive 95/46/CE, a posé le principe du consentement préalable des personnes concernant la réception de messages de « prospection directe »[36]. Or, si cette loi a voulu créer un obstacle (l'obtention du consentement) pour le traitement des données personnelles à des fins de prospection commerciale des consommateurs, le champ de la prospection politique aurait pu en être exclu. Toutefois, la CNIL a rappelé que face au silence de la loi, le régime inauguré par la loi de 2004 devrait s'appliquer également aux opérations électroniques de prospection politique[37], ce que consacre, pour la CNIL, une autre base de traitement possible des données des électeurs.

[34] Le Guide « Communication Politique – Obligations Légales et Bonnes Pratiques. » élaboré par la CNIL en 2012 précisera davantage la typologie dressée par cette recommandation. La CNIL y estimera que sont susceptibles d'être utilisés à des fins de communication politique les fichiers de « membres », de « contacts réguliers » et « occasionnels » d'un parti politique, les fichiers de « contacts réguliers » et de « contacts occasionnels » d'un élu ou candidat, les fichiers constitués dans le cadre de la désignation de candidats, d'un référendum local ou d'une pétition, les listes électorales, le répertoire national des élus, les annuaires mis à la disposition du public et les fichiers du secteur privé.

[35] Le considérant 30 du même texte laissait aussi aux États membres la tâche de préciser les conditions dans lesquelles la prospection faite par les partis politiques pourrait être faite.

[36] L'autre directive transposée à la même année, la Directive *E-privacy* de 2002, va poser le principe du consentement de la personne en matière de courriers électroniques du type SMS ou MMS, largement utilisés par les partis et responsables politiques à des fins de prospection politique. Lors de l'adoption du texte, une série de discussions avec les professionnels a eu lieu autour des nomenclatures '*opt-in,* (« je consens »), et l'*opt-out,* constituant l'exercice du droit d'opposition à cette modalité de prospection.

[37] Cf. Délibération CNIL n° 2006-228, du 5 octobre 2006. Aujourd'hui encore, aucune obligation légale spécifique n'impose aux partis et élus et candidats l'obligation de recueillir le consentement des électeurs au traitement de leurs données en matière de prospection politique, contrairement à ce qui existe en matière de prospection commerciale.

La loi et les recommandations de la CNIL indiquent par ailleurs les conditions dans lesquelles se faisait la collecte des données des électeurs à ce moment. Dans ses premières versions et jusqu'à l'avènement du RGPD, la loi informatique et libertés exonérait de déclaration à la CNIL la constitution de fichiers de membres et de correspondants des groupements politiques. Les sites internet mis en place pour assurer la communication politique partidaire, dès lors qu'ils permettaient la collecte de données personnelles (nom, prénom, adresse mail et autres données collectées avec des formulaires en ligne) ou leur diffusion (contributions à des forums), devaient être déclarés à la CNIL[38].

Eu égard aux dérives potentielles de l'utilisation des fichiers par les acteurs politiques, les commissaires à la protection des données et à la vie privée se sont réunis en 2005 à Montreux pour la 27e Conférence internationale des commissaires à la protection des données et de la vie privée (CIPDPPC). Sous initiative de l'Italie, les commissaires ont adopté une résolution concernant l'utilisation de données personnelles dans le cadre de la communication politique. Les commissaires ont fait savoir, notamment, que « *les données personnelles initialement collectées pour des activités de marketing sur la base d'un consentement éclairé peuvent être utilisées si la finalité de communication politique est spécifiquement mentionnée dans la déclaration de consentement*[39]».

La CNIL a continué d'être saisie en 2005 des plaintes d'internautes concernant l'utilisation par les acteurs politiques en méconnaissance de la loi. Les réclamations concernaient la réception de mails portant sur le programme d'un parti politique. En effet, la campagne pour les législatives portée par l'UMP, l'Union pour un Mouvement Populaire, sur l'internet a soulevé le mécontentement de quelques internautes, qui ont estimé ne jamais avoir autorisé le parti à utiliser leurs données, en assimilant ces messages à du « spam[40] ». La CNIL s'est intéressée aux étapes d'obtention des courriers électroniques par la légende, pour conclure que les mails des électeurs provenaient des sociétés spécialisées dans la location de fichiers – des courtiers de données. Les électeurs avaient de fait accepté, lors de la collecte des données,

[38] C. MAUNIER, *Op. cit.*, p. 81.
[39] Résolution sur l'utilisation des données à caractère personnel à des fins de communication politique, Montreux, Suisse, du 14 au 16 septembre 2005. Si cette résolution faisait état de déclaration d'intention par les autorités de contrôle nationales, sans portée normative contraignante pour les États représentés sur la conférence, elle a néanmoins contribué pour uniformiser la doctrine des autorités de contrôle participantes à l'égard de l'utilisation des fichiers par les acteurs politiques, dans le prolongement des attributions du G29, aujourd'hui Comité Européen de la Protection des Données (CEPD).
[40] En septembre 2005, l'UMP avait mené une campagne largement basée sur la prospection par courriel électronique, en adressant plus de 300.000 courriers électroniques sans avoir obtenu au préalable le consentement des personnes concernées (Article 8 de la loi informatique et libertés).

que leurs e-mails soient mis à disposition de tiers afin qu'il leur soit adressé des offres commerciales ciblées, mais pas des messages de communication politique, ce qui est reproché dans le cas de figure par l'autorité de contrôle sur la base de sa recommandation 96-105[41]. À l'issue de cette affaire, la CNIL se réunira avec les partis politiques pour dialoguer au sujet des conditions d'utilisation des fichiers des électeurs à des fins de communication politique.

Si les frontières entre les deux bases de licéité de traitement des données des électeurs – l'intérêt public et le consentement des électeurs –, manquent toujours de précisions plus nuancées par la littérature juridique, une nouvelle étape législative favorisera néanmoins l'accentuation de la protection des données personnelles des électeurs.

Section 2 – Le renouveau souhaitable du cadre juridique – Acte I

Inscrite dans la ligne droite de la première phase, de découverte des droits à la protection des données personnelles des électeurs, le tournant du XX^e^ au XXI^e^ siècle assistera à une nouvelle phase d'activité législative, cette fois-ci d'élargissement de droits. En outre, des garanties additionnelles aux droits énoncés en Section 1 seront apportées au cadre juridique français (**Paragraphe 1**), ainsi qu'une nouvelle typologie des électeurs dans le cadre de la communication politique, favorisant la création de régimes juridiques spécifiques et plus à même de répondre aux particularités et enjeux de chacun (**Paragraphe 2**).

Paragraphe 1 – Les garanties aux droits des électeurs prospectés : une sauvegarde nécessaire à la protection de droits à l'ère du web social, ou Web 2.0

L'arrivée des réseaux sociaux au paysage des communications numériques a eu des incidences importantes sur la forme de transmission des messages entre les internautes. Le développement de nouvelles formes de diffusion et de partage de l'information, qui se déverticalise au profit d'une approche décentralisée, centrée non plus sur le producteur du site ou plateforme de communication, mais sur les utilisateurs-consommateurs de contenu, donne lieu à ce que la théorie du marketing qualifie de web social (Web 2.0)[42]. Dans cette configuration, les internautes sont amenés à interagir sur le contenu et la structure des pages, en contact permanent avec les autres internautes. Cette approche, profitant davantage à la

[41] 26^e^ Rapport d'activités de la CNIL, 2005, p. 92.
[42] S. MAYOL, *op. cit.,* pp. 7-8.

créativité des professionnels de la parole dans l'espace communicationnel, donne un coup de renouveau aux stratégies de placement des marques auprès des consommateurs.

Les acteurs politiques ont rapidement pris le relais des entrepreneurs. Dès la création des réseaux sociaux partisans jusqu'au développement des microblogs de campagne sur Twitter, la littérature décèle un foisonnement des nouvelles plateformes de communication politique. Des outils numériques sont ainsi mobilisés afin d'apporter le message politique aux électeurs et assurer l'occupation partisane du web. *Coopérative politique* pour le Parti Socialiste (ci-après, le « PS »), *Créateurs du possible* pour l'UMP, *les Démocrates* pour le Modem, *Think Centre* pour le Nouveau Centre, et même une l'application i-Phone du site de campagne de Valérie Pécresse[43]. En septembre 2006, l'UMP est venu à la rencontre de sa jeunesse militante, potentiel vecteur de mobilisation en ligne, pour leur proposer de créer gratuitement leur blog militant en se prévalant du service *Typepad* lancé en 2003[44].

Ces prémices du web politique ne ressemblent guère aux sites internet que l'on connaît à ce jour, la communication politique étant alors marquée par la mise en place de sites internet pour y reproduire la logique du tractage qui se passait dans la rue[45].

C'est dans ce contexte qu'un nouveau degré de transparence est franchi en droit national sous l'initiative du droit européen. La loi n° 2004-801, du 6 août 2004, en transposant la Directive 95/46/CE, crée l'article 32 de la loi informatique et libertés. Cet article augmente l'étendue du droit à l'information des personnes concernées[46]. Des modifications au rôle de la CNIL ont aussi été apportées par le texte[47].

Dès lors, des informations comme l'identité du responsable du traitement, finalité poursuivie par le traitement et les destinataires ou catégories de destinataires des données sont

[43] T. BARBONI et É. TREILLE, « l'Éngagement 2.0 – Les nouveaux liens militants au sein de l'e-parti socialiste », *Presses de Sciences Po*, 2010, p. 1137.
[44] Les premiers blogs ont vu le jour en 1996 aux États-Unis, et ne se ressemblaient pas alors à la conception qu'on en retient aujourd'hui : il s'agissait plutôt de textes très courts, assortis d'une suite de liens afin de commenter l'actualité. *In* T. SOUBRIÉ, « Le blog : retour en force de la fonction d'auteur » *Colloque JOCAIR 2006*, Amiens, pp. 6-7.
[45] A. THÉVIOT, « Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter », *Le Bord de l'Eau*, 2019, p. 16.
[46] Ces droits sont aujourd'hui trouvables dans Articles 12 à 14 du RGPD, lequel augmentera davantage le périmètre des informations mises obligatoirement à disposition des personnes concernées.
[47] « *D'un contrôle a priori, la CNIL se voit octroyer un rôle a posteriori plus important. En effet, ses pouvoirs d'investigation sur place d'accès aux données se trouvent considérablement renforcés. Surtout, la CNIL se voit disposer d'un pouvoir de sanction et donc d'appréciation. Ces sanctions peuvent consister en sanctions administratives, telles que l'avertissement, et en sanctions financières jusqu'à 150.000 Euros, doublées en cas de récidive* ». *In* B. POIDEVIN, « La réforme de la loi Informatique et Libertés : la loi du 6 août 2004 », *Juris Expert*, 2004, p. 2.

à indiquer aux personnes concernées, de manière claire et complète. Cette avancée est à saluer vis-à-vis de la version précédente de la loi informatique et libertés, qui prévoyait notamment un droit d'accès, d'opposition et de rectification à l'égard des personnes concernées.

Cette loi apporte aussi une nuance importante dans le régime de déclaration de traitements à la CNIL. En effet, les formalités ne dépendaient plus seulement de l'attachement du responsable au secteur public ou privé (critère organique), mais aussi d'un critère matériel, à savoir, la sensibilité du traitement. L'article 25 de la loi de 2004 introduit huit catégories de traitements soumis à l'approbation de la CNIL, parmi lesquels le traitement des données sensibles, dont les opinions politiques[48]. Ainsi, le régime d'autorisation de traitement mis en avant par la CNIL à ce moment sera désormais axé sur les seuls traitements présentant des risques particuliers d'atteinte aux droits et aux libertés[49]. Au demeurant, c'est aussi à ce moment que la CNIL se verra confier une nouvelle modalité de contrôle des acteurs sociaux. Cela, de pair avec l'accentuation du pouvoir de sanction financière de l'autorité de contrôle, montant à 300 000 avec la nouvelle loi, indiquait un basculement des activités de contrôle de l'autorité de contrôle vers contrôle *a posteriori* à la mise en place du traitement par les responsables du traitement.

Dans sa délibération n° 2006-228, du 5 octobre 2006, portant recommandation relative à la mise en œuvre par les acteurs politiques de fichiers dans le cadre de leurs activités, la CNIL rappelle que les dispositions de la loi informatique et libertés, telle que modifiée en août 2004, garantissent une protection spécifique au traitement des données relatives aux opinions politiques des personnes. En reprenant l'article 32 de la loi, l'autorité éclaircit les obligations des acteurs politiques, en ajoutant que les mentions devraient figurer sur les bulletins d'adhésion et sur l'ensemble des supports utilisés (tracts, pages web, etc.) permettant collecter de données des électeurs. Lors de la prospection des électeurs, le message envoyé aux électeurs devait préciser de façon claire et visible, l'origine du ou des fichiers utilisés ou du programme de fidélisation, le fait que le parti, l'élu ou le candidat à de poste électif à l'origine de la campagne ne dispose pas de l'adresse utilisée mais a eu recours à un prestataire extérieur (courtier), et du droit des électeurs de s'opposer à recevoir de tels messages.

---

[48] V. BELEN, « Les tentatives de protection des données personnelles des individus : difficultés de définition et risques nouveaux », *ESKA*, 2005, p. 11.

[49] « *Comme le conseiller d'État Braibant l'a relevé, ce contrôle [a priori] a peu joué, puisqu'en vingt-cinq ans, la CNIL n'a effectué qu'un peu plus de 300 missions de vérification, ce qui donne en moyenne 13 contrôles par an* ». *In* F. FOURETS, « *La protection des données, ou le symbole d'une démocratie nouvelle* », Caisse nationale d'allocations familiales, 2005, p. 7.

Si le devoir d'information des électeurs était déjà non négligeable avant 25 mai 2018, avec le RGPD c'est désormais plus d'une dizaine d'éléments qui devront être fournis dans le cadre de l'obligation de transparence des acteurs politiques.

Une fois posés les jalons de ce cadre juridique renouvelé, il est requis d'examiner la catégorisation des électeurs, occasion où seront également abordées les méthodes utilisées le plus souvent par les acteurs politiques pour approcher les électeurs.

Paragraphe 2 – Les techniques d'approche des électeurs par les acteurs politiques

La loi du 6 août 2004 a entraîné d'autres changements relatifs au régime juridique de la communication politique. L'article 8 de la loi informatique et libertés, modifié par la loi de 2004, prévoira désormais que les partis et groupements politiques peuvent déroger l'interdiction existant par défaut de traiter des opinions politiques des électeurs, sous réserve que ces traitements ne concernent que les électeurs qui entretiennent avec eux des contacts réguliers dans le cadre de leur activité.

À la suite de cet apport législatif, la CNIL actualise sa doctrine avec une nouvelle délibération n° 96-105, rendue le 3 de décembre de 1996, portant recommandation sur l'utilisation de fichiers à des fins politiques. À cette occasion, l'autorité indique qu'il faut entendre par « correspondant » toute personne ayant accompli une démarche positive auprès du parti, touchant à son action proprement politique (demande d'informations, versement de fonds, etc.).

La délibération n° 2006-228, du 5 octobre 2006 renverse la logique de la délibération de 1996 au profit de la figure du « contact régulier ». Désormais pour la CNIL, des contacts réguliers sont les personnes qui versent des fonds, qui soutiennent de manière régulière l'action du parti ou de l'organisme politique concerné ou qui sont abonnées à une lettre d'information éditée par le parti ou le groupement à caractère politique. La CNIL rappellera que cette notion est distincte de celle d'un « membre » du parti[50].

[50] « *Est qualifiée de 'membre ou adhérent' toute personne physique qui remplit les conditions définies par les statuts de l'association, et notamment s'acquitte* », *in* Guide CNIL « Communication Politique – Obligations Légales et Bonnes Pratiques. », 2012, p. 11.

Ensuite, la délibération n°2012-021, du 26 janvier 2012, créera la figure du « contact occasionnel ». Elle le fera dans les termes suivants « *toute personne qui sollicite ponctuellement un candidat, élu ou parti politique, sans entretenir avec lui d'échanges réguliers dans le cadre de son activité politique ; ainsi que toute personne sollicitée à des fins de prospection politique à l'initiative du parti, élu ou candidat* ».

Ce partage a été le bienvenu à l'heure où le centre de gravité de la communication politique basculait vers les réseaux sociaux. Ainsi, des interactions ponctuelles avec les responsables politiques ou partis, sur Twitter, Facebook ou d'autres plateformes, comme l'envoi direct de messages aux élus et candidats, l'action d'aimer leurs profils sur les réseaux, ne sauraient être considérées comme de véritables engagements politiques, raison pour laquelle la règle de déclaration préalable à la CNIL en cas de traitement par les acteurs politiques des contacts occasionnels a été maintenue.

Si les techniques d'approche utilisées pour se communiquer avec les électeurs ont expérimenté un niveau d'accentuation notable d'intrusion dans la vie privée des électeurs, l'activité réglementaire de la CNIL en est suivie, avec une phase récente de consolidation des recommandations au sujet de la communication politique[51].

Le porte-à-porte a vu le jour en tant que pratique traditionnelle de prospection politique au début du XX^{e} siècle[52]. Ayant connu au cours des deux dernières décennies une attention plus importante des chefs des partis et groupements politiques, d'abord aux États-Unis puis en France, le porte-à-porte a été présenté, et légitimé scientifiquement[53], comme la technique de mobilisation électorale la plus efficace. Plus récemment, en 2011, l'élite du PS en France s'est renseignée aux États-Unis sur les fruits que la pratique a apportés à la campagne d'Obama, en vue des prochaines présidentielles.

[51] « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? », site internet officiel de la CNIL, 8 novembre 2016, consulté en ligne le 26 février 2021, 20h01.
[52] « *Aux Etats-Unis, le canvassing est pratiqué au moins depuis les années 1920* ». Une description intéressante, pour l'entre-deux-guerres, en est livrée par Whyte (W. F.), Street Corner Society. The Social Structure of an Italian Slum, Chicago, University of Chicago Press, 1943, p. 220-223. En France, la situation est moins claire, le recours au porte-à-porte étant évoqué parfois dans les années 1970 (notamment chez les syndicats étudiants). », *in* J. TALPIN ; R. BELKACEM, « Frapper aux portes pour gagner des élections ? », *De Boeck Supérieur*, 2014, p. 188.
[53] A. S. GERBER ; D. P. GREEN « The Effects of Canvassing, Direct mail, and Telephone Contact on Voter Turnout: A Field Experiment », *American Political Science Review*, Vol. 94, n. 3, 2000.

Probablement au vu du faible degré d'atteinte à l'intimité des électeurs liée à la pratique sur le terrain, la législation et règlementation nationales sur la protection des données personnelles n'ont pas apporté d'attention particulière à cette méthode de prospection.

En revanche, la communication politique par téléphone, autre technique d'approche, a fait l'objet de précisions par la CNIL depuis les prémices de l'activité réglementaire de l'autorité, d'abord par moyen de l'utilisation des listes d'abonnés aux services téléphoniques[54], et puis des annuaires des télécoms[55]. En 2006, la CNIL présente des bonnes pratiques concernant l'utilisation des SMS, MMS politiques, et même des automates d'appels[56].

À titre de rappel, un automate d'appel est un appareil permettant de déclencher par programme un grand nombre d'appels téléphoniques simultanés afin de délivrer un message préenregistré[57]. Contrairement à l'utilisation des SMS et des MMS, et compte tenu du caractère fortement intrusif des automates d'appel, la CNIL considère[58] qu'aucune exception au principe de collecte du consentement préalable des électeurs peut être invoquée par les acteurs politiques lors de la mise en place de cette méthode de communication[59].

Pour ce qui est du contact des électeurs par le web, il convient de distinguer l'approche par courrier électronique et par réseau social.

Selon les recommandations posées par la CNIL, les électeurs ne peuvent être prospectés par courrier électronique qu'après avoir autorisé leur contact à des fins de communication politique, quelle que soit l'origine de l'obtention du courrier par l'acteur politique concerné (collecte directe auprès des électeurs ou indirectement)[60]. Renouant avec les interdictions posées par la Directive 95/46/CE, la CNIL précise qu'aucun tri ne peut être opéré sur la base

[54] Délibération CNIL n° 85-60, du 05 novembre 1985.
[55] Délibération CNIL n° 96-105, du 03 de décembre de 1996.
[56] Délibération CNIL n° 2006-228, du 5 octobre 2006.
[57] Avec la délibération de 2006, la CNIL recommandait aux acteurs politiques de s'abstenir d'utiliser les automates d'appel dans la communication politique, position sur laquelle l'autorité est revenue en 2012, sans pour autant oublier d'en encadrer l'utilisation.
[58] Délibération CNIL 2012-020, du 26 janvier 2012.
[59] Selon l'énoncé du considérant 47 de la Directive 1995 alors en vigueur, le fait de faire appel à des entreprises tierces pour lancer des appels automatiques ne saurait constituer un obstacle à la responsabilisation des acteurs politiques pour les abus : « *lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message* ».
[60] Les partis, élus et candidats à des fonctions électives peuvent utiliser uniquement des fichiers de clients ou de prospects, et non des fichiers de gestion des ressources humaines, gestion de la paye, fichier administratif, l'annuaire interne d'un organisme, par exemple, au vu de la collecte des données qui s'y retrouvent pour atteindre une autre finalité.

de la consonance du nom des électeurs ou de leur lieu de naissance aptes à laisser apparaître leur origine ethnique[61].

En ce qui concerne l'approche sur les réseaux, il faut noter que la typologie contact régulier et occasionnel sera reprise lors de la recommandation récente de la CNIL sur les pratiques à adopter par les acteurs politiques dans cet environnement. L'autorité de contrôle a ainsi précisé que les contacts réguliers devront être informés des conditions de traitement de leurs données, par le biais des onglets « politique vie privée », alors que, pour les contacts occasionnels, il ne leur serait pas possible d'adresser directement des messages de communication politique, dans la mesure où ils n'auront pas pris connaissance de ces onglets en amont[62].

Il est à noter finalement que l'exigence de transparence posée par cette autorité aux acteurs politiques s'est accentuée sensiblement dans cet environnement, victoire dont les électeurs peuvent se féliciter au vu des atteintes potentielles à leurs droits et libertés, notamment le droit à la vie privée et à l'information, plus susceptibles dans l'écosystème des réseaux que dans celui du web 1.0 ou des campagnes sur le terrain. Pour éviter des dérives, la CNIL énonce que l'acceptation des électeurs à recevoir des newsletters ne vaut pas consentement à nouer des relations avec le candidat cherchant soutien, ainsi que la qualité de contact régulier sur Facebook ne saurait impliquer accord d'utiliser ses données sur Twitter[63].

Présentés les principaux enjeux de la communication politique trouvés dans les textes juridiques et la règlementation de la CNIL, il faudra s'intéresser par la suite au potentiel nuisible de l'arsenal communicationnel mis en avant par les partis, élus et candidats à des fonctions électives dans les premières années du web sémantique.

[61] Délibération n° 2006-228, du 5 octobre 2006.
[62] « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? », site internet officiel de la CNIL, 8 novembre 2016, consulté en ligne le 26 février 2021, 20h01.
[63] *Idem.*

CHAPITRE 2 – UNE STRATÉGIE AUX EFFETS MAÎTRISÉS POUR LA PROTECTION DES DONNÉES PERSONNELLES DES ÉLECTEURS

Les nouveaux horizons ouverts à la communication politique par les réseaux sociaux ont remis en cause l'efficacité des techniques classiques d'approche des électeurs par les partis politiques, élus et candidats à des fonctions électives. Désormais, il appartiendra aux acteurs politiques de s'emparer de l'interface, codes et grammaire de ce nouveau théâtre du débat électoral et politique pour porter efficacement son message. Dans un premier temps, il faudra souligner les implications juridiques du basculement de la communication politique vers les réseaux sociaux et des premières utilisations des algorithmes (**Section 1**), pour ensuite s'intéresser aux premières étapes de la personnalisation de l'approche des électeurs par les partis, élus et candidats à des fonctions électives (**Section 2**).

Section 1 – La prospection politique apparemment dépersonnalisée et les risques limités aux droits des électeurs

Les moyens d'ingérence des acteurs politiques dans la vie privée des électeurs, plus élaborées dans les réseaux qu'en dehors, ne sont pas facilement repérables dans le tournant des années 2010 (**Paragraphe 1**). L'absence de changement important du cadre normatif et réglementaire dans le début de la décennie témoigne de la stabilité de cette étape initiale de la personnalisation de la communication politique (**Paragraphe 2**).

Paragraphe 1 – Le traitement des données personnelles des électeurs à l'aube du web sémantique, ou Web 3.0

« *Discrétiser un objet (une image, un texte, une vidéo) revient à le transformer en une suite d'unités élémentaires (…) manipulables par une machine* »[64]. Le web sémantique, en tant qu'environnement favorisant la catégorisation détaillée des données sur la Toile, notamment par la division du contenu des pages web en fragments (titre, sous-titre, corps du texte, pied de page) repérables par des balises de codes HTML et d'autres langages informatiques, franchira une nouvelle étape dans la production et circulation des informations[65].

[64] G. SAMUEL « Outils d'écriture du Web et industrie du texte : Du code informatique comme pratique lettrée », *Réseaux*, vol. 206, n° 6, 2017, p. 68.
[65] « *The Semantic Web is about two things. It is about common formats for integration and combination of data drawn from diverse sources, where on the original Web mainly concentrated on the interchange of documents. It is also about*

C'est dans ce contexte socio-technologique, à l'ère de l'infobésité[66] inaugurée par le web social, que les algorithmes prendront l'essor. À des fins de ce travail, on retiendra la définition d'algorithme proposée par la CNIL pour discuter les enjeux éthiques de l'intelligence artificielle sur la communication politique. Selon autorité, un algorithme serait « *la description d'une suite finie et non ambigüe d'étapes (ou d'instructions) permettant d'obtenir un résultat à partir d'éléments fournis en entrée* »[67].

L'autorité avait déjà entrevue le potentiel des algorithmes pour la communication politique lorsqu'elle confirme la possibilité d'opérer, à partir des listes électorales, des extractions en fonction de l'âge ou du bureau de vote de rattachement des électeurs[68]. À l'égard des tris réalisables sur les données des électeurs, la CNIL rappelle qu'ils sont déloyaux et illicites lors qu'ils sont réalisés sur la base de la consonance du nom des électeurs, sur leur département ou lieu de naissance afin de s'adresser à eux en raison de leur appartenance, réelle ou supposée, à des communauté ethniques ou religieuses spécifiques. Cela est tout à fait compréhensible vu le risque de sélection et de discrimination susceptible de porter atteinte aux droits et libertés des électeurs[69]. Ainsi, des pratiques comme celles avérées aux États-Unis consistant à rassembler des e-mails des électeurs (12 millions pour les élections d'Obama)[70] pour en recouper selon ces et autres critères serait susceptible de sanction par l'autorité e contrôle française.

Les premières utilisations des algorithmes sur Twitter semblent avoir pris place peu de temps après la parution de ce réseau social, avec les bots[71]. Programmés pour générer une quantité conséquente de tweets, cela pouvait jouer autant pour relayer des informations utiles

---

language for recording how the data relates to real world objects. That allows a person, or a machine, to start off in one database, and then move through an unending set of databases which are connected not by wires but by being about the same thing », *in* « W3C Semantic Web Activity », sans date, consulté en ligne le 28 mars 2021 à 15h30.

[66] « *État résultant d'une information jugée trop abondante par rapport aux besoins ou aux capacités d'assimilation des utilisateurs* ». In Site internet officiel de l'Office québécois de la langue française.

[67] « *Comment Permettre à l'Homme de Garder la Main ?* », Synthèse du débat public animé par la CNIL dans le cadre de la réflexion éthique confiée par la loi pour Une République Numérique, 2017, p. 15.

[68] Délibération CNIL n° 2006-228, du 5 octobre 2006.

[69] Dans le paysage britannique, autorité de contrôle pour la protection des données d'outre-manche (*the Information Commissioner's Office* - ICO) estime qu'une donnée personnelle concernant l'ethnie sera probablement une donnée sensible.

[70] « 2012 : la bataille du Web *», Le Monde,* 12 octobre 2011, consulté en ligne le 28 avril 2021, 18h04.

[71] GitHub, an application development platform, was launched on April 10, 2008. « *Twitter bots have been present from the very beginning of the site's history. The oldest bot repository found was created only four days after GitHub's official launch date. The number of Twitter bots has been growing quickly. In GitHub's first two years, 2008 and 2009, almost 100 different bot codes were published* », *in* B. KOLLANYI « Where Do Bots Come From? An Analysis of Bot Codes Shared on GitHub », *International Journal of Communication*, 2016, p. 6.

que du spam ou du mauvais contenu. Des atteintes comme des ajouts aléatoires des membres de la communauté d'utilisateurs par les bots ont également été constatées.

Sur Facebook, les premiers moyens de classer mathématiquement l'information à afficher sur l'écran des utilisateurs ont vu le jour en 2006 avec le News Feed, l'outil mis en place par le réseau de Zuckerberg qui recense les informations et l'activité des proches des utilisateurs[72].

Dans le paysage politique français, l'avant-garde de la prospection politique à l'appui des technologies d'information et communication a été assurée par le PS français, qui voyait débarquer dans les années 2000 des nouveaux membres ayant adhéré par internet, en vue de préparer le terrain pour les présidentielles de Ségolène Royal. La campagne de Mme Royal pariait ainsi sur ce nouveau terrain de bataille pour rendre la candidate plus présidentiable aux yeux du bureau national du PS[73] et des électeurs potentiels. Naturellement, le traitement électronique des données des électeurs, se basant essentiellement sur des mails des électeurs[74], n'avait alors pas l'intention de déceler des opinions ou sensibilités électorales algorithmiquement exploitables par la direction du parti, mais uniquement de repérer et faire adhérer des électeurs susceptibles de voter pour le PS.

Pour les présidentielles de 2012, un nouveau moyen de prendre part à la vie démocratique nationale est créé. Dans les « Primaires citoyennes », environ 2,8 millions d'électeurs se sont déplacés, les 9 et 16 octobre 2011[75], pour désigner le candidat officiel du PS.

Des critères très souples, mais impliquant déjà un niveau plus accentué d'emprise par le parti sur les opinions politiques, se sont posés à la participation électorale de l'ensemble de la population dans le cadre des Primaires du PS : la signature d'une déclaration de soutien aux valeurs de la gauche et le versement d'un euro pour financer la campagne[76]. À cet égard, la

[72] « Can Facebook Fix Its Own Worst Bug? », *New York Times*, 25 avril de 2017, consulté le 28 mars 2021, 22h40.
[73] Selon l'étude de cas est issue du cours « *Être un élu 2.0 et gérer sa e-réputation sur Internet* » assuré par Pierre GUILLOU à des élus locaux le 30 janvier 2010.
[74] Sur cela, Arnaud Dassier, l'animateur de la campagne Internet de Nicolas Sarkozy en 2007, se souvient que le PS avait constitué pour les présidentielles de cette année une base d'environ 100 000 mails d'électeurs ou sympathisants. L'UMP en avait constitué une de 340 000. « 2012 : la bataille du Web *», Le Monde,* 12 octobre 2011, consulté en ligne le 28 avril 2021, 18h04.
[75] Les Primaires, compte tenu de leur nouveauté et importante pour le paysage politique français de ce moment, ont fait l'objet d'un examen minutieux par la CNIL, trouvable dans son 32e Rapport d'activités de 2011, p. 74.
[76] T. BARBONI et É. TREILLE, *op. cit.*, p. 1150.

CNIL a rappelé de manière assez opportune que le fait même d'enregistrer des données personnelles dans un fichier tenu par un parti politique, élu ou candidat à des postes électifs est déjà un traitement « sensible » puisque susceptible de révéler l'opinion politique, réelle ou supposée, des personnes concernées[77].

Si la règle alors applicable au traitement des données des membres et des contacts réguliers était celle de l'exonération de déclaration à la CNIL, cette même règle ne pouvait, selon l'autorité française, s'appliquer pour les fichiers mis en œuvre dans le cadre des primaires ouvertes, qui ne relèvent pas de la gestion des membres du parti[78]. Une primaire est dite « ouverte » lorsque des personnes autres que les seuls membres ou adhérents du parti peuvent y participer[79].

La doctrine de la CNIL sur l'utilisation des fichiers des participants à un scrutin donné (et les primaires en sont un exemple) était pour qu'ils soient collectés toujours pour la finalité spécifique dudit scrutin. Dans ce sens, des fichiers de participants constitués pour un scrutin ne pourraient – et ne le peuvent toujours pas –, être gardés pour les scrutins suivants, devant faire l'objet de radiation dans les meilleurs délais après l'investiture officielle du candidat victorieux.

Alors même que les fiches constitués par le PS dans le cadre de ces Primaires seraient détruits à la fin de ce scrutin, les votants que se sont rendus au parti pour voter ont été invités à laisser leurs coordonnées, ce qui a fait qu'après le premier tour des élections, entre 30% et 50% des participants auraient laissé leurs adresses e-mail *« pour être informés de la suite de la campagne »*[80]. Cette base de données constituée sur la base du consentement des votants donne au PS une avance remarquable vis-à-vis de l'UMP, lequel fait appel, encore une fois, à des bases de données commerciales auprès des agences spécialisées[81].

Si les moyens mis en œuvre par ces deux partis pour communiquer avec les électeurs et sympathisants étaient ceux traditionnellement utilisés dans les élections précédentes – à savoir, les rassemblements, le porte-à-porte, le mail, parmi d'autres, il faut souligner que la campagne

[77] Guide CNIL « Communication Politique – Obligations Légales et Bonnes Pratiques. », 2012, p. 6.
[78] Délibération CNIL 2012-020, du 26 janvier 2012.
[79] « Les fichiers constitués dans le cadre des primaires », site internet officiel de la CNIL, 16 janvier 2020, consulté en ligne le 06 juin 2021, 09h25.
[80] « 2012 : la bataille du Web *», Le Monde,* 12 octobre 2011.
[81] « L'UMP utilise de nouveau le marketing politique », *Le Figaro,* 25 janvier 2012.

pour les présidentielles de 2012 en France a marqué un tournant dans l'utilisation du *data analytics*[82] par les partis de tous bords pour ajouter de la valeur à la donnée traitée.

S'appuyant sur des bases de données d'électeurs, cette nouvelle technique n'a pas pour autant été mise en avant par les équipes de campagne, que ce soit à l'UMP ou au PS[83]. La communication avec les électeurs et les grands médias s'est portée sur des dispositifs plus traditionnels, tels que les *riposte-parties*[84] ou le porte-à-porte. Et pour cause. Dans les mots du directeur de campagne Web du PS de 2012 : « *Un travail sur les bases de données, sur le nombre de mails collectés, sur les taux de clics, sur les transfo en bases de données, etc. Le niveau de couverture de la presse* […] *ce n'est pas très sexy. Pas très sexy à expliquer, à raconter*[85] ».

La crainte de se voir reprochée par la CNIL la mauvaise utilisation des données personnelles des électeurs et l'absence de volonté politique de la publier expliquent le peu d'écho médiatique de ce début de raffinement de l'analyse la donnée avant et pendant les élections de 2012. Cela explique également que la CNIL n'en ait visiblement pas pris connaissance : sa recommandation de 2012, parue quelques mois avant la tenue effective des élections présidentielles de la même année, envisage et autorise expressément la communication politique ciblée, sans pour autant innover ou nuancer davantage sa doctrine déjà présentée en 2006.

Paragraphe 2 – Un cadre juridique adéquat à la protection des données personnelles des électeurs ?

Malgré les constats dressés, il est légitime de penser qu'il existait, lors des présidentielles de 2012 et même avant, un encadrement juridique robuste de la protection de la communication politique en France.

[82] La data analytics (DA) désigne le processus de collecte, d'organisation et d'analyse de données, souvent en Big data, dans le but de découvrir de nouveaux modèles et en tirer des conclusions et d'autres informations utiles.
[83] A. THÉVIOT, « Les data : nouveau trésor des partis politiques – Croyances, constitutions et usages comparés des données numériques au Parti Socialiste et à l'Union pour un Mouvement Populaire », *Politiques de Communication*, 2016, p. 140.
[84] « 'Riposte-party' : la guerre du web aura-t-elle lieu ? », Le Parisien, 12 avril 2012, consulté en ligne le 02 juin 2021, 21h01.
[85] Extrait de l'entretien de Valerio Motta, directeur du Web du PS accordé à Anaïs Théviot le 21 mai 2012.

En effet, l'article 34-5 du Code des postes et des communications électroniques interdisait dans ses premières versions la prospection directe sans consentement préalable de la personne physique, abonné ou utilisateur, règle qui a été reprise par la Directive 2002/58/CE.

Si ces textes envisageaient au départ la prospection commerciale, la CNIL avait rappelé quelques années auparavant que l'alignement des régimes juridiques encadrant la prospection commerciale et la prospection à caractère politique était de rigueur, d'où sa recommandation de bannir l'approche des électeurs à des fins de communication politique sans leur consentement préalable[86].

Sur le premier degré de raffinement de l'analyse de la donnée des électeurs évoqué dans le paragraphe précédent, la CNIL estimait que l'utilisation de données d'usage (pages visitées, nombre de fois qu'une personne interagit avec un candidat sur Facebook et dans quel moment) requiert également le consentement des internautes, compte tenu de leur caractère sensible[87].

Le Code électoral interdisait la communication au public à des fins de propagande électorale durant la période électorale, ce qui diminuait sensiblement le périmètre de la collecte des données personnelles par les acteurs politiques. Ainsi, d'après l'article L52-1 du Code électoral, dans sa version modifiée par la loi n°2011-412 du 14 avril 2011, l'utilisation à des fins de propagande électorale de tout procédé de publicité commerciale par tout moyen de communication est interdite. Si les candidats peuvent diffuser leurs messages et idées politiques pendant cette période, il ne leur est pas loisible d'acheter d'outils dits *« publicitaires »*, sur un réseau social ou autre moyen de communication.

S'agissant de l'incitation des électeurs à voter à la veille du scrutin, le Conseil constitutionnel, dans le cadre des élections des législatives de 2012, tout en constatant qu'un grand nombre de messages informatiques ayant le caractère de documents de propagande électorale ont été diffusés les 16 et 17 juin, veille et jour de la tenue du second tour, avait rappelé que ces messages étaient à reprocher sur la base de l'article L49 du code électoral, qui interdit la distribution de bulletins, circulaires et d'autres documents à la veille du scrutin[88].

[86] Délibération CNIL n° 2006-228, du 5 octobre 2006.
[87] Article 8, paragraphe 1, de la loi informatique et libertés alors en vigueur.
[88] Cons. const., 2012-4589 AN, 7 décembre 2012, *A.N., Meurthe-et-Moselle,* cons. 7.

Le Conseil s'est intéressé à plusieurs reprises à la communication politique à des fins de propagande à la veille de la tenue de ces élections : diffusion de courriels aux agents dépendants des assemblées territoriales ; apposition d'affiches électorales hors des emplacements prévus réglementairement à cet effet ou hors des délais fixés par la loi ; distribution de documents ; validité des listes électorales, eu égard au grand nombre de courriers de propagande envoyés par la candidate[89], parmi d'autres sujets. Si le Conseil n'associe pas directement la méconnaissance aux dispositifs pénaux évoqués à des atteintes particulières aux données des électeurs, il semble évident que la contrainte de temps imposée par les articles du Code électoral aux acteurs politiques a des incidences sur le rythme de la collecte et traitement de ces données, ce qui éviterait d'autres dérives plus susceptibles de prendre place à la vie politique.

Et si le Conseil ne remet pas en cause la légitimité des griefs à l'encontre des responsables politiques dans les cas de figure mentionnés, il estimera que ces courriels envoyés ou diffusés en violation des dispositifs légaux, aussi reprochables soient-ils, n'ont pas vocation à atteindre un nombre d'agents territoriaux ou d'électeurs suffisant pour influencer la sincérité de tout le scrutin. La sincérité du scrutin fera objet de la deuxième partie de ce travail, mais il convient de noter dès maintenant cette grille de lecture téléologique adoptée par le Conseil selon laquelle une action est en mesure de porter atteinte à la sincérité du scrutin si elle fausse la légitimité de l'expression de la volonté d'une partie conséquente des électeurs.

Avec sa recommandation de 2012[90], la CNIL précise les conditions d'application de ce cadre et les garanties à adopter par les partis, élus et candidats à des fonctions électives lors de la communication par l'intermédiaire de courriers électroniques, de SMS, des réseaux sociaux, des blogs ou des pétitions en ligne.

Lors de la collecte des numéros de téléphone et de l'adresse électronique sur internet (ce qui était déjà fait par la droite et la gauche en France, notamment sur Facebook et Twitter, bien avant que l'affaire *Cambridge Analytica*[91] ne défraye la chronique), la CNIL recommandait que les acteurs politiques recueillent le consentement des personnes, s'ils souhaitent les utiliser aux fins de communication politique.

[89] Cons. const., 2012-4606 AN ; 2012-4622 AN et 2012-4635 AN, rendues le 20 juillet 2012.
[90] Délibération CNIL 2012-020, du 26 janvier 2012.
[91] L'entreprise britannique utilisée par l'équipe de campagne de Donald Trump durant sa campagne pour les présidentielles de 2016 aux États-Unis pour faire de l'extraction des données des électeurs, pour la plupart à leur insu.

Des interdictions existaient aussi pour traiter des données relevant de la consonance des noms des personnes ou sur leur lieu de naissance et ne doit pas faire apparaître les origines raciales ou ethniques.

Dans ce contexte, la CNIL a mis en place, à la veille des législatives et présidentielles de 2012, un observatoire interne des élections, l'objectif étant, parmi d'autres, d'accompagner les partis et les candidats dans la mise en place de leurs opérations de communication politique. Le bilan dressé par l'observatoire à l'issue de ces élections met en évidence les deux points d'attention principaux pour les prochaines élections. En constatant que la prospection par message électronique a concentré l'essentiel des critiques des citoyens[92], la CNIL propose les améliorations suivantes : 1) l'information des destinataires sur les modalités d'exercice des droits reconnus par la loi, et 2) demandes de désabonnement facilitées et prises en compte immédiatement. (« *un clic pour s'abonner, un clic pour se désabonner* »)[93]. Il y est également recommandé que l'origine des données utilisées (fichier de contacts, listes électorales communales ou consulaires, base de données commerciale louée, etc.), la fréquence d'envoi et l'identité des émetteurs de messages (candidat, équipe du candidat, fédération locale, etc.) soient désormais précisés.

Les imbrications entre la communication politique et l'utilisation des réseaux montant d'un cran, le dispositif juridique qui existait jusqu'alors semblait être en mesure de répondre à une partie considérable des atteintes potentielles à la protection des données personnelles des électeurs. Il faudra par la suite essayer de comprendre comment le début de la personnalisation de cette communication conduira à l'accentuation des risques à la protection de ces données.

Section 2 – Le début de la granularisation de la communication politique – vers l'accentuation des risques pour les données personnelles des électeurs

Les acteurs politiques, historiquement orientés à des pratiques liées à collaboration sur le terrain et l'interactivité en personne, retrouveront de la difficulté de se saisir des promesses

[92] Principaux motifs de plaintes reçues par la CNIL pendant les élections de 2012 : réception non sollicitée de messages : 87% ; fréquence excessive des messages : 49% ; problèmes pour se désabonner d'une liste de communication : absence de prise en compte : 70% ; absence de lien de désinscription : 23 % ; présence d'un lien non valide : 7%. *In* 33e Rapport d'activités de la CNIL de 2012, p. 26.
[93] *Id.*, p. 25.

du Web 2.0. La dispute pour l'attention et votes prend sûrement un tournant dans ce nouveau champ de bataille en réseau. Aux méthodes traditionnelles d'approche des électeurs se sont ajoutés d'autres, plus à même de porter un message politique percutant et, donc, d'augmenter l'influence des acteurs sur le débat public. Il convient de s'intéresser par la suite aux premières étapes de granularisation des données employées par les partis, élus et candidats à des fonctions électives à l'heure du Web 3.0 (**Paragraphe 1**), pour s'intéresser dans un deuxième temps aux changements du degré de responsabilisation des acteurs politiques que ces pratiques ont entraîné (**Paragraphe 2**).

Paragraphe 1 – Une technique innovatrice de traitement des données à l'épreuve du Web 3.0

Jusqu'à récemment, les usagers de l'internet consistaient pour la plupart de jeunes gens étant à peine débarqués sur l'environnement numérique lors qu'ils avaient affaire à des impératifs académiques ou professionnels. Aujourd'hui, plus de 50% de la population mondiale connectée est née sur un monde branché au web. En 2010, la plupart des usagers de l'internet était déjà des *digital natives*[94].

L'intérêt de la communauté scientifique pour l'intelligence artificielle a été galvanisé à ce moment, comme le rappelle l'un des pionniers du sujet et professeur à l'université de New York Yann LeCun[95]. Grâce à l'apparition d'ordinateurs à puissance de calcul conséquente et de bases de données suffisamment grandes pour les entraîner, les algorithmes refont la une des journaux pour leurs applications innombrables et leur pouvoir de granulariser la donnée.

Par granularisation, il emporte de comprendre l'extraction, séparation ou l'analyse de la donnée pour en faire des sous-parties individualisables et catégorisables, à des degrés variables selon les techniques algorithmiques employées.

---

[94] « *Digital natives are the people born since the turn of the century in countries where device networks are a ubiquitous part of social life* » *In* S. C. WOOLEY ; P. N. HOWARD, « Political Communication, Computational Propaganda, and Autonomous Agents », *International Journal of Communication 10*, 2016, p. 3.

[95] « *On parle de révolution parce que jusque dans les années 2010, les techniques utilisées étaient relativement simples. En quelques mois, les groupes qui travaillaient sur la reconnaissance de la parole ont changé les méthodes. Cela a été une révolution qui m'a moi-même surpris par sa rapidité surprenante* », *in* « Prix Turing : le Français Yann LeCun couronné avec deux autres pionniers de l'intelligence artificielle » *France Culture*, 27 mars 2019, consulté en ligne le 05 avril 2021.

« *Le problème, ce sont les fichiers* »[96]. Il s'est avéré très tôt dans le paysage politique français que l'utilisation des fichiers informatiques pourrait porter atteinte à la liberté de choix, voire même de conscience, des électeurs, si des techniques élaborées d'analyse de la donnée étaient employées pour établir de la communication politique. L'ancienne ministre de l'écologie Nathalie Kosciusko-Morizet, auteur de la phrase suscitée, avait attiré l'attention des acteurs politiques sur l'utilisation que le PS souhaitait faire des listes électorales lors des primaires citoyennes présidentielles de cette année.

L'UMP avait à cette occasion essayé d'interdire la collecte d'adresses mail par le PS en recadrant la pratique du parti rival comme du « fichage » d'électeurs. En misant sur l'argument reposant sur les atteintes potentielles à la liberté de choix des électeurs, Jean-François Copé lui emboîte le pas pour indiquer que « *Dans les villes socialistes, vous imaginez les conséquences pour les agents municipaux ou les présidents d'association qui ont des subventions, s'ils ne participent pas à cette parodie d'élection* ?[97] ».

Dans le même temps, la doctrine de la CNIL avait précisé que le simple enregistrement des données personnelles saurait déjà être pris comme un traitement « sensible » puisque susceptible de révéler l'opinion politique, réelle ou supposée, des personnes concernées[98]. Cette interdiction, assortie de l'obligation des acteurs politiques de radier les listes d'adresse mail des électeurs après un scrutin donné, avait pour but d'éviter que ces acteurs identifient indirectement l'orientation politique des électeurs. Munis de cette information indéfiniment, ces acteurs seraient à même d'entreprendre des campagnes ciblées à des effets incalculables pour les droits et libertés des électeurs, notamment la vie privée et la liberté de conscience, d'où l'opportunité juridique de la précision de la CNIL.

La rationalisation du porte-à-porte par les équipes de campagne lors des régionales de mars de 2010 et ensuite nationales de 2012 a été le point de départ de l'utilisation de la science des données et du Big data dans la communication politique en France[99]. Trois étudiants[100] issus de prestigieuses universités américaines à Boston, experts du Big data, mettent au profit du PS leur expérience acquise en œuvrant pour la campagne d'Obama en 2008. En se prévalant de

[96] « Primaire socialiste : l'UMP s'inquiète de nouveau de l'usage des listes électorales *», Le Monde,* 19 juin 2011, consulté en ligne le 05 avril 2021, 10h40.
[97] *Id.*
[98] Guide CNIL « Communication Politique – Obligations Légales et Bonnes Pratiques. », 2012, p. 6.
[99] A. THÉVIOT, « *Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter* », Le Bord de l'Eau, 2019, p. 121.
[100] Guillaume Liegey, Arthur Muller et Vincent Pons, créateurs de l'entreprise Liegey Muller Pons.

fichiers comme la liste électorale, les Bostoniens ont repéré les zones à fort taux d'abstention de personnes susceptibles de voter pour la gauche, pour leur adresser des mails ciblés ou déterminer des conditions optimales de réalisation du porte-à-porte.

En tant que forme de militantisme, le porte-à-porte ne constitue pas une nouvelle pratique de communication politique. Ce qui change en 2012 est l'ouverture de la stratégie à un nombre considérable de potentiels militants (non seulement les adhérents du PS) et l'application des techniques marketing redorées par les Bostoniens, qui ont donné à la militance des informations précieuses en amont sur les personnes à visiter et leurs habitudes.

C'est ainsi que, avec la donnée collectée concernant les personnes à visiter, les Bostoniens et les chefs de campagne du PS ont encadré sensiblement au préalable le parcours des entretiens des militants, avec l'objectif de toucher le plus rapidement au but en fonction des personnes visitées[101].

Le porte-à-porte ciblé aurait permis une accentuation de l'engagement des électeurs des DOM et d'ascendance maghrébine, indiquant que dans ce groupe, il « *a permis de convaincre un abstentionniste sur neuf d'aller voter* »[102]. Le résultat aurait cependant été nul chez les autres électeurs.

Depuis lors, les experts du Big data électoral français sont passés d'une forme d'amateurisme à un degré de professionnalisation plus accentué, avec des acteurs qui proposent des logiciel à de typologies et prestations variables.

À la veille des différentes échéances électorales, et compte tenu de l'exploitation montante de données disponibles dans les réseaux à l'appui des logiciels de stratégie électoral, la doctrine de la CNIL est mise à jour pour tenir compte de ces avancées technologiques. Dans sa recommandation de 2016, l'autorité va préciser l'obligation créée par l'article 34-5 du Code des postes et des communications électroniques, en estimant que la collecte massive des données issues des réseaux sociaux n'est pas non plus légale en l'absence d'information des personnes concernées et sans leur avoir donné la possibilité de s'opposer à cette collecte[103].

[101] *Id.*, p. 125.
[102] J. TALPIN, R. BELKACEM, *Op. cit.*, p. 192.
[103] « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? », site internet officiel de la CNIL, 8 novembre 2016, consulté le 10 avril de 2021, 20h38.

Si la publicité des données personnelles sur les réseaux se prêtait à des hésitations de la part des fournisseurs des logiciels et des équipes de campagne, la CNIL précise que le caractère « public » des données disponibles sur les réseaux sociaux ne leur fait pas perdre le statut de données personnelles, en jetant davantage de clarté au sujet : « *si leur simple consultation est toujours possible, le traitement de ces données (extraction, enregistrement, utilisation, enrichissement, etc.) est soumis à l'ensemble des conditions prévues par la loi informatique et libertés* ». Cela réoriente la pratique des prestataires de logiciel qui se prévalaient des données personnelles des réseaux pour en proposer ses services.

L'autorité de contrôle s'est même intéressé à la manière dont les personnes doivent être informées sur les conditions de traitement de leurs données, en précisant que des onglets « politique vie privée » doivent être intégrés sur les pages dédiées aux candidats ou partis de ces réseaux sociaux. Aussi critiquables soient ces précisions, il convient de rappeler que, dans ces recommandations, la CNIL se permet d'habitude d'aller au-delà de la lettre de la loi pour préciser la manière de sa mise en œuvre le plus justement possible à ses destinataires.

Avec ces nouveaux outils de stratégie électoral, il est désormais possible de granulariser non seulement l'analyse des données déclaratives des profils (nom, prénom, profession et d'autres données renseignées), mais également de quelques métadonnées de navigation des internautes (moment, fréquence d'interaction de la personne avec le candidat, pages visitées, etc.).

Parallèlement à sa recommandation de 2016, la CNIL et le Conseil supérieur de l'audiovisuel publient un guide pratique élaboré conjointement, l'objectif étant de rappeler aux acteurs politiques les principes élémentaires des lois relatives à la liberté de communication, applicable aux médias audiovisuels, et à la protection des données personnelles, pour les fichiers mis en œuvre par les candidats ou partis politiques[104]. Des questions de pluralisme dans les médias audiovisuels et des règles Informatique et Libertés ont aussi été traitées dans le même support.

[104] 37e Rapport d'activités de la CNIL de 2016, p. 72.

Les problématiques et enjeux pour les libertés individuelles entourant les logiciels de stratégie électorale seront approfondies dans la deuxième partie de notre travail.

Enfin, l'absence d'actualisation législative importante au sujet de la communication politique jusqu'à l'avènement du RGPD est à souligner. Alors même que d'autres dispositifs ont pu avoir une incidence sur la matière depuis la loi du 6 août 2004 (dernière actualisation importante), cette incidence s'est avérée moindre. Cela a malheureusement diminué le périmètre d'action de la CNIL, qui s'est vu en partie démunie d'un pouvoir réglementaire plus effective sans un cadre normatif justifiant son recadrage. Ainsi, des sujets comme la complexification du marché de courtage de données personnelles et les données personnelles inférées, à forts enjeux pour la communication politique, ont été partiellement délaissés par la première vague législative sur la protection des données à caractère personnel.

Il appartient maintenant d'apporter de la lumière au recadrage des responsabilités des partis, élus et candidats à des fonctions électives que le Web 2.0 et 3.0 auront entraîné.

Paragraphe 2 – La responsabilité changeante des acteurs politiques

La responsabilité des acteurs politiques concernant le traitement de la donnée personnelle peut être facilement saisie par la notion de responsable de traitement. En 2004, lors de la transposition de la Directive 95/46/CE, le dispositif européen instituant la figure du responsable de traitement est entré en vigueur en France, attirant les partis politiques, élus et candidats à des fonctions électives à son champ d'incidence.

Selon ce texte, le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel[105]. Or, dans la mesure où les partis politiques, élus et candidats à des fonctions électives déterminent les moyens (par exemple financiers, de format des fichiers, étendue de leur circulation, public-cible, etc.) et les finalités du traitement (faire de la communication politique), ils tombent sous le champ d'application de cette figure juridique.

[105] Article 2, alinéa « d » de la Directive de 1995, repris sans modifications importantes par l'Article 4, paragraphe 7, du RGPD.

Le législateur européen attribuera[106] aux États-membres l'obligation de déterminer le périmètre juridique de cette responsabilité, stipulant que ceux-ci prévoient les mécanismes pour réparer les dommages subis par les personnes concernées en raison d'un traitement illicite. Le considérant 55 a par ailleurs apporté des balises importantes à l'action des États-membres, en imposant d'une part qu'une loi (et pas n'importe quel acte juridique) prévoie un recours juridictionnel en cas de non-respect des droits des personnes concernées par le responsable du traitement, et d'autre part que les dommages qu'elles subissent du fait d'un traitement illicite soient réparés par celui-ci. Ce considérant faisait foi de ligne directive – étant donc dépourvu de force normative – destinée aux États-membres pour la mise en œuvre du dispositif européen[107].

La loi du 6 août de 2004, en mettant en œuvre les innovations apportées par le droit européen, change la loi informatique et libertés afin de confier à la CNIL le pouvoir d'avertir et mettre en demeure le responsable du traitement méconnaissant les obligations découlant de la loi[108], et de demander, par référé, le juge compétent d'ordonner les mesures de sécurité nécessaires à la sauvegarde des droits et libertés des personnes concernées. Désormais, selon l'article 34 révisé de la loi, le responsable du traitement est également tenu de prendre les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Avec sa recommandation de 2012, la CNIL met à jour sa doctrine pour préciser davantage les contours de la figure du responsable de traitement appliquée à la communication politique. L'autorité estimera que lorsque les acteurs politiques font appel à un support de communication en ligne – réseau social, ou blog – à des fins de prospection politique, collecte et utilisation de données à caractère personnel, ils deviennent en effet responsables de traitement et doivent alors en assumer toutes les obligations[109].

[106] Article 23 de la Directive 95/46/CE
[107] Outre la figure du responsable de traitement, les acteurs publics et privés disposaient depuis 2004 d'un « outil » privilégié pour se prémunir des risques liés au développement des TIC : le Correspondant Informatique et Libertés (CIL), figure assimilable à celle du Délégué à la protection des données personnelles. Sous la logique déclarative d'avant RGPD, la désignation d'un CIL permettait aux responsables de traitement de bénéficier d'un allègement conséquent des formalités préalables au traitement. L'organisme pourrait ainsi être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants s'il en désignait un, à l'exception des traitements des données sensibles.
[108] Article 45 de la loi informatique et libertés, modifié par loi n°2004-801 du 6 août 2004.
[109] Délibération CNIL 2012-020, du 26 janvier 2012.

Par ailleurs, il faudrait noter que la responsabilité de traitement continue d'être appréhendée notamment sous l'angle du détournement de finalité jusqu'à ce moment. Aux élections municipales de 2014[110], quatre plaintes sont portées à la CNIL contre le directeur du Théâtre national de Bretagne (TNB), qui aurait utilisé la liste de courriers électroniques des abonnés du théâtre pour leur envoyer un message de soutien à la politique culturelle de l'équipe municipale sortante. Il s'agissait, pour la CNIL, d'un détournement de la finalité de la gestion des coordonnées des abonnés, le traitement des adresses de messagerie électronique des abonnés au TNB n'étant autorisé au départ que pour la gestion de leurs abonnements et l'envoi d'informations culturelles. Celle-ci prononce donc un avertissement public à l'encontre du TNB[111], qui est confirmé par le Conseil d'État par la suite (CE, 28 sept. 2016, n° 389448).

Le détournement de finalité du traitement des données personnelles constitue en outre une infraction pénale passible de 5 ans d'emprisonnement et 300 000 euros d'amende (Code pénal, Article 226-21). L'effectivité de ce dispositif reste pour autant à vérifier, vu la pratique de ne pas poursuivre le responsable de traitement pénalement dans des cas pareils, qui semble se perpétuer[112].

Dans un autre registre, la CNIL adresse en 2016 un avertissement public au PS, pour un manquement à la sécurité de son application d'adhésion en ligne : n'importe qui pouvait accéder à la base de plusieurs dizaines de milliers de primo-adhérents, contenant notamment leur identité, adresse, numéros de téléphone, adresse IP, moyen de paiement et le montant de leur cotisation au parti. En outre, les données des adhérents – sur la base depuis 2010 – étaient conservées sans limitation de durée. Dans les motifs de sa décision, l'autorité s'appuie notamment sur l'article 34 précité de la loi informatique et libertés, en suggérant que c'était l'obligation de sécurité des données inscrite dans cet article qui aurait justifié la décision pour l'avertissement public[113].

---

[110] En 2014, pour les élections municipales, l'Observatoire des élections a reçu 150 témoignages dont 133 ont abouti à des plaintes. Selon le site internet officiel de l'Observatoire, la prospection par e-mail était la manière la plus concernée par ces plaintes (65% du total) et plus précisément l'origine des données utilisées (47,5%). Même si la CNIL y remarque que des contrôles ont été réalisés, des partis politiques et des candidats ont été mis en demeure de répondre aux demandes d'opposition et que des sanctions ont été prononcées Les rapports d'activité les plus récents produits par l'autorité ne nous apportent davantage de clarté au sujet de ces contrôles.

[111] Délibération de la formation restreinte CNIL n° 2015-040, du 12 février 2015. La loi Lemaire (n° 2016-1321, du 7 octobre 2016) étend le périmètre d'action de la CNIL pour lui confier désormais le pouvoir de d'avertir les responsables de traitement, de les imposer une sanction pécuniaire ou les enjoindre à cesser le traitement pour une durée maximale de trois mois.

[112] A. D. FATÔME, « Principe de finalité du traitement - Un office public de l'habitat rappelé à l'ordre par la CNIL et le Conseil d'État ! » Commentaire 92, *Communication Commerce électronique n° 12*, Décembre 2020.

[113] Délibération CNIL n° 2016-315, du 13 octobre 2016.

Il est à noter finalement la difficulté de retracer l'histoire récente des contrôles réalisés par la CNIL sur les activités des acteurs politiques, en raison notamment de l'absence de publicité de quelques avertissements, sanctions et d'autres actes pris par l'autorité de contrôle envers ces acteurs. Si la vie privée des personnes et la faible répercussion de certaines affaires peuvent justifier la décision de la CNIL de ne pas les rendre publiques, il semble que l'intérêt sous-jacent de ces décisions pour la formulation de politiques publiques plus protectrices des droits des électeurs s'impose. Le manque de publication des bilans et recommandations dressés par l'Observatoire des élections mis en place par la CNIL en 2012 affaibli en égale mesure la portée des critiques que la littérature juridique pourrait dresser à ce sujet. La vie privée des personnes pourrait par exemple être protégée par le biais de l'anonymisation des avertissements et sanctions.

***

Dans cette première partie, il a été mis en avant la manière dont les partis, élus et candidats à des fonctions électives se sont emparés des techniques traditionnellement consacrées par le débat politique pour s'approcher et entretenir avec les électeurs un contact à des fins politiques. À l'aide des outils de technologie d'information et communication changeants, le contact avec les électeurs a subi des redressements importants, ce qui n'a pas été sans incidence sur l'encadrement juridique de la communication politique. Dans la deuxième partie de l'étude, l'accent sera mis sur les nouvelles techniques de prospecter et fidéliser les électeurs et les effets que la personnalisation de la communication politique aura pour la protection des données personnelles des électeurs.

DEUXIÈME PARTIE

LA PERSONNALISATION DE LA COMMUNICATION POLITIQUE : UNE NOUVELLE STRATÉGIE AUX EFFETS DÉCUPLÉS POUR LA PROTECTION DES DONNÉES PERSONNELLES DES ÉLECTEURS

Depuis les années 2010, les réseaux sociaux prennent le dessus sur les autres moyens traditionnels de communication pour devenir le principal théâtre du débat politico-électoral. Facebook, Twitter et des blogs politiques constitueront désormais non seulement la caisse de résonance des attentes et mécontentements de l'électorat, mais aussi le point de connexion le plus logique et efficace pour entretenir des contacts directs et réguliers entre les électeurs et les partis politiques, élus et candidats à des fonctions électives. Cette nouvelle manière de communiquer, en temps réel, plus agile et horizontale, dont se prévalent les acteurs politiques pour prospecter et fidéliser des électeurs, se traduit par un besoin de connaissance plus raffiné, granularisé des envies des électeurs. C'est avec les logiciels de stratégie électorale que la promesse de parler presque individuellement aux électeurs, en prenant en considération les circonstances particulières des interlocuteurs des acteurs politiques, va en partie se réaliser **(Chapitre 1)**. Cette approche, plus personnelle, ne sera pas sans incidence sur la protection des données à caractère personnel des électeurs et, plus largement, sur la vie privée de ces derniers **(Chapitre 2)**.

CHAPITRE 1 – UNE NOUVELLE STRATÉGIE DE CIBLAGE ÉLECTORAL ANCRÉE SUR L'UTILISATION DES LOGICIELS DE STRATÉGIE ÉLECTORALE

La deuxième vague législative européenne et française de protection des données à caractère personnel, inaugurée à l'heure du Web sémantique, où la puissance algorithmique rejoint les données en *Big data*, avait vocation à renforcer le cadre juridique précèdent par la création de nouveaux droits aux personnes concernées et l'élargissement de l'étendue de leurs garanties. Le droit à la protection des données à caractère personnel, élevé au rang de droit fondamental par le droit européen, jouit désormais d'un statut juridique particulier, retrouvant des échos importants dans la communication politique **(Section 1)**. Cet effort législatif est d'emblée remis en question par les bouleversements technologiques et des modèles de business adoptés par les parties prenantes de cette communication **(Section 2)**.

Section 1 – Le renouveau impératif du cadre juridique à l'heure de la personnalisation du ciblage électoral – Acte II

L'autonomisation du cadre juridique de la protection de la donnée personnelle à la fin du XX^{e} siècle en Europe s'est largement bâtie pour permettre aux citoyens de garder la main sur l'activité informatique montante, dont les effets pour les droits et libertés individuels étaient inconnus. Plus récemment, une nouvelle couche normative s'est ajouté à ce dispositif juridique, remplaçant en partie l'ancienne, renforçant la protection des données personnelles des citoyens et des électeurs (**Paragraphe 1**). C'est dans ce contexte que les techniques d'approche des électeurs connaissent un renouveau significatif avec les logiciels de stratégie électorale (**Paragraphe 2**).

Paragraphe 1 – Le dispositif européen et français renouvelé

L'affaire Cambridge Analytica[114] a-t-elle sonné le glas d'un temps faible de la protection des données personnelles dans le contexte du ciblage à des fins électorales ? La question est complexe et mérite d'être contextualisée.

[114] Selon l'autorité de la concurrence américaine (FTC), durant l'été de 2014, Alexandr Kogan, alors *data scientist* collaborateur de l'entreprise d'analyse de données Cambridge Analytica, aurait développé, utilisé et analysé les données obtenues à partir d'une l'application. Ces données auraient ensuite été utilisées pour entraîner un algorithme qui générait des scores de personnalité pour les utilisateurs de l'application et leurs amis Facebook. Cambridge Analytica et Kogan faisaient ainsi correspondre ces scores de personnalité avec les dossiers des électeurs américains, ce qui aurait permis à l'entreprise d'utiliser ces scores pour ses services de profilage des électeurs et de publicité ciblée.

Il faut tout d'abord savoir que l'utilisation des données par les acteurs politiques est apparue depuis longtemps comme technique performante pour cibler les électeurs et ainsi réduire l'incertitude entourant le résultat des élections[115].

Dès 2005, la Résolution concernant l'utilisation de données personnelles dans le cadre de la communication politique adoptée à Montreux[116] évoquait l'idée de personnalisation de la communication adressée aux électeurs. Néanmoins, ce n'est qu'à la fin des années 2000 aux États-Unis et début des années 2010 en Europe, que les techniques de ciblage électoral se sont perfectionnées, largement à l'appui des logiciels de stratégie électorale.

Lors des élections législatives et présidentielles françaises de 2017, le niveau de professionnalisation des entreprises fournissant ces logiciels[117] leur a permis de les offrir encore plus justes, précis et en phase avec les attentes des acteurs politiques. Cela a conduit, dans un premier temps, à un recadrage du paysage de la communication politique dans le monde, qui ne sera plus constitué uniquement des acteurs sociaux traditionnels, à savoir, les partis politiques, les élus et candidats à des fonctions électives, les plateformes de réseaux sociaux, les groupes d'intérêt et les courtiers en données[118]. Désormais, il comprend également les fournisseurs de ces solutions, qui ont un poids stratégique grandissant pour les campagnes politiques modernes. Il s'est suivi à la parution de ces logiciels, dans un deuxième temps, la réallocation optimisée de ressources financières et humaines engagées par les acteurs politiques dans les campagnes électorales, autant en ligne que sur le terrain.

Lors de sa première utilisation[119], le microciblage électoral se voulait un moyen de personnaliser des messages à des fins politiques, plus particulièrement pour sensibiliser les

---

[115] Des travaux socio-historiques récents témoignent d'un recours croissant à des instruments d'analyse des données produites et recensées à la veille et durant les élections politiques. Au XIX[e] siècle, la circulaire confidentielle du 28 juin 1820 recommandait aux préfets de classer chaque électeur d'après ses opinions, en observant des différences de coloration politiques existantes à l'époque (royalisme constitutionnel, royalisme pur et ultra-royalisme). En 1848, travail de ciblage est devenu plus complexe avec l'ouverture du suffrage et s'est ensuite enrichi de nouveaux outils au fil du temps, notamment au début de la montée en importance des sondages dans les années 1960.

[116] « *Whereas there is invasive profiling of various persons who are currently classified (...) as sympathizers, supporters, adherents or party members, in order to increase personalized communication to groups of citizens* », *in* Résolution sur l'utilisation des données à caractère personnel à des fins de communication politique, Montreux, Suisse, du 14 au 16 septembre 2005.

[117] A. THÉVIOT, « Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter », *Le Bord de l'Eau*, 2019, p. 7.

[118] Déclaration 02/2019 sur l'utilisation de données personnelles dans le cadre des campagnes politiques, adoptée le 13 mars 2019 par le Comité Européen de la Protection des Données.

[119] « *Le concept de* Microtargeting *(micro-ciblage), développé par le cabinet d'études TargetPoint Consulting a été utilisé pour la première fois par l'équipe de campagne de George Bush en 2004* », *in* E. BARQUISSAU, L. SCHLENKER *Op. cit.*, p. 257 à 292.

électeurs aux appels des chefs de campagne de George Bush. Il a connu un renouveau dans les années 2010, avec les techniques de raffinement d'analyse de la donnée permises par les algorithmes.

Par microciblage, l'autorité de contrôle des données personnelles britannique (*the Information Commissioner's Office*, ou ICO)[120] comprend une forme de publicité ciblée en ligne qui analyse les données personnelles pour identifier les intérêts d'un public ou d'un individu spécifique afin d'influencer leurs actions[121]. Le microciblage peut être utilisé pour offrir un message personnalisé à un individu ou à un public utilisant un service en ligne tel que les médias sociaux.

Typiquement, cette manière de cibler des intéressés fait appel à quatre modalités de données personnelles susceptibles d'être mises à dispositions sur internet : 1) les informations de profil des utilisateurs sur la page personnelle des réseaux sociaux, blogs et d'autres sites, telles que le nom, profession, niveau d'études, âge ; 2) les traces des activités sur ces plateformes – likes, les partages de contenu, commentaires, informations sur les groupes rejoints ; 3) les informations tenant à l'activité passive des utilisateurs – pages visités et temps de visitation ; et 4) la géolocalisation des appareils utilisés pour naviguer.

Il convient de relever que le ciblage et le microciblage électoraux peuvent, mais ne doivent pas, faire appel aux données à caractère personnel pour fonctionner, d'autres modalités de données, non personnelles, étant souvent utilisées dans le cadre des stratégies de campagne.

Cette digression introductrice faite, revenons à l'objet du paragraphe.

Le RGPD, entré en vigueur le 24 mai 2016, a en effet inauguré la deuxième vague législative européenne et française de protection des données à caractère personnel. Le texte, largement discuté avec la société civile depuis 2012, confie de nouveaux droits[122] aux personnes concernées, tout en renforçant les garanties des droits acquis.

[120] Le terme n'est apparemment pas défini en tant que tel par la législation européenne et française relative à la protection des données personnelles ni par les recommandations de la CNIL jusqu'à la date de ce travail.
[121] « *What is microtargeting* », site internet officiel de l'autorité de contrôle britannique de la protection des données personnelles, site internet officiel de l'ICO, sans date, consulté en ligne le 9 mai 2021 à 21h10.
[122] Notamment le droit à la limitation du traitement et à la portabilité des données.

À propos de ces droits, il semble que le principal changement concerne le droit d'opposition (Article 21 du RGPD). D'une part, contrairement à ce qui était prévu par le régime juridique antérieur, le nouveau dispositif supprime l'obligation de fonder la demande d'opposition sur des motifs légitimes. Dorénavant, de simples raisons tenant à la situation particulière du demandeur sont suffisantes pour mobiliser ce droit auprès du responsable de traitement. D'autre part, le RGPD opère un basculement important dans la logique sous-jacente d'exercice de ce droit, dans la mesure ou désormais c'est le responsable de traitement qui doit supprimer les données en absence de « *motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée* ».

Or, de tels changements ont vocation à favoriser l'exercice de ce droit par les électeurs, lequel, selon l'Observatoire des élections, était parfois mis à mal depuis quelques années[123]. Enfin, il reste à déterminer si les motifs légitimes et impérieux évoqués précédemment peuvent être assimilés à des « motifs d'intérêt public » à des fins du considérant 56 du RGPD, pour justifier légitimement le traitement des données concernant les opinions politiques des électeurs.

Il faut aussi savoir que le règlement prévoit une disposition spécifique relative aux données à caractère personnel traitées à des fins de prospection. L'article 7 du RGPD précise que lorsque le traitement repose sur le consentement, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. Cela impose, pour les partis, élus et candidats à des fonctions électives, à documenter le consentement collecté auprès des électeurs et d'autres personnes pour le traitement de leurs données personnelles. La nouvelle réglementation apporte aussi une disposition spécifique relative aux données personnelles traitées à des fins de prospection. Il est ainsi expressément prévu par l'article 21 que la personne concernée est en droit de s'opposer à tout moment au traitement de ces données pour une telle finalité[124].

[123] La CNIL remarque que des contrôles ont été réalisés auprès des partis politiques pour les élections municipales de 2014. Des partis politiques et des candidats ont été mis en demeure de répondre aux demandes d'opposition et que des sanctions ont été prononcées.

[124] Comme vu précédemment, la doctrine juridique de la CNIL d'avant le RGPD était pour l'alignement des régimes encadrant la prospection commerciale et la prospection à caractère politique, ce que nous autorise à croire que l'article 21 du RGPD s'applique aux deux modalités de prospection, et en égale mesure.

Si le consentement demeure une des bases de licéité du traitement des données des électeurs sous la nouvelle règlementation, le considérant 56 du RGPD[125] indique que des motifs d'intérêt public peuvent justifier le traitement des données concernant les opinions politiques des personnes concernées par les partis politiques dans le cadre des activités liées à des élections. Ces deux bases de licéité ont été positivées à l'article 6, paragraphe 1, alinéas « a » et « e » du RGPD[126].

Le régime d'interdiction par défaut de traiter des données relevant des opinions politiques a été maintenu par cette nouvelle règlementation, alors même que des dérogations peuvent toujours profiter aux acteurs politiques. Des exceptions comme le consentement de la personne concernée et le traitement des données dans le cadre des activités légitimes des organismes poursuivant une finalité politique peuvent être utilisés par ces acteurs pour traiter des opinions politiques[127]. Dans cette dernière hypothèse, le traitement doit se rapporter exclusivement aux membres ou aux anciens membres de ces organismes ou aux personnes entretenant avec ceux-ci des contacts réguliers en liaison avec ses finalités.

À relever, à cet égard, le manque de précision de l'expression « organismes poursuivant une finalité politique ». S'il est, d'une part, certain que son champ d'incidence recouvre les partis politiques, il est d'autre part moins sûr qu'il recouvre également les élus et des candidats à des fonctions électives. La règlementation de la CNIL serait la bienvenue pour y apporter de la lumière, au vu des fortes implications que le traitement des opinions politiques peut avoir pour l'exercice de la démocratie durant la période électorale[128].

---

[125] Ce considérant reprend globalement le texte du considérant 36 de la Directive 95/46/CE.

[126] Pour une partie de la littérature, à l'instar de l'article 6 du RGPD, qui apporte les bases de licéité « classiques », l'article 9 disposerait qu'il ne peut y avoir de traitement de données sans base juridique « spéciale » comme le consentement explicite. Les règles de la Directive de 2002 (*e-Privacy*), qui prévoiraient une base juridique unique « alternative », visent indistinctement toutes les informations recueillies sur les équipements terminaux des internautes sans différencier donnée sensible et donnée non sensible. En tant que loi spéciale ne faisant pas de distinction, il n'en faudrait pas faire en vertu de la loi générale, ce qui suggèrerait que le consentement donné sous l'égide de la Directive « *e-Privacy* » aurait vocation à couvrir les données sensibles et les données non-sensibles. *In* L. DUBOIS ; F. GAULLIER, « Publicité ciblée en ligne, protection des données à caractère personnel et e-Privacy : un ménage à trois délicat », *Legicom*, 2017, pp. 69 à 102.

[127] Article 9, paragraphe 2, du RGPD.

[128] À titre de curiosité, l'autorité de contrôle britannique, ICO, estime que le traitement des données relevant de l'opinion politique devrait identifier une base de licéité relevant de l'article 6 et une autre base de licéité relevant de l'article 9 du *Data Protection Act* de 2018 pour pouvoir légitimement traiter les opinions politiques. Dans le même sens, les Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, adoptées par le G29 (aujourd'hui Comité Européen de la Protection des Données) le 3 octobre 2017, et révisées le 6 février 2018 (p. 16). Cette contrainte à deux temps n'pas apparemment été suivie par la CNIL pour ce qui est spécifiquement du traitement des opinions politiques.

La sensibilité des données relatives aux opinions politiques, dont le traitement est susceptible par nature de porter atteinte aux libertés fondamentales ou à la vie privée[129], justifie en effet qu'une vigilance particulière soit portée aux conditions dans lesquelles il est possible d'utiliser de telles données. La loi informatique et libertés imposait déjà l'interdiction par défaut de collecter et de traiter ce type de données, même avant la Directive 95/46/CE.

Pour ce qui est de la personnalisation de l'approche des électeurs que le profilage rend possible, il faut se rappeler que, lorsque les acteurs politiques utilisent des logiciels de stratégie électorale pour traiter les données personnelles des électeurs, ils le font en tant que responsables de traitement. Il en ira de même lorsqu'ils le font à l'appui d'un logiciel de stratégie électorale développé par des tiers, comme des *civic techs, et* des *pol techs*[130]. Cette utilisation pourrait, éventuellement, attirer l'application de l'article 22 du RGPD, qui pose le droit des électeurs de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, si le traitement en cause produit des effets juridiques sur ou affecte de manière significative les électeurs. L'analyse des enjeux du profilage dans la communication politique sera nuancée dans un deuxième moment de cette étude.

À la suite de l'affaire Cambridge Analytica, un autre règlement portant création d'une procédure de vérification de l'intégrité des élections européennes a été acté par le Parlement européen et le Conseil visant les partis politiques européens et fondations politiques européennes qui porteraient atteinte aux règles en matière de protection des données à caractère personnel en vue d'influencer le résultat des élections au Parlement européen. Le Règlement UE 2019/493, du 25 mars 2019, constitue ainsi règle spéciale vis-à-vis du RGPD, applicable dans le contexte des élections européennes.

Au titre de ce dernier, les partis et fondations politiques européennes peuvent se voir imposer des amendes financières correspondantes à un pourcentage fixe du budget annuel du parti ou fondation politique européenne concernée[131].

[129] É. SERUGA-CAU ; T. HAVEL, « Campagne Électorale et Utilisation des Données Personnelles : Grands Principes et Points de Vigilance », *Actualité Juridique Collectivités Territoriales*, Février 2019, p. 73.
[130] « Civic tech : la CNIL appelle à la vigilance », *Le Monde,* 9 décembre 2019, consulté en ligne le 11 mai 2021, 00h56.
[131] Article 27, paragraphe 4, alinéa « a » du Règlement UE/Euratom 1141/2014, tel que modifié par le Règlement UE 2019/493.

Le dispositif national a aussi évolué sous l'impulsion du renouveau du droit européen. La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, portant sur l'adaptation des dispositions de la loi informatique et libertés au RGPD, a élargi les pouvoirs d'enquête et contrôle de la CNIL, renforçant ainsi le pouvoir de vigilance de celle-ci sur les traitements mis en œuvre par les acteurs de la communication politique en France. Cette loi a également interdit la réalisation du profilage des personnes concernées à l'appui des données sensibles[132] dans l'hypothèse où le profilage entraîne des discriminations à l'égard des personnes physiques. Cette loi a été suivie par le Décret n° 2019-536, du 29 mai 2019, pris pour l'application de la loi informatique et libertés, son objectif principal étant d'améliorer la lisibilité du cadre juridique national et de le mettre en cohérence avec le droit européen.

La protection des données personnelles des électeurs étant de nouveau renforcée par la deuxième vague législative sur la matière, il convient désormais de comprendre quel rôle jouent les logiciels de stratégie électorale dans la personnalisation de la communication politique, à l'aune du cadre juridique évoqué.

Paragraphe 2 – Les logiciels de stratégie électorale et la personnalisation du ciblage électoral

« *La campagne présidentielle française de 2017 a révélé aux yeux du grand public toute l'ampleur d'un aspect souvent ignoré de la '*révolution numérique*'. Pour la première fois, l'ensemble des candidats ou presque a clairement assumé le fait de mener une campagne électorale où les agences de stratégie numérique se sont imposées comme un élément incontournable* »[133].

Il a été soulignée précédemment que les acteurs politiques, par crainte de se voir reprocher par une mauvaise utilisation des données personnelles, ont choisi de ne pas médiatiser l'utilisation des outils de raffinement des données durant la campagne présidentielle de 2012. La timidité de 2012 a fait de la place à l'utilisation ouverte en 2017, malgré les hésitations sur le nombre des candidats aux présidentielles de cette année ayant y adhéré[134].

[132] Innovation que se retrouve aujourd'hui à l'article 95, paragraphe 3, de la loi informatique et libertés.
[133] M. BARDIN « Les partis politiques et l'outil numérique. », *Pouvoirs*, 2017, p. 43 à 54.
[134] « Présidentielle 2017 : l'enjeu d'Internet pour les candidats », *Franceinfo,* 14 avril 2017, consulté en ligne le 12 mai 2021, 19h19.

Dès lors, si ces logiciels ne rendent pas obsolètes les techniques traditionnelles d'approche des électeurs, comme le porte-à-porte, le tractage, et la communication non-personnalisée dans les réseaux et grands médias, qui ne faisaient globalement pas appel à des données granularisées en amont, il s'en est suivi un rééquilibrage de l'importance de ces techniques vis-à-vis des autres techniques, technologiquement plus performantes.

Maintenant, l'analyse statistique de la donnée prend l'essor dans les campagnes électorales. Grâce à la scientificité des méthodes d'extraction et d'analyse de la donnée, le ciblage des électeurs devient sensiblement plus efficace et percutant, permettant aux acteurs politiques non seulement de mieux maîtriser les techniques traditionnelles évoquées, mais aussi de perfectionner le contenu du message à apporter aux électeurs, à l'appui des données publiques ou personnelles. Ces messages sont désormais plus susceptibles de capturer l'attention de l'électeur ciblé.

La littérature spécialisée distingue deux catégories de logiciels mis à disposition des acteurs politiques. La première consiste à des solutions plus simples techniquement, représentées par des logiciels qui croiseraient des données publiques de l'ensemble des résultats électoraux depuis 1958, et bureau de vote par bureau de vote depuis 2002. Se reposant donc notamment sur des données mises par l'État en open data et libre-accès en ligne, ces logiciels permettent aux développeurs et utilisateurs de compiler et croiser des données à l'appui des outils existants dans les logiciels. Il est possible de regrouper sous cette catégorie des solutions comme FederaVox et eXplain (anciennement Cinquante Plus Un)[135]. La deuxième catégorie, architecturalement plus complexe, est assimilable à un système de gestion de contenus de différentes teneurs, regroupant dans une seule solution des fonctions d'encadrement, organisation et mise en place de la stratégie de communication électorale des acteurs politiques. Les exemples plus évidents de ce deuxième groupe de solution de logiciel de stratégie électorale sont Nationbuilder, le leader du marché, et DigitaleBox.

En entretien accordé en 2017, le responsable du développement de Nationbuilder en Europe a précisé que cette plateforme a le mérite de mettre ensemble les quatre éléments d'une campagne : le CMS (*Content Management System*, ou Système de gestion de contenu –

[135] « *Le matériau source. Il y en a deux principalement. On découpe la France en 60 000 petits carrés. Et chacun de ces carrés correspond au bureau de vote et pour chacun, on a l'ensemble des résultats des élections depuis 2004 et on a également tous les résultats des recensements INSEE. Donc, toutes les données sociodémographiques* ». Entretien accordé par le fondateur de l'agence Civitéo à Anaïs Théviot le 1er juin 2017 ; *Id*., p. 107.

programme informatique utilisé pour gérer l'apparence et le contenu d'un site web) ; le CRM (*Customer Relationship Management*, pour Système de la relation client – programme informatique utilisé pour la gestion de la relation des acteurs politiques avec les électeurs) ; les mails, les mass mailings et les textos ; et enfin les éléments de finance, pour organiser du financement des campagnes, *crowdfundings* etc[136].

Le modèle de business adopté par ces entreprises suggèrerait que les solutions ne sont pas par défaut livrées aux acteurs politiques avec des données personnelles de quiconque, électeurs, militants ou sympathisants[137]. Il appartiendrait donc à ces acteurs de les ramener à la solution.

Il convient maintenant de préciser de fonctionnement de deux solutions parmi les plus utilisées jusqu'à présent en France, eXplain et Nationbuilder.

Selon Guillaume Liegey, l'un des Bostoniens fondateurs d'eXplain, le logiciel Cinquante Plus Un[138] – opérationnel au moins jusqu'aux élections présidentielles de 2017 – offrait des outils d'analyse de l'opinion au niveau local en se prévalant des données de géolocalisation, ce qui lui permettait de savoir, parmi d'autres informations, « *dans quelle région on lisait le plus d'articles de presse sur tel ou tel sujet* »[139]. À l'heure actuelle, la solution de l'entreprise promet de repérer les personnes influentes de l'écosystème local, de reconstituer l'historique d'un territoire, d'anticiper les décisions qui pourraient toucher l'activité des leurs clients, outre permettre à ceux-ci d'accéder à toute la presse locale et aux documents des collectivités[140].

En ce qui concerne Nationbuilder, la solution permet aux partis, élus et candidats à des fonctions électives, tout d'abord, d'assurer un niveau accentué de gestion de consentement des

---

[136] Entretien accordé à Anaïs Théviot le 6 juillet 2017. *In* A. THÉVIOT, « *Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter* », Le Bord de l'Eau, 2019, p. 149.

[137] *« On a des modèles de ciblage électoral qu'on construit depuis plusieurs années et qui utilisent des données agrégées à l'échelle du bureau de vote pour comprendre les endroits où nos clients ont le plus fort potentiel électoral. Il n'y a donc aucune donnée personnelle, ce ne sont que des données agrégées et c'est très important pour nous de ne jamais mettre de données individuelles »,* Laure Vaugeois, responsable des élections municipales chez eXplain, *in* « Les logiciels de stratégie électorale, alliés essentiels des élections municipales *», France Inter,* 10 février 2020, consulté en ligne le 08 mai 2021, 12h15.

[138] Il se peut que ce logiciel ait été renommé « Goodwill », nom utilisé pour se référer á une des solutions offertes par l'entreprise actuellement sur son site web.

[139] « Le scandale Cambridge Analytica aurait-il pu se produire en France ? *», Le Monde,* 23 mars 2018, consulté en ligne le 13 mai 2021, 00h13.

[140] Site internet officiel eXplain.

électeurs pour le traitement de leurs données. Il leur est permis par ailleurs de trouver des numéros SMS cachés dans leurs bases de données, d'améliorer leur taux de livraison aux électeurs[141], et de mieux tracer les routes des campagnes porte-à-porte à l'aide d'une base de données privilégiée. D'origine Étasunienne, l'entreprise mettait à disposition de ses clients au départ de ses activités en France un outil « *Nationbuilder Match* », qui siphonnait les données personnelles des utilisateurs issues de plusieurs réseaux sociaux (Facebook, LinkedIn, Twitter, etc.) par le biais d'une adresse e-mail[142]. Or, il s'agissait d'un outil que, de par son fonctionnement, ressemblait beaucoup à celui se retrouvant à l'origine de l'affaire Cambridge Analytica. Il allait même au-delà, autorisant le recoupage de ces informations avec d'autres types de données, publiques (celles de l'Insee) ou privées (par l'achat ou la location de bases de données collectées par des entreprises), ce qui en faisait un outil central de la plateforme et des opérations de l'entreprise.

Après des réunions tenues entre les équipes de l'autorité de contrôle et de l'éditeur, la CNIL condamne expressément la pratique de siphonnage des données personnelles des profils des potentiels électeurs à leur insu[143]. Deux points sont à regretter néanmoins : la condamnation est venue plus de trois ans après la mise à disposition de l'outil par l'éditeur à ses clients en France, qui y était opérationnel depuis février 2013, et sa désactivation tardive par les éditeurs, qui n'a été actée qu'après la tenue des Primaires de 2016, en 1er mars 2017[144].

Les candidats ayant adhéré systématiquement aux solutions de stratégie électorale dans les présidentielles de 2017, Jean-Luc Mélenchon et Jacques Cheminade choisissent NationBuilder, option retenue aussi par François Fillon, dont l'équipe s'est dotée par ailleurs des outils proposés par FederaVox (axé davantage sur la cartographie électorale). De leur côté, Benoît Hamon et Emmanuel Macron se sont appuyés sur le logiciel Cinquante Plus Un[145]. Macron s'est prévalu, même en amont de la campagne, de la solution offerte par eXplain pour

[141] Site internet officiel Nationbuilder.
[142] M. BARDIN *Op. cit.,* p. 43 à 54.
[143] « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? », site internet officiel de la CNIL, 8 novembre 2016, consulté en ligne le 26 février 2021, 20h01.
[144] « Logiciels électoraux : les politiques français ont dû mettre fin à la récolte de certaines données personnelles *», Le Monde,* 03 avril 2017, consulté en ligne le 21 avril 2021, 11h10.
[145] « Comment le Big data s'est invité dans la campagne présidentielle ? *», Les Echos,* 19 avril 2017, consulté en ligne le 13 mai 2021, 12h46.

déterminer les questions à poser aux électeurs et les portes à frapper, pour ensuite faire appel à la solution Proxem, spécialisée dans l'analyse sémantique des données textuelles[146].

Pour l'anecdote, quelques jours avant la tenue des présidentielles, le candidat victorieux avait fait appel à des automates d'appel pour mieux faire passer son message aux électeurs. Il faut se rappeler que, compte tenu de son caractère intrusif, la CNIL estime qu'aucune exception au principe de collecte du consentement préalable des électeurs ne peut être invoquée par les acteurs politiques lorsque des automates d'appels sont utilisés à des fins de communication politique[147]. L'équipe de campagne de Macron prend ainsi soin de confier aux électeurs ciblés la possibilité de ne pas écouter le message du futur président en appuyant sur la touche numéro 1[148], cela avant même la transmission du message.

Plus récemment, les solutions de microciblage électoral ont connu une phase de diversification et d'augmentation des offres. Une dizaine de jeunes entreprises se partagent désormais le marché et fournissent aux candidats une aide organisationnelle et un outil de ciblage électoral, parmi lesquels NationBuilder, eXplain, Quorum, DigitaleBox, Decidim, Spallian, Cap Collectif, Fluicity ou encore Poligma.

Si l'utilisation des logiciels de stratégie électorale ne va toujours pas avec la personnalisation de la communication politique[149], en pratique, les deux sont difficilement dissociables, au vu de l'utilisation systématique des données des électeurs, adhérents, membres et sympathisants par les acteurs politiques dans ces solutions, et du croisement de ces données avec d'autres données publiques, ce qui accentue la pertinence des messages à ces électeurs.

Face à la puissance technologique redoutable de ces solutions, des questions se présentent quant à la rigidité du dispositif juridique européen et français et son aptitude à relever les défis de maîtriser cette forme de communication politique.

---

[146] Cette dernière aurait œuvré pour la détection des associations de mots, de leur assemblage en grappes, des catégorisations, de la séparation des différents sens des réponses récoltées lors des porte-à-porte, *in* « Comment Emmanuel Macron a fait son 'diagnostic' *», L'Obs,* 21 novembre 2016, consulté en ligne le 13 mai 2021, 14h26.

[147] Délibération CNIL 2012-020, du 26 janvier 2012.

[148] A. THÉVIOT, « Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter », *Le Bord de l'Eau*, 2019, p. 172.

[149] Puisque d'une part, leur utilisation ne présuppose pas l'existence de données personnelles, et d'autre part, le degré de personnalisation change selon les techniques employés pour analyser les informations et les bases de données croisées dans la solution, pouvant aller d'un faible degré (voire inexistant) jusqu'à un très conséquent.

Section 2 – Un cadre juridique inachevé et la perspective de remise en cause de la sincérité du scrutin

Le paysage des solutions en stratégie électorale s'est complexifié depuis les présidentielles de 2012. Il était donc légitime de penser que la réglementation européenne renouvelant le dispositif juridique sur la protection des données personnelles allait procurer aux électeurs et juristes un niveau plus conséquent de protection, à même de répondre efficacement aux menaces posées par l'arrivée des fournisseurs de logiciel en stratégie électorale. Néanmoins, des efforts sont toujours au rendez-vous pour y arriver. Afin de s'intéresser aux perspectives de remise en cause de la sincérité des résultats des élections que la personnalisation du microciblage politique peut entraîner (**Paragraphe 2**), il appartiendra d'aborder en toute première place les limitations juridiques de ce dispositif renouvelé (**Paragraphe 1**).

Paragraphe 1 – Les apports limités du dispositif européen et français

Malgré les avancées trouvables dans le RGPD concernant la protection des données personnelles des électeurs, quelques caps législatifs sont encore à franchir.

Comme partout où l'intelligence artificielle est employée, la matière première des algorithmes utilisés dans la communication politique est la donnée. Dans la mesure où la communication politique est favorisée par la donnée, il appartiendra aux acteurs politiques, afin de mieux comprendre leurs électeurs et établir avec eux une communication plus efficace, de créer et stocker une certaine quantité de données à leur égard. Dans le prolongement de l'ouverture du marché de la donnée sur le web, la communication politique assiste à l'augmentation de la création de données dans le monde[150] et en Europe. Il en est de même pour les données stockées[151].

Or, comme le rappelle la CNIL, les principes de la loi informatique et libertés de 1978 renvoient à la minimisation de la collecte de données personnelles ainsi qu'à la limitation de

[150] Alors qu'en 2010 nous étions à 2 zettaoctets crées dans le monde, nous serons à 47 en 2020 et 2142 en 2035. *In* « Le volume de données mondial sera multiplié par 45 entre 2020 et 2035 », *Journal du Net*, 17 mai 2019, consulté en ligne le 14 mai 2021, 23h49.
[151] « La planète abritera 175 Zo de données en 2025, soit 5,3 fois qu'aujourd'hui », *ZDnet*, 04 décembre 2018, consulté en ligne le 14 mai 2021, 23h53.

leur durée[152]. Il ne serait donc pas illégitime de penser que les principes de minimisation de la collecte et e la conservation des données personnelles, tels que réinscrits dans le marbre du droit européen[153], ne soient pas encore largement respectés par tous les responsables de traitement confondus.

À cet égard, la jurisprudence de la plus haute juridiction administrative ne remet pas directement en cause les décisions des responsables de traitement de conserver les données pour un délai supérieur au nécessaire à la réalisation de la finalité du traitement. En effet, elle ne le fait qu'à l'aune d'un manque de protection des systèmes d'information constaté[154]. Cela pose de questions sur l'opinion de la plus haute cour administrative française à propos du caractère reprochable en soi de la décision de conserver des données pendant un délai supérieur au nécessaire à la réalisation de la finalité du traitement.

Il faut noter aussi que si le régime de responsabilité des responsables de traitement a été renforcé par le nouveau dispositif juridique, ce régime aurait pu faire objet d'attention particulière en ce qui concerne l'utilisation de l'intelligence artificielle. Des textes comme la loi informatique et libertés[155], le code de l'éducation[156], le code des relations entre le public et l'administration[157] et le RGPD n'abordent directement les implications pour le responsable du traitement dysfonctionnel des données à l'appui des algorithmes. L'absence d'un tel périmètre de responsabilité avait déjà été relevée par Cédric Villani dans son rapport « Donner un Sens à l'Intelligence Artificielle »[158].

Par ailleurs, les préoccupations entourant le marché du courtage des données ont partiellement été adressées par l'article 14 du RGPD, qui impose un standard de sécurité pour la protection des données personnelles collectées indirectement, c'est-à-dire, non directement de la personne concernée. Désormais, le responsable de traitement doit non seulement divulguer à celle-ci les informations afférentes à lui-même et ses activités, mais également la source d'où proviennent les données personnelles (Article 14, paragraphe 2, alinéa « f ») et ce, de manière

[152] « *Comment Permettre à l'Homme de Garder la Main ?* », Synthèse du débat public animé par la CNIL dans le cadre de la réflexion éthique confiée par la loi pour Une République Numérique, 2017, pp. 40-41.
[153] Article 5, paragraphe 1, alinéa « c » et « e » du RGPD.
[154] CE 9e et 10e chambres réunies, 04-11-2020 (affaire n° 433311), et CE, section avis, 09-06-2020 (affaire n° 400322).
[155] Article 47.
[156] Article L612-3.
[157] L311-3-1.
[158] « *Parallèlement, il faut s'assurer que les organisations qui déploient et utilisent ces systèmes demeurent responsables devant la loi des éventuels dommages causés par ceux-ci. Si les modalités de ce régime de responsabilité restent à définir, la loi informatique et libertés (1978) et le RGPD (2018) en posent déjà les principes* », 2018, p. 140.

concise, transparente, compréhensible, et aisément accessible, en des termes clairs et simples. À saluer aussi l'initiative du législateur européen d'attribuer au non-respect des règles de transparence prévues par cet article les plus grandes sanctions prévues par le RGPD (Article 83, paragraphe 5, alinéa « e »).

Toutefois, le droit d'accès à l'information des électeurs est mis à mal par l'absence de précisions sur la source d'où proviennent les données personnelles, dans l'hypothèse de transmissions à des multiples acteurs de la chaine. La loi nationale aurait pu, par exemple, imposer aux responsables de traitement, et donc, aux acteurs politiques, un mécanisme de bordereau de transmission de données personnelles à chaque fois que les données sont transmises à d'autres parties prenantes de la chaine de transmission, pour qu'un traçage de l'information soit assuré.

Lors de la première vague législative, évoquée en première partie de ce travail, il a été souligné que la CNIL dénonçait depuis des années[159] l'absence de dispositif légal spécifique encadrant la prospection à caractère politique, et que, de ce fait, l'autorité de contrôle s'appuyait sur les règles existantes pour la communication commerciale, pour en dégager celles applicables à la communication politique. Malgré le rappel aux autorités fait à cet égard en 2012[160], les acteurs politiques ne peuvent toujours pas s'appuyer sur un dispositif légal spécifique à la prospection politique, ce qui pose des questions sur un éventuel conflit d'intérêts entre, d'une part, les élus et les candidats à des fonctions électives – destinataires directs de ce dispositif subissant ses contraintes en première chef – et, d'autre part, le dispositif lui-même.

Par ailleurs, il n'existe toujours pas de dispositif légal pour encadrer la pratique des élections primaires en France, adoptée officiellement depuis 2011, ce qui est aussi à regretter dans une certaine mesure.

Finalement, il faudrait souligner que, malgré le renouvellement du dispositif national, acté pour le mettre en phase avec le RGPD[161], les délibérations de la CNIL n'ont pour l'instant pas suivi cette altération législative. De ce fait, sa délibération 2012-020, du 26 janvier 2012,

[159] Délibération CNIL n° 2006-228, du 5 octobre 2006.
[160] Délibération CNIL n° 2012-020, du 26 janvier 2012.
[161] Notamment la loi n° 2018-493 du 20 juin 2018, relative à la protection des données personnelles, et l'Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018.

reste la dernière sur la matière de la communication politique à ce jour[162]. Après des changements importants apportés par le RGPD dans la mise en conformité des acteurs politiques aux règles de protection des données personnelles des électeurs[163], une nouvelle règlementation de la CNIL s'impose, d'autant plus à l'heure où les logiciels de stratégie électorale et les techniques de *cross-marketing* entre entités publiques et privées[164] ramènent les frontières actuelles de la communication politique à des limites insoupçonnés.

Une fois posées les limitations du cadre juridique actuel, il convient de s'intéresser à la question de savoir si l'intelligence artificielle représente un risque pour la vie et le processus démocratique en France.

Paragraphe 2 – La perspective non lointaine de remise en cause de la sincérité du scrutin

La doctrine constitutionnelle essaie depuis longtemps de tracer les contours de la figure de la sincérité du scrutin, principe de droit électoral. Si le concept tient à la fois à des aspects concernant la formation légitime du corps électoral – élus et futurs élus – et les électeurs[165], c'est ce second volet qui fera l'objet de ce paragraphe. La sincérité du scrutin cristalliserait en quelque sorte la volonté réelle de l'électeur, ce que signifie que si le choix exprimé par les électeurs lors d'un scrutin est connu de manière certaine et sans équivoque, qu'ils l'ont fait en toute conscience et en suivant leur seule volonté, le scrutin est sincère.

Consacré par la jurisprudence du Conseil constitutionnel depuis des années[166], ce principe est manié par le juge constitutionnel soit en tant que juge électoral, soit en tant que juge de la constitutionnalité de la loi[167]. En ce qui concerne sa portée, elle reste assez indéterminée à l'égard des critères que le juge peut soulever pour valider ou annuler une élection. Néanmoins, l'atteinte à la sincérité du scrutin est souvent liée à deux paramètres,

[162] 39e Rapport d'activités de la CNIL, 2018, p. 90.
[163] Comme la disparition des formalités préalables, l'abrogation de la norme simplifiée n° 34 (destinée à encadrer ces formalités préalables dans le cadre de la communication politique), le besoin désormais imposé aux acteurs politiques d'avoir un registre de traitement et, éventuellement, de procéder à une analyse d'impact relative à la protection des données, dans l'hypothèse de traitement des opinions politiques des électeurs.
[164] « *Les grands acteurs de l'Internet, Google et Facebook en tête, proposent d'ores et déjà de compléter les données électorales avec les données libres et propriétaires, sur les habitudes de consommation.* ». *In* E. BARQUISSAU, L. SCHLENKER *Op. cit.*, pp. 257 à 292.
[165] R. GHEVONTIAN, « La notion de sincérité du scrutin », *Cahiers du Conseil constitutionnel*, janvier 2013.
[166] « *Au moment où le droit électoral retrouve, grâce en grande partie à sa 'constitutionnalisation', le rang qui doit être le sien dans un État de droit, il a paru utile de s'intéresser de plus près à ce concept de sincérité du scrutin.* », *in* R. GHEVONTIAN, « La sincérité du scrutin, études réunies et présentées par Richard Ghevontian ». Cahiers du Conseil constitutionnel, 2013
[167] Cons. const., 2013-673 DC, 18 juil. 2013

l'écart de voix et l'influence déterminante de l'irrégularité génératrice du défaut de sincérité. Plus l'écart de voix est faible[168] et l'influence de l'irrégularité est déterminante, plus le juge sera susceptible d'annuler l'élection par non-respect de ce principe.

En 2019, la CNIL avait déjà soulevé le potentiel attentatoire que l'utilisation des opinions politiques pourrait avoir dans le cadre des élections politiques[169]. L'autorité de contrôle a d'ailleurs rappelé que les logiciels de stratégie électorale peuvent avoir des implications pour l'issue des élections en cas d'incidents avec un faible écart de voix[170].

Les algorithmes mis en avant par les réseaux sociaux et les fournisseurs de logiciels de stratégie électorale auraient vocation à remettre en cause la sincérité du scrutin dans la mesure où ils fausseraient le choix en toute conscience des candidats à des élections politiques par les électeurs. Cela s'explique, notamment, par l'effet de bulle informationnelle subi par les électeurs durant leur expérience de navigation sur le web, ou encore, de manière plus subtile, lors que ces électeurs font l'objet des campagnes par téléphone ou SMS, MMS. En rompant avec la symétrie informationnelle propre des médias télévisés et de la presse écrite, l'atteinte au principe d'égalité de distribution de l'information serait susceptible de mettre en danger l'idée même de démocratie[171].

Dans une étude publiée en 2017[172], la *London School of Economics* s'était penchée sur le sujet du ciblage politique. Parmi d'autres points d'attention soulevés, soulignons la tentative d'engager majoritairement des électeurs indécis ou marginalisés. « Quid des autres électeurs ? », provoque l'école de commerce britannique. La question n'est pas sans intérêt lorsqu'on considère que les données des élections précédentes sont souvent utilisées pour guider les acteurs politiques dans les élections suivantes, ce qui comporterait un risque de marginalisation des autres électeurs (ceux qui se sont déjà décidés), dans le cadre de la stratégie des campagnes qui s'en suivraient.

---

[168] Lors des législatives de 2017, le Conseil constitutionnel a constaté que plusieurs requêtes remettant en cause la sincérité du scrutin se fondaient sur des moyens dénonçant des faits dont le caractère irrégulier ou dont la réalité n'étaient pas établis par la requête. Toutefois, le Conseil constitutionnel a estimé « *pouvoir écarter ces requêtes sans instruction dès lors qu'en tout état de cause, à les supposer établis et irréguliers, les faits dénoncés étaient insuffisants pour justifier une annulation de l'élection contestée en raison de l'écart des voix entre les candidats* ».

[169] É. SERUGA-CAU ; T. HAVEL, *Op. Cit.*, p. 75.

[170] « Logiciels électoraux : les politiques français ont dû mettre fin à la récolte de certaines données personnelles *», Le Monde,* 03 avril 2017, consulté en ligne le 21 avril 2021, 11h10.

[171] J. GERSTLÉ ; C. PIAR, *Op. cit*., p. 239 à 247.

[172] « The new political campaigning », *LSE Media Policy Project*, March 2017, page 19.

Toujours selon cette étude, le microciblage politique favoriserait la concentration des ressources des partis et candidats dans des questions polémiques, qui nourrissent le partage d'opinions dans l'espace public, ayant en plus la capacité de mobiliser les électeurs sur les dossiers comme l'immigration et le bien-être. Si les candidats ont tendance à faire davantage de campagne sur ces dossiers dans des forums privés, qu'en serait-il des effets de ces campagnes pour les élections[173] ? Le manque de statistiques sur les campagnes que se déroulent dans ces forums privés, sur leur portée et objet, est source d'inquiétudes de tous bords.

Encore plus insaisissable est « *l'effet boîte noire* » des algorithmes lorsqu'ils sont utilisés dans le cadre de la communication politique. L'impossibilité d'évaluer, de critiquer, d'auditer, tant *ex ante* qu'*ex post*, les choix faits par l'algorithme durant le traitement de la donnée, la manière dont les calculs algorithmiques arrivent à certains résultats et non à d'autres, est sans doute inquiétant. Cela va de pair avec des questions sur le respect de la protection des données personnelles dès la conception et par défaut des plateformes. La société civile aurait-elle le droit d'exiger un niveau accentué de transparence algorithmique des opérateurs de réseaux et fournisseurs de logiciels de stratégie électorale durant la période électorale ? Il faut savoir que ce droit s'inscrit dans la ligne droite de la jurisprudence récente du Conseil constitutionnel, qui a estimé conforme à la constitution la loi imposant aux opérateurs de plateforme de communication la publication des mesures et moyens consacrés à assurer la transparence des algorithmes en cas de manipulation ou soupçon de manipulation de l'information par les opérateurs de plateforme en ligne[174].

Un niveau optimal de transparence algorithmique serait d'autant plus souhaitable dans cette hypothèse que certains fournisseurs de logiciels en stratégie électorale ont déjà déclaré publiquement ne pas commercer avec des partis ou élus d'une certaine coloration politique[175].

Dans l'hypothèse où les données personnelles des électeurs transitent dans la base de données maintenue par les fournisseurs de logiciels de stratégie électorale, et que ceux-ci puissent, de ce fait, être tenus comme des responsables de traitement des données des électeurs,

---

[173] « *Andy Wigmore, communications director of Leave.eu explained in an interview with LSE researchers that his campaign would consider: 'What were their key feelings? What were their anxieties? What, for them, was the issue about the EU or Europe?' Campaigners would then tailor messages accordingly, and 'our mass concentration was on that,' he said.* », *id*.

[174] Cons. const., n°2018-773 DC, 20 déc. 2018, cons « 89 ».

[175] Arthur Muller, l'un des fondateurs de Liegey-Muller-Pons (aujourd'hui eXplain), avouait en 2017 ne pas travailler pour le Front national. *In* « Trois hommes + 1 logiciel = l'Elysée *», Le Monde,* 07 avril 2017, consulté en ligne le 15 mai 2021, 00h12.

ces électeurs auraient le droit d'être informés sur l'existence d'une prise de décision automatisée par les logiciels utilisés par les acteurs politiques. De même que sur des informations utiles concernant la logique algorithmique sous-jacente du traitement et les conséquences prévues de ce traitement pour eux. C'est le sens de l'Article 14, paragraphe 2, alinéa « g » du RGPD. L'article 22, paragraphe 1, de ce texte s'appliquerait également pour interdire le traitement automatisé des données par les fournisseurs de logiciel sans le consentement exprès des électeurs.

Le microciblage politique pose ainsi des questions éthiques et juridiques qui doivent faire objet d'attention des juristes dès maintenant. Le principe de la sincérité du scrutin revient à l'ordre du jour puisque les traitements algorithmiques évoqués peuvent être conduits en utilisant les données personnelles des électeurs à leur insu. En tant qu'expression de la volonté réelle de l'électeur, la sincérité du scrutin est susceptible d'être mise à mal selon, d'une part, les conditions et l'étendue du traitement algorithmique réalisé, et, d'autre part, du fait que les électeurs aient ou pas consenti explicitement à ce traitement (Article 22, paragraphe 1, alinéa « c » du RGPD).

Dans un autre registre, les *deepfakes* politiques peuvent eux-aussi avoir une incidence sur l'expression légitime de la volonté des électeurs dans le cadre des élections. Ces fichiers d'audio, vidéo ou des images font appel à l'intelligence artificielle pour déjouer leurs destinataires en représentant les discours et actions d'une personne n'ayant jamais réalisé ou fait l'objet de tel audio, vidéo ou images[176].

Or, si l'acteur politique derrière l'élaboration de tels fichiers se prévaut de l'effet caisse de résonance de l'internet pour faire relayer, durant la période électorale, un *fake* à un moment à partir duquel les possibilités de le déjouer par la victime sont faibles, voire inexistantes, le risque de remise en cause de la sincérité du scrutin est évident[177].

[176] « Fighting deepfakes when detection fails *», The Brooking Institution,* 14 novembre 2019, consulté en ligne le 16 mai 2021, 13h04.
[177] R. CHESNEY ; D. K. CITRON « Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security », *California Law Review*, 21 juillet 2018, p. 1778.

Les motivations pour l'élaboration d'un fichier de cette envergure peuvent être nombreuses : faire dire à des candidats ce qu'ils n'ont dit[178], réussir ce qu'ils n'ont réussi[179], imputer à l'adversaire un échec jamais subi par celui-ci, etc. Si la technologie derrière les *deepfakes* était relativement inaccessible au grand public au départ, à l'heure actuelle des applications performantes sont déjà à disposition gratuitement dans plusieurs plateformes.

Le *deepfake* constitue pratique reprochable par le cadre normatif en vigueur dans des contextes spécifiques. L'article L116 du code électoral et l'article 226-4-1 du code pénal porteront à la fois sur la fraude aux élections et l'usurpation d'identité. Dans le premier cas, ceux qui portent ou tentent de porter atteinte à la sincérité d'un scrutin, ou changer ou tentent changer les résultats des élections, sont susceptibles à une amende de 15 000 euros et un an d'emprisonnement. Dans le deuxième, le législateur appréhende la question sous le prisme du trouble à la tranquillité ou de l'atteinte à l'honneur ou considération d'un tiers. Si le *deepfake* est réalisé dans le but d'usurper l'identité de quelqu'un d'autre, les peines peuvent aller jusqu'à deux ans d'emprisonnement et 30 000 euros d'amende.

Il a été constaté que, malgré le renforcement du dispositif européen avec le RGPD et l'adaptation du cadre juridique national qui s'en est suivi, des changements importants sont à prévoir, notamment au vu des risques à forts enjeux éthiques et démocratiques. Il convient, dans le chapitre suivant, de traiter des effets que cette nouvelle technologie apportera en pratique pour la protection des données personnelles des électeurs, et des perspectives de règlementation du marché de la donnée, concernant spécifiquement la communication politique.

[178] En Inde, le candidat Manoj Tiwari s'est adressé à ses électeurs dans une langue qu'il ne parle pas grâce à l'intelligence artificielle. *In* « Nouveau Monde : Quand les deepfakes deviennent une arme de communication politique assumée », *Franceinfo,* 21 février 2020, consulté en ligne le 16 mai 2021, 14h36.
[179] « Solidarité Sida lance une vidéo virale avec Trump et deep fake – D. TRUMP : 'Aids is over' », *Youtube*, 08 octobre 2019, consulté en ligne le 16 mai 2021, 14h40.

CHAPITRE 2 – UNE STRATÉGIE AUX EFFETS DÉCUPLÉS POUR LA PROTECTION DES DONNÉES PERSONNELLES DES ÉLECTEURS

Jusqu'à l'avènement de l'intelligence artificielle et son accaparement par la communication politique, le niveau de personnalisation de l'approche des électeurs dans le but de les prospecter ou les fidéliser n'a pas créé des risques significatifs d'atteinte aux droits et libertés fondamentaux des électeurs, notamment au droit à la protection de leurs données personnelles. Dans un deuxième temps, après la consolidation du marché de logiciels de stratégie électorale, les acteurs politiques auront l'occasion de s'intéresser à des données à haut niveau de granularité. Il emporte ainsi de comprendre les risques d'atteinte à ces droits que l'application des algorithmes soulève (**Section 1**), pour ensuite s'intéresser aux perspectives de réglementation des questions pouvant avoir des reflets dans la pratique de la communication politique (**Section 2**).

Section 1 – Les risques accrus à la protection de données personnelles des électeurs

La personnalisation de la communication politique étant à l'ordre du jour à l'heure de l'utilisation des logiciels de stratégie électorale, il faudra dans un premier temps vérifier l'étendue des risques auxquels les électeurs sont soumis lorsque la communication entretenue par les partis, élus et candidats à des fonctions électives passe à un degré accentué de personnalisation (**Paragraphe 1**). Dans un deuxième temps, sera analysée l'accentuation de la responsabilité de traitement des acteurs politiques en conséquence du niveau plus important de personnalisation de la communication politique (**Paragraphe 2**).

Paragraphe 1 – La communication politique à l'épreuve des logiciels de stratégie électorale

Avant de rentrer dans le vif du sujet, il convient de s'attarder sur un des premiers emplois de l'intelligence artificielle à la communication sur les réseaux : les *bots*[180].

[180] « *The software engineers (…) who automate communication on social or device networks often call their creations bots. The word* bot *is an abbreviation of robot, itself a 20th century Czech term meaning 'forced labor' or 'slave'. This is a fitting etymology for bots in that they exist, in a manner of speaking, as digital versions of their embodied cousins.* », *in* S. C. WOOLEY, P. N. HOWARD, *Op. cit.*, p. 2.

Expression ultime du nouveau théâtre du débat politique, Twitter a été reconnu pour avoir réussi à fédérer autour d'une plateforme une partie considérable des chefs d'États mondiaux. Grace à sa politique d'accès facilitée à l'interface de programmation d'application[181], les bots – logiciels programmés par des tiers pour prendre des actions en lieu et place des hommes –, se sont emparés des comptes Twitter pour exécuter les ordres des programmeurs, pour suivre ou laisser de suivre d'autres usagers, mettre en place des sondages, poster des images ou envoyer des messages à des usages spécifiques[182].

Ces actes, humains par excellence, sont élevés à leur paroxysme lorsqu'ils sont mis en place par des bots. Exécutés dans des fréquences et échelles temporelles beaucoup plus optimisées que celles des humains, ces actions ne seront pas sans incidence sur la communication politique. Facilement programmables par un utilisateur moyen, ces bots ont été utilisés comme moyen de déstabilisation du débat politique par l'apparat institutionnel de plusieurs pays[183].

La montée en influence des bots dans la communication politique s'inscrit dans la tendance de vulgarisation des cybercrimes, au vu, notamment, des a) coûts fixes minuscules impliqués de la communication par ce biais (un même bot est utilisé des milliers de fois) ; b) faibles coûts variables d'exploitation de la technologie, (typiquement, le temps consacré à la mise en place du logiciel) ; et c) bénéfices escomptés importants (la mise à mal des élections, en l'occurrence).

Pour ce qui est des logiciels de stratégie électorale, de nombreuses atteintes peuvent être portées à certains droits fondamentaux. Comme il a été souligné auparavant, la fonction Match de Nationbuilder a été désactivée en France par le développeur de l'application en mars 2017. Pour rappel, elle permettait à Nationbuilder de collecter des données des utilisateurs issues de plusieurs réseaux sociaux, dont Facebook, à l'appui de leurs mails personnels. Si l'atteinte à la

[181] Selon le Grand Dictionnaire terminologique de l'Office québécois de la langue française, le terme désigne de routines standards, accessibles et documentées, qui sont destinées à faciliter au programmeur le développement d'applications. Aussi connu sous la rubrique d'« *application programming interface* » (API).
[182] B. KOLLANYI, in *Op. cit.,* p. 1.
[183] « Weaponizing bots and data: The Brazilian electoral experience of 2018 », *Israel Public Policy Institute*, 2 mars 2021, consulté en ligne le 17 mai 2021, 18h18 ; et « What are Russia's goals with disinformation on social media ? », *Brandeis Now*, 22 octobre 2020, consulté en ligne le 17 mai 2021, 18h37.

vie privée que cette collecte sans autorisation entraîne est bien appréhendée par le droit pénal[184], elle est moins saisissable de prime abord sur le plan du droit civil[185].

Malgré la désactivation en France, l'intérêt de parler sur la fonction demeure, eu égard à la tendance de la constitution des bases de données et de la conservation de documents grandissante et au potentiel d'utilisation des données des électeurs sur les réseaux sociaux toujours présent. L'intérêt apparent de remise en cause de la désactivation a par ailleurs été évoqué expressément quelques années auparavant[186].

Plus récemment, la CNIL a dressé, dans son 41e Rapport d'Activités, un bilan de l'application des règles concernant la communication politique par les acteurs politiques lors des élections municipales de 2020. L'autorité de contrôle note tout d'abord un recours grandissant par ces acteurs aux logiciels de stratégie électorale, pour suggérer ensuite que, dans le cadre de ces élections, « *les solutions proposées aux candidats n'offrent pas de possibilité de ciblage des électeurs aussi fines que ce qui a parfois pu être évoqué dans les médias* »[187]. La CNIL salue enfin le respect par les acteurs politiques à l'interdiction de recours aux données issues des réseaux sociaux et de l'utilisation d'outils statistiques en open data.

Le droit à la protection des données à caractère personnel des électeurs, élevé au rang de droit fondamental par l'article 1er, alinéa 2 du RGPD, peut également faire l'objet d'atteintes dans le cadre de l'utilisation des logiciels de stratégie électorale. Les droits qui en découlent (Articles 15 à 21 du RGPD) sont susceptibles d'être relativisés par les acteurs politiques, comme dans le cas d'absence de prise en compte du droit à l'opposition.

---

[184] L'article 226-1 du code pénal condamne l'atteinte à la vie privée lorsque quelqu'un capte, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel. L'article suivant vise « le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document » ainsi obtenu.

[185] Le code civil (article 9) prévoit que chacun a le droit au respect de sa vie privée, tout en garantissant l'intervention du juge pour en faire cesser les obstacles.

[186] « *(...) Je pense que ça va être une conversation qu'on va continuer à avoir parce que ça fait peur et ça, c'est justement, c'est le rôle, un rôle qu'on doit prendre : éduquer à notre métier. Il y a un besoin d'apprentissage.* » Responsable du développement de Nationbuilder en Europe. Entretien accordé à Anaïs Théviot le 6 juillet 2017. *In* A. THÉVIOT, « Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter », *Le Bord de l'Eau, 2019*, p. 114.

[187] 41e Rapport d'activités de la CNIL, 2020, pp. 59-60. Si dans le cadre des élections municipales le ciblage ne se sont montrés si fines, il emporte de se demander s'il en irait de même dans le cadre des élections nationales, eu égard aux intérêts plus conséquents en jeu.

Il reste à déterminer dans quelle mesure la liberté d'expression, dont découlent la liberté de la communication audiovisuelle et la liberté d'expression sur le réseau internet[188], peut être mise à mal par l'utilisation des logiciels de stratégie électorale, notamment à l'aune des messages personnalisés aux électeurs que certains d'entre eux permettent d'envoyer.

De par leur sensibilité, les opinions politiques posent aussi des questions concernant la capacité des algorithmes de les déduire en regroupant ou recombinant des données, personnelles ou pas, d'une personne existante sur le web. En effet, rien techniquement n'empêcherait le développement d'un outil par les fournisseurs des logiciels de stratégie électorale pouvant avoir accès à des données comme l'identité, comportement, goûts, achats précédents, parcours professionnel ou académique, rêves, pour ensuite les recombiner afin d'en découler d'autres modalités de données, dont les opinions politiques. Alors même que le consentement pourrait être envisagé préalablement à la collecte des données, l'étendue des recombinaisons, aménagements et découpages susceptibles d'être réalisés par l'algorithme soulève des inquiétudes, spécialement à au vu de l'effet boîte-noire évoqué.

En 2018, l'autorité de contrôle britannique a mis en garde les partis politiques des risques que la pratique d'inférer les données implique pour le débat politique. En constatant que ces formations ne considéraient pas les données inférées comme étant des données personnelles vu leur caractère non factuel, l'ICO profite de l'occasion pour poser sa doctrine sur le sujet en indiquant que dans la mesure où elles peuvent être rattachées à des individus, elles doivent être considérées comme des données personnelles[189].

À cet égard, dans une recommandation publique, la CNIL note qu'à des fins de communication politique, le croisement des données personnelles ne peut concerner que les contacts réguliers, ce qui pour l'homologue français de l'ICO serait acceptable compte tenu de la fréquentation assidue de ces contacts avec les acteurs politiques en cause[190].

[188] « Qu'est-ce que la liberté d'opinion ? » *Portail Vie-publique,* 12 février 2021 (dernière modification), consulté en ligne le 24 mai 2021, 16h05.
[189] « Democracy Disrupted, Personal information and political influence », *the Information Commissioner's Office*, 11 juillet 2018, p. 30.
[190] « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? », site internet officiel de la CNIL, 8 novembre 2016, consulté en ligne le 26 février 2021, 20h01. Pour le concept de contact régulier, se référer au paragraphe où nous avons traité la distinction juridique des approches aux électeurs par les partis politiques, élus et candidats à des fonctions électives.

Si la CNIL ne reconnaît dans ces recommandations publiées à ce jour l'existence d'une telle catégorie distincte de données – les données inférées –, elle l'a expressément fait dans un document non publié, présenté en séance plénière le 10 janvier 2019. Dans ce document, obtenu par des journalistes couvrant des sujets liés au monde de la tech[191], l'autorité française s'intéresse au sujet en admettant la possibilité d'inférer des données politiques à partir de données non politiques.

La position de la CNIL de ne pas publier une doctrine solide à ce sujet peut se comprendre au vu des impacts peu visibles dans les grands médias des technologies qui mobilisent ces croisements de données. Il n'en demeure pas moins que, devant la myriade de combinaisons possibles, les risques d'atteinte à la limitation des finalités du traitement des données personnelles[192] sont sensiblement accrus dans le cadre de la communication politique, vu la difficulté d'anticiper, au moment de la collecte des données, l'étendue de l'inférence à laquelle l'algorithme pourra donner lieu. À ces croisements se rajoute celui des informations issues de différents appareils connectés (technique connue sous la rubrique de *cross-devicing*), dont les effets ne sont pas non plus très connus aujourd'hui.

La déduction des données à partir d'autres données fait l'objet de préoccupation des institutions européennes au moins depuis 2018, lorsque le Comité Européen de la protection des données – CEPD (alors dénommé G29) lie la pratique à la possibilité, plus saisissante aujourd'hui qu'auparavant, de profilage des consommateurs[193]. La logique s'applique évidemment au profilage des électeurs dans le cadre de l'utilisation des logiciels de stratégie électorale. Sans surprise, l'opacité de la pratique y est soulevée à l'aune du consentement des personnes concernées : le CEPD y indique que si le responsable de traitement souhaite faire du profilage avec les données collectées sur cette base de licéité, le consentement doit être le plus éclairé possible pour tenir compte de toute la complexité des déductions susceptibles d'être conduites par les algorithmes.

[191] « Point d'étape relatif á l'activité de l'Observatoire des élections : Bilan et perspectives à l'aune du RGPD », p. 20, récupéré sur la page internet « Data : pourquoi il n'y a pas (encore) de campagne électorale 2.0 en France », *Nextinpact,* 04 janvier 2021, consulté en ligne le 14 mai 2021, 12h22. Ne s'agissant pas d'un document publié par la CNIL directement, l'intégrité de son contenu est susceptible de critiques.
[192] Article 5, paragraphe 1er, alinéa « b » du RGPD.
[193] Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du Règlement (UE) 2016/679, version révisée et adoptée le 6 février 2018, p. 14.

Le considérant 71 du RGPD jette les bases du traitement algorithmique des données à des fins du profilage. Si la portée normative des considérants en droit européen reste faible[194], ils font néanmoins office de déclaration d'intentions des parties prenantes du projet de texte du RGPD. Ce considérant appréhende la question sous l'angle des erreurs que le traitement algorithmique peut entraîner et, par conséquent, des risques de discrimination à l'égard des personnes concernées, fondés sur l'origine raciale ou ethnique, les opinions politiques, et d'autres critères. L'intérêt des acteurs politiques de réfléchir sur les implications de cette modalité de traitement de données avant même de le mettre en œuvre est donc d'autant plus important.

Il semble ainsi que le profilage des données, couplé à la capacité d'inférence des calculs algorithmiques, reste un point d'attention à ne pas négliger pour la règlementation de la matière, notamment en vue des échéances électorales de 2022.

Il convient désormais d'analyser en quoi ce nouveau paysage de la communication politique, complexifié par l'intelligence artificielle, impliquera un degré de responsabilité plus important des acteurs politiques.

Paragraphe 2 – La responsabilité augmentée des acteurs politiques

Le RGPD a apporté un nouveau standard de responsabilisation des acteurs sociaux dans le cadre de la protection des données personnelles. Contrairement à ce qui prévalait auparavant, le texte inaugure l'obligation de conformité du traitement dès sa conception, c'est-à-dire, avant sa mise en place[195]. L'essentiel des formalités préalables de traitement, soit le régime de communication et autorisation à certains traitements, est remplacé par la nouvelle logique de conformité des traitements dès la conception – et démonstration de conformité dès la conception (*accountability*). La mise en conformité doit être documentée, notamment à l'appui d'un registre des traitements, mais aussi d'une analyse d'impact, si le traitement est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes[196].

[194] Guide Pratique commun du Parlement européen, du Conseil et de la Commission à l'intention des personnes qui contribuent à la rédaction des textes législatifs de l'Union européenne, 2015, p. 31.
[195] Cf. considérant 78 et Article 25 du RGPD.
[196] Article 30 et 35 du RGPD.

Le RGPD évoque par ailleurs pour la première fois le concept de responsabilité conjointe de traitement[197]. Évocation très pertinente pour ce qui concerne la communication politique, eu égard aux points d'intersection possibles entre les pratiques des acteurs politiques et des fournisseurs de logiciels stratégie électorale.

Si ce texte vient qualifier juridiquement cette modalité de traitement, la pratique de déterminer conjointement les moyens et finalités d'un traitement était néanmoins monnaie courante avant le RGPD. Ainsi, la Cour de justice de l'Union européenne avait, en 2018, précisé les contours de la pratique en indiquant que le fait de participer à des actions de paramétrage d'une page Facebook fait de l'administrateur de la page un participant effectif à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de la page[198]. Ainsi, selon la cour, un administrateur d'une page Facebook serait co-responsable, avec Facebook, des traitements de données personnelles réalisés dans la page.

L'apport de cette décision pour la communication politique tient à la pratique du paramétrage d'une page web d'un parti politique, qui peut parfaitement être assuré par un fournisseur de logiciel, ce qui aurait vocation à le faire participer, dans certaines occasions, aux moyens et finalités du traitement des données des électeurs conjointement avec les acteurs politiques[199]. Même si cette décision a été rendue sous l'égide de la Directive 95/46/CE, la décision de la cour est tout à fait compatible avec l'idée de traitement conjoint des données personnelles présente à l'article 26 du RGPD.

Sans mobiliser directement le concept de responsabilité de traitement, la Cour d'appel de Paris a apporté sa contribution à la détermination du périmètre de responsabilités des éditeurs et hébergeurs de site web. Dans une décision rendue le 1er mars 2019, la cour dégage l'idée de responsabilité subsidiaire des hébergeurs concernant le contrôle de la publication des contenus illicites d'une page web, en indiquant que cette responsabilité relève d'abord de l'auteur et de l'éditeur du site. En l'absence de réponse de ceux-ci, c'est à l'hébergeur d'y faire face[200].

[197] Article 26 du RGPD
[198] CJUE, 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, affaire C-210/16, pt. 39.
[199] La participation conjointe entre les acteurs politiques et le fournisseur de logiciel s'avère possible lorsque les acteurs politiques maintiennent une page web de support à un parti avec le soutien des fournisseurs de logiciel via une interface de programmation d'application (API, en anglais), des cookies développés par ceux-ci ou d'autres moyens.
[200] Cour d'appel de Paris, pôle 1 – Ch. 8, arrêt du 1er mars 2019.

Encore une fois, les incidences de cette décision se font sentir tout de suite dans l'univers de la communication politique. Si un acteur politique choisit de faire héberger son site web chez un cloud tiers, les limites du partage de responsabilité entre les parties apparaitront. Il en va de même lorsqu'un parti politique choisit de faire héberger son site chez le cloud d'un fournisseur de logiciel de stratégie électorale – cas du parti communiste français, qui héberge sa page officielle chez le cloud de Nationbuilder[201]. La décision est encore à saluer en ce qu'elle pose des clés de lecture importantes pour définir le bon moment d'intervenir pour chaque acteur prenant partie à la mise en place d'une page web potentiellement polémique durant la période électorale.

Pour ce qui est de la responsabilité des acteurs politiques sur la gestion de la finalité des traitements, la CNIL a récemment actualisé sa doctrine pour la mettre en phase avec le RGPD. En rappelant que, pour être licite, la transmission des données aux partis, élus ou candidats à des fonctions politiques doit être prévue lors de la création du fichier contenant les données, la CNIL rappellera à l'ordre une députée de la Manche et le rectorat de l'académie de Normandie[202], dans le cadre de l'envoi par celle-ci à la députée des fichiers de nombreux élèves conçus en dehors du cadre de la communication politique.

Des questions concernant la sécurité des systèmes d'information des acteurs politiques et ses partenaires se poseront davantage à l'heure de la montée en importance du microciblage électoral en ligne. La protection des données des électeurs, davantage convoitées, fera désormais appel à un niveau de sécurité de système plus accentué de la part des acteurs politiques afin de prévenir des atteintes à la confidentialité, disponibilité, ou intégrité[203] des données des électeurs susceptibles de mettre à mal leurs droits et libertés.

C'est bien pour parer à ces risques que le RGPD consacre dans son article 32, en reprenant l'essence de l'article 17 de la Directive 95/46/CE, l'obligation des responsables de traitement et des sous-traitants de mettre en œuvre des mesures techniques et organisationnelles à même de garantir un niveau de sécurité adapté au risque que le traitement implique.

[201] Site internet officiel du parti communiste français : www.pcf.fr/mentions_legales, consulté en ligne le 26 mai 2021, 16h14.
[202] Délibération CNIL SAN-2020-005, du 3 septembre 2020.
[203] Selon le ministère de la défense, la sécurité des systèmes d'information se définit comme l'ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. *In* « La cyberdéfense » site internet officiel du Ministère des Armées, consulté en ligne le 20 mai 2021, 19h36.

À ce sujet, l'autorité de contrôle italienne impose en 2019 une amende conséquente à une entité liée au Movimento 5 Stelle dans le cadre de la mise en place d'un système de vote en ligne créé pour favoriser le déroulement des élections au sein du mouvement[204]. L'autorité condamne ainsi l'entité organisatrice du scrutin au paiement d'une sanction de 50 000 euros sur la base du non-respect des critères de l'article 32 du RGPD. À noter qu'il est reproché aux responsables de traitement non pas l'absence d'adoption de mesures de sécurité les plus performantes du marché, mais d'un niveau de sécurité adapté au risque que le système de vote en ligne représente.

Il est judicieux, enfin, de souligner que la sécurité du traitement des données des électeurs est spécialement importante durant la période électorale, où la confiance des électeurs est sollicitée davantage par les formateurs d'opinion et candidats.

Pour ce qui concerne l'analyse d'impact relative à la protection des données, le RGPD impose aux acteurs politiques l'obligation d'en effectuer une si les traitements mis en place sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment lorsqu'ils font appel à l'évaluation systématique et approfondie d'aspects personnels des électeurs, ou au traitement à grande échelle de catégories particulières de données[205].

Il est ainsi possible que les acteurs politiques, en s'appuyant sur des logiciels de stratégie électorale pour cibler et profiler les électeurs, ou en cas de traitement volumineux des opinions politiques, engendrent les risques évoqués aux droits et libertés des électeurs. Cela devrait être pris en compte par ces acteurs lors de la conception du traitement, pour envisager en amont ces risques et déterminer des actions susceptibles d'être mises en place en cas de vérification du risque.

---

[204] « *Dans les deux cas, et dans tous les autres où le système de vote électronique de l'Association de Davide Casaleggio a été utilisé, il n'est pas techniquement possible d'exclure 'd'éventuelles altérations' des résultats en raison de la faible sécurité de la structure, qui persiste malgré la suppression de certaines des vulnérabilités signalées précédemment, notamment en raison de 'l'obsolescence des systèmes utilisés.'* », traduction libre de « Il Garante per la privacy multa Rousseau per 50 mila euro: 'Il sistema di voto non è adeguato' *», Corriere della sera*, 18 avril 2019 (dernière modification), consulté en ligne le 20 mai 2021, 20h57.

[205] Article 35, paragraphe 3, alinéas « a » et « b » du RGPD.

En mars 2021, l'autorité de contrôle britannique est venue offrir aux opérateurs du droit des clés de lecture supplémentaires à ce sujet, en indiquant qu'une analyse d'impact est également requise lorsque les acteurs politiques combinent ou croisent des données appartenant à des différentes sources d'information ou bien collectent les données des électeurs auprès des tiers sans que ceux-ci en soient prévenus[206].

Finalement, comme n'importe quel autre responsable de traitement, les acteurs politiques et les fournisseurs de logiciel de stratégie électorale peuvent faire l'objet de sanctions prononcées par la formation restreinte de la CNIL par méconnaissance de leurs obligations relevant de la protection de la donnée personnelle des électeurs. Avec le RGPD, le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros, ou dans le cas d'une entreprise (comme les fournisseurs des solutions), jusqu'à 4 % du chiffre d'affaires annuel mondial. Ces sanctions peuvent être rendues publiques au seul critère de la CNIL.

Eu égard au nouveau paysage de la communication politique inauguré par les logiciels de stratégie électorale, il convient désormais de porter un regard sur les nouvelles perspectives de règlementation de la matière et des solutions aux risques et au cadre juridique inachevé soulignés dans les paragraphes précédents.

Section 2 – Nouvelles perspectives de règlementation de la communication politique – le droit dur et le droit souple

L'utilisation de l'intelligence artificielle dans la communication politique française pour prospecter, fidéliser et comprendre les habitudes des électeurs a connu un essor dans les échéances électorales nationales de 2016-2017. Les révélations liées aux mauvaises utilisations des données personnelles des électeurs par Cambridge Analytica ont paru en mars 2018. Le RGPD, à son tour, est entré en application dois mois après, mai 2018. Des décalages entre ce texte et les pratiques adoptées récemment par les acteurs politiques en France pour s'adresser aux électeurs ont dès lors été repérés. Il convient ainsi, dans cette dernière section, de s'intéresser aux projets et perspectives de règlementation juridique qui peuvent encadrer davantage ces nouvelles pratiques de communication politique (**Paragraphe 1**), pour ensuite s'intéresser à quelques initiatives mises en avant à l'heure actuelle par les parties prenantes du

[206] « Guidance for the use of Personal Data in Political Campaigning », *ICO*, 09 mars 2021, p. 20.

débat politique pour mieux maîtriser les risques que ces nouvelles pratiques impliquent (**Paragraphe 2**).

Paragraphe 1 – Une réglementation juridique possible

Comme le fait savoir l'Union Européenne par son Office des publications, les nouveaux moyens de communication sur internet, comme la voix sur IP, la messagerie instantanée et le courrier électronique ne sont en général pas soumis au cadre réglementaire actuel de l'Union en matière de communications électroniques, notamment à la Directive 2002/58/CE, la Directive *e-Privacy*[207].

Or, la messagerie instantanée et le courrier électronique sont devenus des grands alliés des acteurs politiques. Pour diminuer le décalage législatif existant à l'égard de la réalité des communications, une nouvelle proposition de Règlement concernant les communications électroniques est en débat au sein du Conseil. Cette proposition abrogera la Directive 2002/58/CE et uniformisera l'application des règles d'obtention de consentement dans les États membres dans le cadre de ces nouveaux moyens de communication.

La proposition a donc vocation à faire un progrès important dans la règlementation de l'utilisation des données personnelles dans le cadre des communications commerciales. En ce qui concerne la communication politique, des législations spécifiques sont encore au rendez-vous dans les États membres.

Une autre initiative a été présentée en décembre 2020 par la Commission européenne. Le Digital Service Act, qui vise à proposer un cadre harmonisé de règles pour les services en ligne en matière de modération des contenus illicites et transparence du service, a été également proposé sous forme de Règlement.

Avec des incidences potentielles concernant la relation entre les acteurs politiques et les fournisseurs de logiciels de stratégie électorale lorsque ceux-ci fonctionnent en tant

[207] Exposé de motifs de la proposition de Règlement du Parlement et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques. Cette directive se cantonne à poser un principe de consentement de la personne concernée notamment en matière de courriers électroniques du type SMS ou MMS.

qu'hébergeurs de contenus (Article 2, alinéa « f »)[208]. Si adopté tel quel, ce texte, qui définit le service d'hébergement comme le simple stockage des informations fournies par un bénéficiaire du service, n'apportera d'innovation significative sur la notion d'hébergeur dégagée par la jurisprudence européenne[209]. Dans le même sens, le faible degré de responsabilisation des hébergeurs existant aujourd'hui dans le dispositif européen sera maintenu[210].

Malgré ces avancées, le véritable apport des textes en gestation se retrouve dans une autre proposition de Règlement publiée par la Commission européenne en avril 2021 établissant des règles harmonisées sur l'intelligence artificielle. L'*Artificial Intelligence Act*[211], très attendu par les juristes, a vocation à combler des vides législatifs importants, notamment par le biais de ces définitions encadrantes, quarante-quatre au total, la nomination des acteurs concernés, la typologie dressée des systèmes d'intelligence artificielle et des responsabilités qui en découlent.

Sans tomber dans le piège de définir ce que serait l'« intelligence artificielle », la Commission adopte une approche plus englobante en choisissant de définir plutôt les « systèmes d'intelligence artificielle ». La définition renvoie, dans ses grandes lignes, à celle posée par la CNIL en 2017 pour le terme « algorithme », abordée dans la première partie de ce travail[212] : la Commission, comme la CNIL, allie l'acte machinal à l'obtention de résultats escomptés à partir d'instructions prédéfinies.

Le système d'intelligence artificielle est ainsi défini comme un logiciel développé en faisant appel à une ou plusieurs techniques, parmi lesquelles la plus célèbre, appelée l'auto-apprentissage ou *machine learning*, mais également les techniques statistiques, les estimations *bayesiennes*[213] et les méthodes de recherche et d'optimisation (Article 3, paragraphe 1er). Or, la définition aurait tendance à concerner les logiciels de stratégie électorale, en vertu de leurs

[208] Proposition de Règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la Directive 2000/31/CE.
[209] CJUE, 23 mars 2010, *Google c. Louis Vuitton Malltetier*, affaires C-236/08 à C-238/08.
[210] Selon le texte actuel de la proposition de Règlement, la responsabilité de l'hébergeur ne pourra être engagée que si l'hébergeur n'ait pas connaissance de l'activité ou du contenu illicite, ou, dès le moment où il en a connaissance ou conscience, il agisse promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible.
[211] Comm. eur., 21 avr. 2021, COM(2021) 206 final, Artificial Intelligence Act.
[212] « *Comment Permettre à l'Homme de Garder la Main ?* », Synthèse du débat public animé par la CNIL dans le cadre de la réflexion éthique confiée par la loi pour Une République Numérique, 2017, p. 15.
[213] The Bayes theorem « *is a simple mathematical formula used for calculating conditional probabilities. It figures prominently in* subjectivist *or* Bayesian *approaches to epistemology, statistics, and inductive logic. Subjectivists, who maintain that rational belief is governed by the laws of probability, lean heavily on conditional probabilities in their theories of evidence and their models of empirical learning. Bayes' Theorem is central to these enterprises both because it simplifies the calculation of conditional probabilities and because it clarifies significant features of subjectivist position.* », *in Stanford Encyclopedia of Philosophy,* le 30 septembre 2003 (dernière modification), consulté en ligne le 23 mai 2021, 14h55.

modèles statistiques et inférentiels, alors même que leurs détails logiques demeurent largement protégés par le secret industriel.

Trois autres définitions importantes sont dégagées par le texte de la proposition : 1) « fournisseur » : la personne qui développe ou fait développer le système d'intelligence artificielle en vue de le mettre sur le marché ou en service sous son propre nom ou sa propre marque ; 2) « distributeur » : la personne dans la chaîne d'approvisionnement autre que le fournisseur ou l'importateur qui rend le système disponible sur le marché de l'Union européenne sans en affecter les propriétés ; et 3) « utilisateur » : toute personne utilisant le système sous son autorité, hormis le cas d'utilisation personnelle non professionnelle (Article 3, paragraphes 2, 4 et 7).

Il est évident que les fournisseurs français de solutions en stratégie électorale, comme eXplain, DigitaleBox et Spallian peuvent être assimilés à des fournisseurs à des fins de la proposition, du fait même de la technologie propriétaire sous-jacente aux logiciels. Des entreprises étrangères comme Nationbuilder, en revanche, seraient soit assimilables à des distributeurs, lorsqu'un de leur représentant n'affectant pas les propriétés de la solution s'occuperait de la mise en marché de celle-ci en Europe, soit à des fournisseurs, lorsque le représentant s'occupant de sa mise en marché en Europe modifierait en quelque sorte les propriétés de la solution avant ou durant la mise en marché. Enfin, les acteurs politiques, comme les partis politiques, élus et candidats à des fonctions électives, seraient assimilables à des utilisateurs, en tant que parties qui se prévaudront de la solution pour faire de la communication politique.

Pour ce qui est de la typologie des systèmes d'intelligence artificielle, les systèmes impliquant des pratiques présentant un risque inacceptable sont prohibés (Article 5)[214], ceux présentant un haut risque sont soumis à un régime de mise en conformité détaillé (Article 6 à 51) et ceux présentant un faible risque font l'objet d'obligations de transparence (Article 52)[215].

[214] Parmi ces pratiques, on retrouve celles utilisées pour manipuler le comportement humain, l'exploitation de vulnérabilités d'un groupe social handicapé, la surveillance de masse et le *social scoring*.
[215] L'article 52 de l'*Intelligence Artificial Act* régule quelques modalités de systèmes d'IA, qu'ils soient à haut risque ou non.

Si les logiciels de stratégie électorale n'impliqueraient en principe un risque inacceptable aux électeurs, des hésitations pourraient se prêter à leur classification en tant que systèmes présentant un haut ou faible risque. Sachant que l'approche adoptée par la Commission pour caractériser les systèmes à haut risque est à la fois sectorielle et matérielle, on voit mal la possibilité de faire échapper une grande partie de ces logiciels à la catégorie de systèmes à haut risque.

La responsabilisation des acteurs concernés par la proposition de Règlement est envisagée à l'aune de l'apposition de leur nom ou marque sur le système d'intelligence artificielle. La définition de fournisseur évoquée en est un indice. Dans le même ordre d'idées, les distributeurs, importateurs ou utilisateurs seront considérés comme des fournisseurs lorsque leur nom ou marque y sont également apposés, ce qui, selon l'article 28 de la proposition, entraînerait l'application à ces acteurs de toutes les obligations à la charge du fournisseur[216].

Ce partage de responsabilités porte des effets considérables aux acteurs politiques, en ce que la communication politique réalisée à l'appui de ces outils devra désormais être assurée en associant la pièce de communication politique au nom ou à la marque des fournisseurs des outils, pour pouvoir faire échapper les acteurs de tout grief porté par les électeurs sous l'argument de la mauvaise utilisation de leurs données.

Les acteurs politiques, en tant qu'utilisateurs des systèmes d'intelligence artificielle, se voient eux-aussi attribuer des obligations spécifiques par le texte. À ce titre, celle qui impose aux utilisateurs la vérification de la pertinence des données collectées à être utilisées dans les systèmes, lorsque ces utilisateurs exercent un contrôle sur les données d'entrées (Article 29, paragraphe 3). Avec ce dispositif, le contrôle de l'adéquation des données personnelles à la finalité pour laquelle elles ont été collectés auprès des électeurs a ainsi vocation d'être renforcé. Cela cristalliserait, dans la figure des acteurs politiques, un obstacle bienvenu à la tendance montante d'inférences et déductions algorithmiques des données, atténuant les risques d'atteinte à la limitation des finalités du traitement des données personnelles soulevés dans le paragraphe premier de section précédente.

[216] Article 16, *id*.

Cette nouvelle règle, couplée à d'autres obligations comme celle impartie aux utilisateurs d'utiliser le système conformément aux instructions d'utilisation posées par le fournisseur, des obligations d'information à destination des utilisateurs (Article 13), de surveillance humaine (Article 14), et de robustesse, d'exactitude et de sécurité (Article 15), constitueront des gages contre des atteintes aux droits et libertés fondamentaux des électeurs, les véritables bénéficiaires de ce cadre normatif actuellement en phase de discussion dans le Conseil de l'Union européenne.

Finalement, l'article 52 du texte prévoit des obligations de transparence aux fournisseurs de systèmes d'intelligence artificielle destinés à interagir avec des personnes physiques. Si le texte est adopté en état, les fournisseurs devront s'assurer que leurs systèmes soient conçus de manière à permettre aux personnes physiques d'être informées qu'elles interagissent avec un système d'intelligence artificielle. Le même article pose aussi une règle importante dans le cadre du combat contre les *deepfakes*, en ce qu'il inscrit dans le marbre pour la première fois l'obligation d'informer le public du fait que le contenu a été artificiellement généré ou manipulé.

Face à ce cadre normatif qui s'annonce dans le paysage européen et français, il convient de souligner d'autres initiatives qui ont été ou seront prises par les acteurs sociaux afin d'endiguer certains risques relevant de la communication politique, au niveau mondial et européen.

Paragraphe 2 – Une autorégulation incontournable par les acteurs du Web

L'intelligence artificielle ayant vocation à s'appliquer partout où la communication politique peut engager des citoyens et électeurs, l'approche multi-partisane, qui rendrait possible la participation des acteurs publics et privés, à la société civile et troisième secteur dans la construction d'un modèle idéal de gouvernance algorithmique, est de rigueur.

En suggérant que ces approches doivent être le plus hétérogènes possible, l'UNESCO a tenu à rappeler les intéressés en 2019, dans le cadre de l'étude « *What if we all governed internet ?* », que l'absence de participation du secteur privé s'est avérée susceptible d'affaiblir

la légitimité et l'efficacité des initiatives multi-partisanes, entraînant d'ailleurs, dans certains cas, des atteintes à des droits humains[217].

En Octobre 2018, des opérateurs importants des plateformes de communication et d'autres parties prenantes du débat politique en ligne se sont réunis autour du Code de Bonnes Pratiques Contre la Désinformation, entré en vigueur en Europe. Ce Code, bien que dépourvu de force normative, affiche comme l'un de ces principaux objectifs la mise en cause les revenus publicitaires des partis faisant relayer les désinformations[218].

Des acteurs majeurs comme Google, Facebook, Twitter, Microsoft, Mozilla et TikTok ayant adhéré à l'instrument, les acquis du Code se sont vite fait sentir : Facebook a fait savoir qu'il prenait acte contre 600.000 annonces par mois dans l'Union Européenne depuis le début 2019, en mettant en cause des contenus considérés comme trompeurs ou faux. Google et Twitter ont également indiqué avoir pris des décisions à l'égard des milliers d'utilisateurs pour non-respect de leurs politiques de divulgation de contenu et publicité[219].

Wikipédia a suivi l'initiative de la Commission pour proposer, en février 2021, le premier code de conduite universel contre l'abus, la manipulation et le la désinformation sur sa plateforme. À la transversalité de l'autorégulation adoptée par l'encyclopédie en ligne s'ajoute la variété des volontaires participant à l'élaboration du code[220].

Si l'incidence des algorithmes se fait moins sentir dans les activités de Wikipédia, la Commission européenne, chef de file des efforts derrière la mise en place du Code de Bonnes Pratiques Contre la Désinformation, n'a pas manqué l'occasion d'y insérer une disposition par laquelle les signataires reconnaissaient l'importance de coopérer afin de fournir, parmi d'autres, des informations générales sur les algorithmes impliqués dans la réalisation des objectifs du Code (Section 1 – Finalités, alinéa « xi »).

---

[217] « Steering AI and advanced ICTs for knowledge societies: a Rights, Openness, Access, and Multi-stakeholder Perspective », *UNESCO Publishing*, 2019, p. 121.

[218] Si la notion de « désinformation » adoptée par ce Code est plus large que celle posée par la loi française du 22 de décembre de 2018 aux « fausses informations », les deux textes reprochent également le fait de relayer des informations trompeuses aux citoyens dans le contexte politico-électoral.

[219] Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, *Commission Staff Working Document*, 10 septembre 2020, p. 4.

[220] « *More than 1,500 Wikipedia volunteers from 19 different Wikipedia projects representing five continents and 30 languages participated in the creation of the universal code of conduct* ». *In* « Wikipedia Embraces First-of-Its Kind Universal Code of Conduct, Conceived For The New Internet Era », *Wikimedia Foundation*, 02 février 2021, consulté en ligne le 24 mai 2021, 19h27.

En faisant un bilan de la première année d'entrée en vigueur de ce Code, la Commission a estimé que, malgré les avancées atteintes grâce aux signataires du Code – concernant notamment le combat contre les spams, faux comptes et comptes dirigés par les *bots* –, des efforts restent à faire au niveau de la transparence des informations comme les acteurs, le contenu, les mécanismes de diffusion et les modes de propagation des messages destinés à manipuler l'opinion publique[221], que les signataires sont censés rendre à la Commissions à des échéances spécifiques. Or, afin de saisir l'évolution des menaces et des tendances des campagnes de désinformation dans le cadre des objectifs fixés par le Code, ces informations sont d'importance capitale.

Il est néanmoins à regretter que la Commission n'ait pas adressé des impressions spécifiquement sur la transparence algorithmique des signataires dans le cadre de ce bilan, que ceux-ci devaient assurer dans le cadre de la Section 1 du Code. En toute hypothèse, la proposition de Règlement établissant des règles harmonisées sur l'intelligence artificielle évoquée dans le paragraphe précédent aurait, de par sa force normative, vocation à combattre le laxisme des plateformes vis-à-vis de leurs compromis assumés dans le cadre de ce Code.

D'autres initiatives ont également été repérées dans le troisième secteur. L'entité « PersonalData.IO » prétend, par exemple, vulgariser l'accès aux droits relevant de la protection des données personnelles, en leur rendant « *personnellement actionnables et collectivement utilisables* »[222]. Soutenue par des activistes, chercheurs et éducateurs, la plateforme vise encourager des dynamiques collaboratrices entre le grand public et la société civile pour relayer davantage ces droits qui restent pour la plupart assez inconnus. Cela pourrait sûrement profiter aux électeurs avant et durant la période électorale, comme le souhaitaient les fondateurs de la plateforme au départ[223].

Le risque d'un débat politique en ligne faussé par les techniques de microciblage et l'intelligence artificiel n'étant pas moindres, les spécialistes ont pris part à la défense de plus de transparence autour de la technique concernant la prise de décision algorithmique. Il a même

[221] Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, *Commission Staff Working Document*, 10 septembre 2020, p. 9.
[222] « Welcome to PersonalData.IO », *PersonalData.IO,* 02 octobre 2020 (dernière modification), consulté en ligne le 24 mai 2021, 23h06.
[223] « Cambridge Analytica, big data et gros dégâts », *Libération,* 17 août 2017, consulté en ligne le 24 mai 2021, 23h32.

été suggéré de renvoyer aux acteurs sociaux exploitant les technologies de personnalisation de la communication la charge des audits de leur algorithmes[224]. En France, l'audit des algorithmes reste à l'heure actuelle une affaire non tranchée par la jurisprudence.

Il convient de relever que l'approche des acteurs du Web vers l'autorégulation aurait d'ailleurs vocation à freiner l'activité législative dans le territoire où l'autorégulation est mise en place, si bien encadrée en amont et exécutée par les parties prenantes. Contrairement aux lois, la souplesse des engagements pris en dehors du cadre normatif institutionnalisé peut servir à implémenter et changer les engagements en cours de route, ce qui a un intérêt particulier à l'ère des bouleversements technologiques, où l'innovation met à chaque fois en cause l'adéquation et complétude de ce cadre normatif.

Des controverses demeurent autour du véritable intérêt qui auraient des compagnies comme Facebook et Twitter à faire avancer la régulation algorithmique dans leurs plateformes en ligne, eu égard à l'inhérence de leur modèle de business, qui encourage l'engagement des utilisateurs. Plus le contenu partagé est polémique et biaisé, voire porteur de mensonges[225], plus il est susceptible d'engager d'autres utilisateurs et, donc, plus les plateformes sont attirantes aux annonceurs. À cet égard, Twitter a récemment[226] fait savoir que sa politique de labélisation de désinformation concernant des élections ou des procédures civiques allait être renforcée, pour offrir plus de contexte sur les informations relayées sur la plateforme. Des tweets labélisés comme trompeurs ou mettant en cause ces manifestations démocratiques ont depuis lors leur visibilité réduite sur la plateforme. La mesure, en vigueur depuis septembre 2020, a vocation à être appliquée aux États-Unis et d'autres pays.

Outre cette initiative – déjà appliquée par Facebook et améliorée par celui-ci récemment[227], les spécialistes de l'éthique de l'intelligence artificielle mettent en avant une alternative porteuse de réglementation des algorithmes tenant essentiellement à trois points : dépriorisation de l'engagement en ligne par les Big Tech, des partenariats avec des agences de presse et détection de la désinformation à l'appui des volontaires et de l'intelligence

[224] « *I propose algorithm auditing as a compatible ethical duty for providers of content personalization systems to maintain the transparency of political discourse* ». *In* B. MITTELSTADT, « Auditing for Transparency in Content Personalization Systems », *Oxford Internet Institute*, 2016, p. 2.
[225] « The spread of true and false news online », *Science*, 9 mars 2018, consulté en ligne le 08 juin 2021, 18h16.
[226] « Expanding our policies to further protect the civic conversation », *Twitter*, 10 septembre 2021, site internet officiel consulté en ligne le 08 juin 2021, 18h38.
[227] « Facebook a une idée contre les fake news : plus vous partagez, moins vous serez visible », *Numerama*, 27 mai 2021, site internet officiel consulté en ligne le 08 juin 2021, 19h10.

artificielle[228]. L'intérêt de cette approche plurilatérale est évident pour le déroulement optimal de la communication politique, qui est elle-même source de polémique et désinformation dans certains régions du monde.

Alors même que des obstacles importants sont au rendez-vous, il semble plus que nécessaire que ces acteurs, publics et privés, la société civile et le troisième secteur, mettent en avant des compromis permettant d'encadrer davantage l'utilisation algorithmique durant la période électorale. Mis en pratique de manière intelligente, à l'échelon continental ou, du moins, transnational, cet encadrement pourrait favoriser sensiblement la communication politique, sans pour autant figer les pratiques entrepreneuriales propres à chaque acteur privé en dehors du cadre des élections.

***

Dans cette deuxième partie, nous avons abordé les techniques plus raffinées de prospection et fidélisation des électeurs, employées notamment à l'aide des logiciels de stratégie électorale. La vulgarisation de l'accès à ces outils parmi les partis, élus et candidats à des fonctions électives entraîne des changements importants dans la communication politique. Ces changements, portant notamment sur l'accentuation du degré de la personnalisation du message communiqué aux électeurs, sont largement viabilisés par la mise en Big data des données personnelles des électeurs, et d'autres données non personnelles, et la puissance algorithmique qui voit le jour dans les années 2010. Des avancées juridiques sont faites par le législateur national et européen pour confier aux personnes concernées (dont les électeurs) un niveau plus important de maîtrise de leurs données personnelles, ce qui comble quelques faiblesses existantes jusqu'alors à ce niveau. Ces avancées s'avèrent aussitôt insuffisantes concernant la communication politique, eu égard à sa personnalisation montante, qui dépasse en complexité les bornes protectrices posées par ce cadre juridique. Sensibles au besoin de répondre à ces impératifs, la communauté juridique et des acteurs publics et privés – les institutions européennes, les Big Tech et le troisième secteur –, avancent des alternatives qui s'annoncent comme des points de repères importantes à la prise de décision et à l'élaboration de politiques publiques robustes pour la matière.

[228] SUSARLA, A. « If Big Tech has the will, here are ways research shows self-regulation can work », *The Conversation*, 22 février 2021.

BIBLIOGRAPHIE

I – OUVRAGES

- GLOTZ G., *La cité grecque*, Albin Michel, 1928
- MAYOL S., *Le Marketing 3.0*, Chapitre 2, Marketing 1.0, 2.0 et 3.0, Dunod, 2011
- THÉVIOT A., *Big Data Électoral, dis-moi qui tu es, je te dirai pour qui voter*, Le Bord de l'Eau, 2019

II – ARTICLES

- BARBONI T. ; TREILLE É., *l'Éngagement 2.0 – Les nouveaux liens militants au sein de l'e-parti socialiste*, Presses de Sciences Po, 2010
- BARDIN M., *Les partis politiques et l'outil numérique*, Pouvoirs, 2017
- BARQUISSAU E. ; SCHLENKER L., *Marketing et Communication Politique,* EMS Editions, 2017
- BELEN V., *Les tentatives de protection des données personnelles des individus : difficultés de définition et risques nouveaux*, ESKA, 2005
- CHAUVEAU A., *L'Homme Politique et la Télévision*, Presses de Sciences Po, 2003
- CHESNEY R.; CITRON D. K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, 2018
- DAADOUCH C., *Listes électorales, une exploitation contestable*, Plein droit, n° 28, 1995
- DUBOIS L.; GAULLIER F., *Publicité ciblée en ligne, protection des données à caractère personnel et e-Privacy : un ménage à trois délicat*, Legicom, 2017
- FATÔME A. D., *Principe de finalité du traitement - Un office public de l'habitat rappelé à l'ordre par la CNIL et le Conseil d'État !*, Commentaire 92, Communication Commerce électronique, n° 12, 2020
- FOURETS F., *La protection des données, ou le symbole d'une démocratie nouvelle*, Caisse nationale d'allocations familiales, 2005
- FRAYSSINET J., *La communication et l'utilisation des listes électorales : de l'organisation du scrutin à la communication politique*, La Semaine Juridique Edition Générale, 1989
- GERBER A. S.; GREEN D. P., *The Effects of Canvassing, Direct mail, and Telephone Contact on Voter Turnout: A Field Experiment*, American Political Science Review, Vol. 94, n. 3, 2000

- GERSTLÉ J. ; PIAR C., *La communication politique*, Armand Colin, 2020
- GHEVONTIAN R., *La notion de sincérité du scrutin*, Cahiers du Conseil constitutionnel, 2013 ; et *La sincérité du scrutin, études réunies et présentées par Richard Ghevontian*, Cahiers du Conseil constitutionnel, 2013
- GUILLOU, P., *Être un élu 2.0 et gérer sa e-réputation sur internet*, cours assuré à des élus locaux, 2010
- KOLLANYI B., *Where Do Bots Come From? An Analysis of Bot Codes Shared on GitHub*, International Journal of Communication, 2016
- LOISEAU G., *La démocratie électronique municipale française : au-delà des parangons de vertu*, CNRS Éditions, 2000
- MAUNIER C., *La Communication politique en France, un état des lieux*, Éditions ESKA, 2006
- MITTELSTADT B., *Auditing for Transparency in Content Personalization Systems*, Oxford internet Institute, 2016
- MOLE A., *Protection des personnes sur internet : conditions posées par la CNIL*, Victoires Éditions, 1995
- POIDEVIN B., *La réforme de la loi Informatique et Libertés : la loi du 6 août 2004*, Juris Expert, 2004
- SAMUEL G., *Outils d'écriture du Web et industrie du texte : Du code informatique comme pratique lettrée*, Réseaux, vol. 206, n° 6, 2017
- SERUGA-CAU É. ; HAVEL T., *Campagne Électorale et Utilisation des Données Personnelles : Grands Principes et Points de Vigilance*, Actualité Juridique Collectivités Territoriales, 2019
- SOUBRIÉ T., *Le blog : retour en force de la fonction d'auteur*, Colloque JOCAIR, 2006
- SUSARLA, A., *If Big Tech has the will, here are ways research shows self-regulation can work*, 2021
- TALPIN J.; BELKACEM R., *Frapper aux portes pour gagner des élections ?*, De Boeck Supérieur, 2014
- THÉVIOT A., *Les data : nouveau trésor des partis politiques – Croyances, constitutions et usages comparés des données numériques au Parti Socialiste et à l'Union pour un Mouvement Populaire*, Politiques de Communication, 2016
- WOOLEY S. C. ; HOWARD P. N., *Political Communication, Computational Propaganda, and Autonomous Agents*, International Journal of Communication 10, 2016

III – RAPPORTS ET LITTERATURE INSTITUTIONNELLE

A – Guides

- CNIL, « Communication Politique – Obligations Légales et Bonnes Pratiques », 2012
- CNIL et Conseil Supérieur de l'Audiovisuel, « Campagnes électorales : tout savoir sur les règles CSA et CNIL », 2016
- CNIL, « Comment Permettre à l'Homme de Garder la Main », Synthèse du débat public animé par la CNIL dans le cadre de la réflexion éthique confiée par la loi pour Une République Numérique, 2017
- ICO, « Democracy Disrupted, Personal information and political influence », 2018
- ICO, « Guidance for the use of Personal Data in Political Campaigning », 2021

B – Rapports d'Activités CNIL

- 6e Rapport d'Activités CNIL, 1985
- 12e Rapport d'Activités CNIL, 1991
- 15e Rapport d'Activités CNIL, 1994
- 16e Rapport d'Activités CNIL, 1995
- 26e Rapport d'Activités CNIL, 2005
- 27e Rapport d'Activités CNIL, 2006
- 28e Rapport d'Activités CNIL, 2007
- 32e Rapport d'Activités CNIL, 2011
- 33e Rapport d'Activités CNIL, 2012
- 34e Rapport d'Activités CNIL, 2013
- 35e Rapport d'Activités CNIL, 2014
- 36e Rapport d'Activités CNIL, 2015
- 37e Rapport d'Activités CNIL, 2016
- 38e Rapport d'Activités CNIL, 2017
- 39e Rapport d'Activités CNIL, 2018
- 40e Rapport d'Activités CNIL, 2019
- 41e Rapport d'Activités CNIL, 2020

C – Délibérations rendues par la CNIL

- Délibération CNIL nº 83-58 du 29 novembre 1983
- Délibération CNIL nº 85-60 du 5 novembre 1985
- Délibération CNIL nº 91-118 du 3 décembre 1991
- Délibération CNIL nº 96-105 du 3 décembre 1996
- Délibération CNIL nº 2006-138 du 9 mai 2006
- Délibération CNIL nº 2006-228 du 5 octobre 2006
- Délibération CNIL nº 2012-020 du 26 janvier 2012
- Délibération CNIL nº 2012-021 du 26 janvier 2012
- Délibération CNIL nº 2015-040 du 12 février 2015
- Délibération CNIL n° 2016-315 du 13 octobre 2016
- Délibération CNIL n° 2019-093 du 4 juillet 2019
- Délibération CNIL n° SAN-2020-005 du 3 septembre 2020

D – Autres

- Cédric Villani, « Donner un Sens à l'Intelligence Artificielle », 2018
- CNIL, « Point d'étape relatif à l'activité de l'Observatoire des élections : Bilan et perspectives à l'aune du RGPD », 2019
- CEPD, « Déclaration 02/2019 sur l'utilisation de données personnelles dans le cadre des campagnes politiques », 2019
- Commission européenne, « Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, *Commission Staff Working Document* » 2020
- Federal Trade Commission (FTC), « Complaint No. 182 3107, in the matter of Cambridge Analytica », 2019
- G29, « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 », 2018
- LSE Media Policy Project, « The new political campaigning », 2017
- Parlement européen, Conseil de l'Union européenne et Commission européenne, « Guide Pratique commun du Parlement européen, du Conseil et de la Commission à l'intention des personnes qui contribuent à la rédaction des textes législatifs de l'Union européenne », 2015
- UNESCO Publishing, « Steering AI and advanced ICTs for knowledge societies: a Rights, Openness, Access, and Multi-stakeholder Perspective », 2019

IV – TABLE DE JURISPRUDENCE

A – Jurisprudence européenne

- CJUE, 23 mars 2010, *Google c. Louis Vuitton Malltetier*, affaires C-236/08 à C-238/08
- CJUE, 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, affaire C-210/16

B – Jurisprudence constitutionnelle

- Cons. const., 2002-2690 AN, 20 janvier 2003, *A.N., Paris*
- Cons. const., 2012-4589 AN, 7 décembre 2012, *A.N., Meurthe-et-Moselle*
- Cons. const., 2012-4606 AN ; 2012-4622 AN et 2012-4635 AN, le 20 juillet 2012
- Cons. const., 2013-673 DC, 18 juil. 2013
- Cons. const., 2018-773 DC, 20 déc. 2018

C – Jurisprudence administrative

- CE, 28 sept. 2016, (affaire n° 389448)
- CE, section avis, 9 juin 2020 (affaire n° 400322)
- CE 9e et 10e chambres réunies, 4 oct. 2020 (affaire n° 433311)

V – ENCYCLOPEDIES ET DICTIONNAIRES

- Centre de Recherches Inter-Langues sur la Signification en Contexte (CRISCO)
- Centre National de Ressources Textuelles et Lexicales
- Dictionnaire Larousse Bilangue (Français-Anglais)
- Dictionnaire WordReference Bilangue (Français-Portugais)
- Grand Dictionnaire terminologique de l'Office québécois de la langue française
- Stanford Encyclopedia of Philosophy

VI – SITOGRAPHIE

- CAIRN, site official : https://www.cairn.info/
- CNIL, site institutionnel : https://www.cnil.fr/

- Corriere della sera, site officiel : https://www.corriere.it/
- C-Marketing : https://c-marketing.eu/
- Eurlex, l'accès au droit de l'UE : https://eur-lex.europa.eu/homepage.html?locale=fr
- eXplain, site officiel : https://explain.fr/
- France Culture, site officiel : https://www.franceculture.fr/
- Franceinfo, site officiel : https://www.francetvinfo.fr/
- ICO, site institutionnel : https://ico.org.uk/
- Israel Public Policy Institute, site officiel : https://www.ippi.org.il/
- Journal du Net, site officiel : https://www.journaldunet.com
- Légifrance, site institutionnel : https://www.legifrance.gouv.fr/
- Les Echos, site officiel : https://www.lesechos.fr/
- Libération, site officiel : https://www.liberation.fr/
- Le Figaro, site officiel : https://www.lefigaro.fr/
- Le Monde, site officiel : https://www.lemonde.fr/
- Le Parisien, site officiel : https://www.leparisien.fr/
- L'Obs, site officiel : https://www.nouvelobs.com/
- Ministère des Armées, site institutionnel : https://www.defense.gouv.fr/
- New York Times, site officiel : https://www.nytimes.com/
- Nationbuilder, site officiel : https://nationbuilder.com/
- Nextinpact, site officiel : https://www.nextinpact.com/
- Numerama, site officiel : https://www.numerama.com/
- Parti communiste français, site officiel : www.pcf.fr/
- Science, site officiel : https://science.sciencemag.org/
- The Brooking Institution, site officiel : https://www.brookings.edu/
- The Conversation, site officiel : https://theconversation.com
- Twitter, site officiel du blog : https://blog.twitter.com
- Vie-publique, site institutionnel : https://www.vie-publique.fr/
- ZDnet, site officiel : https://www.zdnet.fr/
- Wikimedia Foundation, site officiel : https://wikimediafoundation.org
- W3C Consortium, site officiel : https://www.w3.org/Consortium/
- Youtube, site officiel : https://www.youtube.com/

VII – AUTRES

- Résolution sur l'utilisation des données à caractère personnel à des fins de communication politique, adoptée à la 27e Conférence internationale des commissaires à la protection des données et de la vie privée (CIPDPPC), 2005

VIII – ENTRETIENS

- Valerio Motta, directeur du Web du PS. Entretien accordé à Anaïs Théviot le 21 mai 2012
- Laure Vaugeois, responsable des élections municipales chez eXplain. Entretien accordé à France Inter le 10 février 2020

TABLE DE MATIÈRES