La triche électorale en ligne

Le nouveau territoire des campagnes numériques

Par **Jean-Baptiste Soufron**

Le 29 mars 2017

À moins de quelques jours de l'élection présidentielle et de quelques semaines des élections législatives, la question de la fraude numérique se pose avec d'autant plus d'acuité que personne ne semble disposer de solutions concrètes pour y remédier.

Cela fait pourtant plusieurs années que ces nouvelles pratiques de manipulation se répandent et que les scandales s'enchaînent à l'étranger. Quel que soit le candidat, chacun peut aujourd'hui constater l'existence de campagnes de diffamation sur les réseaux sociaux, de l'enregistrement de faux followers, de l'utilisation de faux likes, du partage massif de fake news *ou du risque permanent de divulgation d'information confidentielles piratées par des groupes décidés à perturber le scrutin. Ce qui était autrefois sans importance risque désormais d'avoir un impact démesuré.*

À la suite des péripéties des récentes élections américaines, l'ensemble acteurs du numérique a pris conscience du problème et commencé la mise en place d'une certaine forme d'autorégulation. De leur côté, les acteurs des médias se sont également emparés du sujet et proposent maintenant des plateformes de vérification de l'information. Enfin, emmené par la CNIL, plusieurs institutions commencent à se mobiliser.

Au-delà, et vu l'importance de l'enjeu, il serait opportun que l'État se dote de moyens permettant de garantir la sincérité et la loyauté des scrutins. À défaut, le risque est de réagir trop tardivement et de créer des situations injustes, comme par exemple l'interdiction de vote en ligne survenue en février qui empêchera cette année une partie des français de l'étranger de pouvoir participer au scrutin. Au pire, d'autres scénarios plus graves sont désormais possibles. Il est encore temps de réagir et de se préparer. Cette note formule plusieurs recommandations :

Synthèse

- De façon générale, encadrer l'industrialisation numérique des campagnes électorales pour préserver la loyauté et la sincérité des scrutins.

- Favoriser l'auto-régulation des acteurs du numérique et des médias, mais également demander une meilleure information des usagers pendant la période électorale et un effort supplémentaire de réactivité aux notifications pendant la période électorale.

- Renforcer les obligations en matière de transparence des algorithmes pour garantir l'accès à une pluralité d'information.

- Soutenir la recherche éthique et scientifique sur les algorithmes.

- Doter l'état de moyens de les analyser et de les contrôler, sur le modèle de ce que pourrait faire la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) en matière de droit de la consommation.

- Confier à l'Autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) une mission de conseil et d'accompagnement sur la sécurité informatique auprès des candidats, pour diffuser par exemple un référentiel de sécurité des outils numériques de campagne.

- Renforcer les peines prévues pour la fraude numérique aux élections.

- Alléger la contrainte de l'impact sur le scrutin pour tenir compte des impacts indirects que peuvent avoir la manipulation en ligne.

- Mieux intégrer la prise en compte des dispositifs numériques et dans les comptes de campagne.

- Créer un délit spécifique relatif aux préparatifs de la disruption du scrutin en amont de la campagne elle-même.

En mars 2016, *Business Week* a eu l'occasion de publier les déclarations d'Andrés Sepúlveda, un informaticien de 31 ans qui affirmait avoir été payé depuis 8 ans par divers candidats pour organiser des campagnes de triche numérique lors d'élections au Mexique et dans différents pays d'Amérique du Sud[1]. Ses premières missions étaient d'abord simples : bloquer le site web d'un candidat, obtenir et publier la liste de ses soutiens et donateurs, etc. Mais, progressivement, à mesure que s'accélérait la numérisation de la société, ses missions sont devenues plus complexes et combinaient diffusion de fausses informations (f*ake news*), réseaux de *bots* (logiciels "robots" automatiques qui infectent des ordinateurs et qui peuvent être commandés à distance pour mener des attaques coordonnées), création de faux comptes sur les réseaux sociaux (Facebook, Twitter...), intelligence artificielle, *big data*, piratages de sites (*hacking*), courriels piégés (*phishing*), fraude au vote électronique, etc. Se mêlaient ainsi la manipulation des foules et le piratage technologique.

Bon an, mal an, ses services semblent avoir été suffisamment efficaces pour lui permettre de prétendre avoir altéré le résultat d'au moins cinq scrutins majeurs sur le continent au cours des huit dernières années.

À l'occasion de sa dernière mission, lors de l'élection du Président vénézuélien Nicolas Maduro, il affirme par exemple avoir réussi à prendre le contrôle du compte Twitter du candidat, conduisant ensuite à la fermeture du réseau Internet pendant une vingtaine de minutes afin d'éviter d'autres piratages aux conséquences plus graves - et notamment le piratage du site du Conseil National des Elections.

S'agit-il de scénarios réservés aux démocraties les plus fragiles de la planète ? Ce serait se bercer d'illusions, car les attaques contre les élections existent déjà ailleurs. Aux Pays-Bas, les récentes élections législatives ont été victimes d'attaques visant à rendre impossible la consultation de sites d'information sur le scrutin (attaques par déni de service ou *distributed denial of service*, DDOS). En France, le Ministre des Affaires étrangères a été contraint de supprimer la possibilité de voter par Internet pour les français de l'étranger - jugeant préférable de ne prendre aucun risque de nature à compromettre le scrutin.

En avril 2016, Bruce Schneier, un spécialiste mondial de la cybersécurité, avait déjà lancé un avertissement : « les pirates mettent les élections américaines en situation de risque ». En novembre 2016, il se faisait plus affirmatif : « des élections américaines seront piratées » - selon lui, dès lors que c'est possible, il est inévitable que cela arrive.

Mais de son point de vue, le risque le plus nouveau et le plus dangereux ne réside pas dans les attaques pirates, mais dans le recours désormais de plus en plus massif des candidats à des techniques de manipulation numérique pour convaincre les électeurs - ce qui rejoint le discours d'Andrès Sepulvéda.

[1] « How To Hack An Election », Bloomberg, 31 mars 2016

UNE CONSÉQUENCE DE L'INDUSTRIALISATION NUMÉRIQUE DES CAMPAGNES ÉLECTORALES

Comment en effet les candidats pourraient-ils se priver des nouveaux outils numériques dès lors que les préférences des électeurs sont désormais enregistrées jour après jour dans des bases de données ouvertes à tous pour leur vendre de la publicité ? Comment croire que le marché de la fabrication des réputations en lignes, par l'intermédiaire des « faux avis » (*fake reviews*) des sites de vente en ligne, ne finirait pas un jour par donner des idées à de nouveaux entrepreneurs de la politique ? Le parti démocrate américain a été l'un des plus prompts à numériser ses campagnes. Mais hormis le double mandat de Barack Obama, il est aussi l'un de ceux qui a essuyé les défaites les plus importantes depuis ces quinze dernières années. Au lieu de travailler sur l'importance de l'émotion et du narratif en politique, leurs stratèges se sont repliés sur des tactiques orientées vers la récolte massive de données personnelles des électeurs, jusqu'à créer toute une nouvelle industrie de la science politique quantitative - dont le logiciel de gestion de campagne électorale *Nation Builder* est l'exemple le plus connu.

C'est ce mouvement vers une industrialisation numérique des campagnes politiques qui est en partie responsable de la mauvaise qualité des débats publics, et qui laisser penser que le pire reste encore à venir.

Pour reprendre l'expression d'Olivier Cimelière, il existe aujourd'hui un véritable « syndrome de la boîte-à-outils »[2]. L'efficacité décuplée des techniques de communication en ligne désincarne le message et donne l'impression qu'il suffit d'installer un logiciel, d'ajuster quelques réglages, et de profiter d'un tableau de bord interactif pour observer les résultats de son opération. En combinant ce sentiment de détachement du message avec les règles traditionnelles de la responsabilité sur Internet qui protègent les « hébergeurs » et les « tuyaux », il se crée un sentiment d'impunité qui peut donner l'impression que tout est permis.

Historiquement la première campagne marquée par le numérique et les réseaux sociaux fut celle du « non » au référendum constitutionnel de 2005, donnant déjà des indices quant à la capacité du numérique à générer de la surprise à l'occasion des scrutins. Plus près de nous, les élections américaines et le référendum sur le Brexit ont aussi donné l'occasion de mettre en lumière des problèmes massifs liés à la numérisation des campagnes : faux comptes d'utilisateurs et faux *likes* sur les réseaux sociaux, qui créent l'impression artificielle qu'un message d'un candidat est largement approuvé et relayé (*Astroturfing*), diffusion de documents confidentiels par des réseaux de *hackers* avec l'aide éventuelle de puissances étrangères (WikiLeaks, etc.), publication de sondages informels pendant la période de réserve, détournement de fichiers d'électeurs, publication et partage de fausses informations, fraudes en matière de vote électronique, etc.

[2] « Communication : verra-t-on disparaître un jour ce trop récurrent syndrome de la boîte à outils ? », Olivier Cimelière, Le Blog du Communicant - http://www.leblogducommunicant2-0.com/humeur/communication-verra-t-on-disparaitre-un-jour-ce-trop-recurrent-syndrome-de-la-boite-a-outils/

Ces pratiques existent en dehors du temps politique lui-même. Des questions sur l'achat de faux *likes* ou de faux *followers* étaient par exemple déjà apparues à l'occasion de l'impressionnante mobilisation de 1,6 millions de personnes en soutien à un bijoutier niçois victime d'une attaque à main armée en 2014[3], voire à l'occasion de la progression spectaculaire des comptes de plusieurs personnalités politiques[4].

Dans le champ de la politique, le principal sujet semble être celui de l'appréhension par les partis et par les journalistes du nouveau territoire du numérique et des réseaux sociaux, ainsi que des outils qui permettent de s'y exprimer.

La question se pose alors de savoir si nos propres élections pourraient aujourd'hui être mises en danger de la même façon, si ces pratiques issues d'une nouvelle catégorie de dirigeants politiques avertis de l'industrialisation numérique des campagnes sont acceptables ou relèvent d'une forme de triche. Comment faudra-t-il réagir si un candidat se révèle disposer d'une audience artificielle grâce à l'usage de faux *followers* sur Twitter ? Ou si des *fake news* diffusées quelques jours avant une échéance importante accaparent et détournent le débat public, voire donnent le sentiment que l'issue du scrutin a été influencée ?

La campagne présidentielle actuelle a déjà été l'occasion de voir les messages de candidats relayés par des logiciels robots (*bots*) sur les réseaux sociaux, de façon plus ou moins subtile. Des alertes ont déjà eu lieu dès la primaire des Républicains quand Alain Juppé avait été attaqué de manière massive et coordonnée : présenté comme favorable aux islamistes après avoir autorisé l'ouverture d'une mosquée à Bordeaux, celui-ci était mis en scène dans des montages photos ou vidéos, affublé d'une barbe ou d'un *qamis* saoudien, soumis aux imams extrémistes ou à Tariq Ramadan. Le personnel politique considérait jusqu'à présent que ces pratiques relevaient du folklore politique et que leur impact sur la vie démocratique était extrêmement limité. Mais Alain Juppé a malheureusement découvert à ses dépens à cette occasion qu'il ne lui était pas possible de démentir ces fausses nouvelles et ces diffamations en utilisant les voies de communication dont il avait l'habitude.

Il ne suffit pas de faire une interview dans un quotidien ou d'aller à l'a télévision pour contester une information relayée par des individus des dizaines ou des centaines de milliers de fois par ses propres citoyens. Attaqué à son tour pour avoir inauguré une mosquée à Argenteuil en 2010, François Fillon l'a bien compris en préférant ne pas répondre à ces provocations dans les médias traditionnels - pariant sur l'extinction progressive de cette mauvaise dynamique.

S'il est abusif et sans doute manipulateur de parler de société « post-factuelle » (*post-truth*), force est de constater que les discours sur Internet et les réseaux sociaux peuvent être particulièrement violents, dirigés par des communautés d'intérêt, voire soutenues par des

[3] « L'arnaque aux faux soutiens du bijoutier », Sébastien Musset, Après l'abondance - http://sebmusset.blogspot.fr/2013/09/facebook-bijoutier-nice-intox.html

[4] « Les abonnés Twitter des politiques passés au crible », Paris Match, 31 décembre 2015 - http://www.parismatch.com/Actu/Politique/Les-abonnes-Twitter-des-politiques-passes-au-crible-679890

organes de propagande étrangers. Les candidats l'ont bien compris dont certains s'abstiennent aujourd'hui de toute référence à la réalité des faits. Le New York Times a eu l'occasion de traiter Donald Trump de menteur pathologique[5] mais le phénomène est en pleine expansion et touche désormais d'autres candidats, partout dans le monde. Dans la mesure où cela n'entraine aucune sanction, à quoi bon se priver ? Juridiquement, les risques portent essentiellement sur la diffamation et l'injure, mais pas sur le mensonge. Jusqu'à présent, on faisait confiance aux citoyens et aux médias pour limiter la diffusion des rumeurs ou des contre-vérités les plus évidentes. Ces précautions volent aujourd'hui en éclat, sans conséquences pour ceux qui s'en servent - avec un impact certain sur le scrutin[6].

Ce n'est pas un hasard. Tristan Harris dénonce désormais la façon dont les acteurs du numérique s'emploient à contrôler les choix de leurs usagers par le *design* de leurs interfaces, cherchant à générer de la dépendance, à leur faire accomplir des tâches à leur insu, à les empêcher de se déconnecter et à « casser » leur concentration et leur esprit critique en divisant l'information en blocs assez petits pour retenir leur attention de façon indépendante[7]. Initialement conçues pour maximiser la rentabilité des publicités sur le réseau, ces stratégies de contrôle de l'audience sont devenues une science en elle-même - avec par exemple le laboratoire universitaire des « technologies de la persuasion » de l'université de Stanford[8].

Transporté dans le champ du politique, ces techniques ont d'abord été qualifiées avec euphémisme de techniques du « Nudge » (*coup de coude*) selon le titre de l'ouvrage de Richard Thaler, Professeur d'économie comportementale au MIT, et Cass Sunstein, Professeur de droit à Harvard et ancien « tsar » de la régulation de l'administration Obama. En effet, pourquoi ne pas intervenir en amont des problèmes en « orientant » les choix des citoyens ? À quoi bon s'inquiéter des voitures mal garées si l'on a supprimé les places de parking ? Pourquoi s'inquiéter du vote des électeurs si ceux-ci ont été « correctement » informés ? Si cette approche a rapidement rencontré ses limites au sein d'une administration malgré tout soucieuse de l'intérêt général et de la liberté de conscience de ses citoyens, c'est finalement par le biais du détournement des outils modernes de communication que la même volonté de contrôle a fini par s'exprimer.

[5] « A Lie By Any Other Name », Charles M. Blow, New Yorker - https://www.nytimes.com/2017/01/26/opinion/a-lie-by-any-other-name.html?_r=0

[6] Ce qui tient pour beaucoup à l'efficacité du « digital labor », c'est-à-dire de l'exploitation dérégulée de leurs usagers par les réseaux afin de donner le plus d'écho possible aux messages qu'ils doivent véhiculer - et ce sans aucun regard pour l'intérêt personnel des usagers eux-mêmes au regard de ces messages.

[7] « How Technology Hijacks People's Minds—from a Magician and Google's Design Ethicist », Tristan Harris - https://medium.com/swlh/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3#.ud44t31pk

[8] Stanford Persuasive Tech Lab - http://captology.stanford.edu/

Ses dommages collatéraux apparaissent aujourd'hui considérables - à tel point que certains en viennent même à comparer l'industrie des médias à celle de la cigarette[9], et ce d'autant plus que les usages du numérique se diversifient, et qu'ils deviennent la colonne vertébrale de notre quotidien.

UN TRANSFERT DES PRATIQUES DE LA COMMUNICATION VERS LE POLITIQUE

L'année 2016 aura ainsi été témoin d'une hystérisation de la vie politique, en France comme à l'étranger. Face aux *fake news*, aux faux *followers*, aux erreurs de sondages, les gens n'ont plus d'intérêt à chercher à se convaincre les uns les autres. Selon le terme imaginé par Richard Spencer, l'extrême-droite est devenue la droite « alternative » aux Etats-Unis. Combinant « fascisme » et « *fashion* », le hashtag #fash suggère qu'il serait désormais « à la mode » de se revendiquer de ces mouvances. L'antisémitisme s'affirme en ajoutant trois « ‘’’ » autour du nom d'une personne afin de pointer sa judéité.

Les réseaux sociaux ne sont ni subtils, ni cachés. Mais ils donnent une caisse de résonance et des outils à une petite clique d'entrepreneurs de la haine et de la triche. Selon une étude de l'*Anti-Defamation League*[10], 68% des tweets antisémites visant les journalistes n'étaient envoyés que par 1 600 comptes Twitter. Mais ceux-ci ont appris à utiliser les outils offerts par le numérique et savent s'en servir pour faire levier et influencer le débat public et les élections.

Pour ce faire, ils utilisent les mêmes failles que tous les startupeurs qui veulent mettre un site en avant, faire du « *growth hacking* », donner une dynamique artificielle à une page sur un réseau social, etc. Les méthodes sont bien connues des publicitaires et des entrepreneurs. Elles passent par l'optimisation des moteurs de recherche (SEO), des algorithmes de réseaux sociaux (SMO), l'utilisation de faux comptes pour créer une audience artificielle (*Astroturfing*), la diffusion de fausses informations, l'exploitation de fausses identités, la mobilisation par des communautés militantes d'internautes qui contribuent massivement en ligne en parasitant les réseaux sociaux (*trolls*), l'automatisation et l'usage de *bots,* la publicité contextuelle (*retargeting*), etc.

L'ensemble de ces pratiques n'avait jusqu'alors été abordé que sous l'angle de la fraude au consommateur. Elles concernent désormais aussi le débat entre les candidats à l'élection présidentielle.

Mais qu'il s'agisse de publicité commerciale ou de propagande électorale, les outils sont les mêmes. Comme le rappelle le sociologue Antonio Casilli, cela fait des années qu'il est possible

[9] « Design de nos vulnérabilités : la Silicon Valley est-elle à la recherche d'une conscience ? », Hubert Guillaud - http://www.internetactu.net/2016/11/09/design-de-nos-vulnerabilites-la-silicon-valley-est-elle-a-la-recherche-dune-conscience/

[10] « Anti-Semitic Targeting of Journalists During the 2016 Presidential Campaign » - https://www.adl.org/sites/default/files/documents/assets/pdf/press-center/CR_4862_Journalism-Task-Force_v2.pdf

d'acheter des faux comptes ou des faux likes sans bouger de son bureau[11]. Si ces pratiques sont surtout utilisées dans un objectif commercial, ou pour des sites de piratage, leur réexportation en politique était parfaitement prévisible. Sur les sites de vidéos en ligne, 1000 « vues » ne coûtent que 3,96 dollars et 25 000 « vues », 89 dollars. Pourquoi s'en priver ?

LES POSSIBILITÉS LIMITEES DE L'AUTO-RÉGULATION

Face à ces questions inédites, le premier réflexe est souvent de s'en remettre à l'auto-régulation. Si les usagers sont capables de diffuser des fausses nouvelles, ils sont également capables de les signaler aux plateformes ou simplement de cesser de les diffuser.

Malheureusement, cette logique est limitée, et ce encore plus dans des secteurs comme l'information politique où les biais de confirmation, c'est-à-dire la tendance à ne tenir compte que des informations qui confortent nos convictions, ont tendance à jouer plus encore que d'habitude. Joshua Benton, le directeur du Nieman Lab, prend ainsi l'exemple d'une fausse information diffusée pendant la campagne électorale américaine prétendant que le Pape avait décidé de soutenir Donald Trump[12]. Si celle-ci a réussi à obtenir 868 000 partages sur Facebook, l'article corrigeant cette information et expliquant pourquoi elle était fausse n'a réussi à en obtenir que 33 000 - 26 fois moins. Le phénomène est difficile à contenir, un récent travail d'étude piloté par Sciences-Po et l'Ina[13] montre que la propagation des fausses nouvelles en ligne peut se faire en 4 secondes seulement (pour 10% d'entre elles), 230 secondes (pour 25%), 25 minutes (pour 50%) et seulement 175 minutes en moyenne - le tout alors que seuls 1/5e des documents publiés en ligne sont totalement originaux et que les autres consistent essentiellement en copiers/coller plus ou moins adaptés.

Plusieurs initiatives visent à détourner cette fluidité et cette vitesse de propagation en s'appuyant sur une logique de tri par les usagers - avec des réussites et des échecs. Les plus connues sont sans doute Crosscheck - un projet de journalisme collaboratif qui réunit des géants du web ainsi que des rédactions de toute la France et de l'étranger, et le Decodex - un outil créé par Les Décodeurs du journal *Le Monde* pour indexer le web et éviter l'utilisation de faux sites construits pour ressembler à de grands médias.

Preuve de leur bonne volonté, certaines plateformes ont mis en place des projets spécifiques aux élections. Google a par exemple décidé d'interdire l'achat de mots-clés correspondants aux noms des candidats et fournit des outils gratuits à travers le programme « Protection Elections » pour permettre aux équipes de campagne de se protéger contre les attaques[14].

---

[11] « Qui a fait élire Trump ? Pas les algorithmes, mais des millions de tâcherons du clic sous-payés » - http://www.casilli.fr/2016/11/17/qui-a-fait-elire-trump-pas-les-algorithmes-mais-des-millions-de-tacherons-du-clic-sous-payes/

[12] « The forces that drove this election's media failure are likely to get worse », Joshua Benton, Nieman Lab - http://www.niemanlab.org/2016/11/the-forces-that-drove-this-elections-media-failure-are-likely-to-get-worse/

[13] « L'information à tout prix », Julia Cagé, Nicolas Hervé, Marie-Luce Viaud - Ina Éditions

[14] https://protectyourelection.withgoogle.com/intl/fr

Si ces initiatives sont louables et destinées à se développer, il n'est pas certain qu'elles soient suffisantes, notamment au regard de l'importance de l'enjeu pour la vie démocratique - ce n'est d'ailleurs pas leur prétention.

LE SCRUTIN, UN ÉLÉMENT ESSENTIEL DE LA DÉMOCRATIE

Avant toute chose, il convient de se souvenir que les élections obéissent à l'article 3 de la Constitution et que le suffrage doit toujours être « universel, égal et secret » ce qui se traduit dans la jurisprudence du Conseil constitutionnel par le respect des cinq principes que sont « le pluralisme, l'égalité, l'impartialité, la loyauté et la dignité » - l'égalité et l'impartialité concernant essentiellement la participation aux élections des personnes exerçant déjà un mandat ou une fonction publique.

Signe de l'importance accordé en France au respect du droit de vote, fondement de notre démocratie, ce contentieux repose sur un même corpus de règles, rassemblées en grande partie au sein du Code électoral[15] et qui intéresse l'ensemble des juridictions françaises.

Comme le rappelle le Conseil d'État[16], cette unicité de règles tient, tout d'abord, à ce que les différentes élections soulèvent des questions communes, notamment en matière d'inscriptions sur les listes électorales, de déroulement de la campagne ou de modalités du vote. Elle tient, ensuite, à ce que les juridictions administratives et le Conseil constitutionnel, entre lesquels est réparti le contentieux des élections politiques, partagent la conception selon laquelle le juge électoral n'est pas seulement un gardien des formalités, mais aussi et surtout le garant de la sincérité du vote. Quant aux juridictions judiciaires, elles jouent aussi un rôle en matière électorale : les litiges relatifs aux inscriptions et radiations de personnes déterminées sur les listes électorales relèvent du juge civil ; la fraude électorale au sens de l'article L. 97 du code électoral constitue un délit réprimé par le juge pénal.

GARANTIR L'ACCÈS À UNE DIVERSITÉ D'INFORMATION

Le pluralisme des courants d'expression socioculturels est l'un des piliers de la démocratie.

Il est notamment mis en question par l'apparition des bulles de filtre ou tunnels informationnels, c'est-à-dire les situations où des citoyens sont « encouragés » par des algorithmes à ne plus être confrontés qu'à des informations partisanes. Victimes de leur propre « digital labor », ils participent activement à la construction de leur bulle informationnelle par le choix de leurs interlocuteurs, de leurs abonnements, de leurs likes et par l'ensemble de leurs activités en ligne.

[15] Historiquement, il y manque les élections présidentielles (loi de 62), européennes (loi de 77) et les référendums. Le contentieux du financement de la vie politique et de la transparence y échappe aussi, ainsi que les règles concernant les sondages.

[16] « Le juge administratif et le droit électoral » - http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Dossiers-thematiques/Le-juge-administratif-et-le-droit-electoral

Dans la mesure où l'algorithme de recherche qui conduit préférentiellement les usagers vers ce qu'il présume être l'objet de leurs recherche fait gagner beaucoup de temps et d'efforts, cette contrainte est vécue comme un service auquel ils n'ont pas envie de renoncer. Mais ces algorithmes fonctionnent surtout via des logiques d'auto-renforcement. Ils créent un cercle vicieux où les citoyens sont majoritairement exposés aux informations partisanes qui correspondent le plus à leurs opinions, auxquelles ils réagissent positivement, et qu'ils contribuent ainsi à renforcer.

En théorie, chaque candidat ou formation politique doit pouvoir intervenir de manière au plus égale et au moins équitable au cours de la campagne. Mais ce pluralisme n'est garanti qu'à deux conditions.

La première consiste à garantir la plus grande diversité d'opinions disponibles et accessibles. Elle est parfaitement réalisée dans le numérique, et se retrouve même renforcée par lui.

La seconde vise à permettre à chacun d'entre nous d'avoir une chance de rencontrer cette diversité, ou même simplement de l'apercevoir. Bien sur, mis en balance avec le principe de la liberté d'expression, le principe du pluralisme n'a jamais été absolu. Son volet audiovisuel qui est le plus fort s'applique à des degrés différents en fonction des élections - égalité stricte pour l'élection présidentielle sous le contrôle du CSA, égalité relative pour les élections législatives. Il est encore plus subtil en ce qui concerne la presse puisque les unes et le contenu des journaux ne sont soumis à aucune obligation. Seule contrainte indirecte, la loi Bichet fait obligation aux marchands de journaux de présenter toute la presse, permettant ainsi notamment aux passants d'apercevoir la Une de *l'Humanité* quand ils achètent *Le Figaro*.

Or, c'est sur cette confrontation à la diversité que le numérique se révèle aujourd'hui défaillant, voire toxique. Dans son ouvrage de 2001, *Republic.com* Cass Sunstein estimait déjà que les citoyens en ligne avaient tendance à « se restreindre à leur propre point de vue - les libéraux regardent et lisent surtout des libéraux ; les modérés, des modérés ; les conservateurs, des conservateurs ; les neo-Nazis, des neo-Nazis ». Le phénomène des tunnels informationnels s'exprime tout particulièrement sur les réseaux sociaux, mais il est tout aussi puissant en ce qui concerne les sites de vidéos en ligne ou les forums. Reste à savoir s'il faut considérer que la communication en ligne relève plutôt de la liberté de la presse écrite, ou de la liberté réglementée des médias audiovisuels. Mais ce débat est encore compliqué par le caractère intersubjectif des échanges qui ont lieu entre les usagers puisque ce sont eux qui se font les instruments de la diffusion des informations contestées en se les transmettant via leurs likes, leurs partages, leurs retweets ou leurs articles de blogs.

GARANTIR LA TRANSPARENCE DES ALGORITHMES

Pour répondre à ces questions, peut-être ne faut-il pas considérer les médias numériques comme un ensemble indifférencié. Il semble évident qu'il y a une différence entre une page d'accueil régie par un algorithme - dont le comportement a été défini par le choix de ses

programmeurs - , et des informations relayées par email ou par messages privés, lesquels ne relèvent que du libre choix des citoyens qui décident de les relayer.

À cet égard, dans la lignée de l'émergence du principe de loyauté des plateformes, la tendance juridique exprimée par les nouveaux textes est ouvertement à réclamer plus de transparence aux plateformes sur les données qu'elles exploitent et sur les algorithmes qu'elles leurs soumettent. Applicable à compter de mai 2018, le règlement européen 2016/679 sur les données personnelles prévoit par exemple dans certains cas la diffusion par la plateforme « des informations utiles concernant la logique sous-jacente » qui permet de profiler ses usagers[17]. D'autres initiatives commencent à vouloir imposer des règles à ces algorithmes, à l'exemple de la Commission Européenne qui réfléchit déjà à imposer des quotas d'oeuvres culturelles européennes aux moteurs de recommandation des plateformes de vidéos en SVOD. Quant à la Commission nationale informatique et liberté (CNIL), elle vient de lancer un grand débat national sur la régulation des algorithmes - visant expressément les questions d'ouverture culturelle et pluralisme démocratique[18]. De son côté, le Conseil national du numérique a été saisi d'une réflexion sur un outil grand public capable de collecter et répertorier les mauvaises expériences rencontrées par des utilisateurs avec des algorithmes, tandis que l'Institut national de recherche en informatique et en automatique (INRIA) doit coordonner le lancement d'une plateforme scientifique explorant l'enjeu éthique des algorithmes. Le Conseil Général de l'Economie de l'Industrie, de l'Énergie et des Technologies (CGEIET) recommande carrément d'étudier la méthode de fabrication des algorithmes des plateformes par rétro-ingéniérie (*reverse engineering*), et d'en confier le contrôle à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)[19].

Toute cette réflexion en matière de respect des règles de la concurrence et de protection du consommateur aura nécessairement un impact en matière électorale. Les deux problèmes principaux étant de disposer des compétences pour l'analyser correctement, et d'éviter le passage de la sous-régulation à la sur-régulation. Si l'Italie et l'Allemagne ont essayé de combattre l'émergence des fausses informations par une législation les interdisant, le texte permettant d'y arriver se révèle presque impossible à mettre en oeuvre sans porter atteinte de façon bien trop importante à la liberté d'expression et au droit à l'innovation[20].

Il n'empêche que le déroulement des élections les plus récentes appellent des réponses. L'auto-régulation collaborative permet de résoudre un certain nombre de problèmes, mais rien n'interdit

[17] « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) » - http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

[18] « Ethique et numérique : les algorithmes en débat » - https://www.cnil.fr/fr/ethique-et-numerique-les-algorithmes-en-debat-0

[19] « Modalités de régulation des algorithmes de traitement des contenus » - http://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2016_05_13_Rapport_Algorithmes(1).pdf

[20] « Spread of Fake News Provokes Anxiety in Italy » - https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html?_r=0

finalement d'imposer aussi un certain nombre de règles aux algorithmes qui recommandent des contenus aux usagers des plateformes - c'est d'ailleurs ce que fait déjà le Règlement Européen qui donne des instructions aux concepteurs d'algorithmes en leur demandant de prévenir « entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur la l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle ».

MODERNISER LES RÈGLES RELATIVES À LA PROPAGANDE ÉLECTORALE POUR GARANTIR L'ÉGALITÉ DES RÈGLES ET LA DIGNITÉ DU SCRUTIN

Les questions relatives à la loyauté et à la dignité du scrutin sont plus subjectives. Elles rappellent tout d'abord que l'élection n'est pas un combat mais une compétition, et que les candidats doivent se comporter de manière loyale les uns envers les autres. C'est l'une des règles essentielles qui régit les questions de propagande électorale - faux tracts, affirmations calomnieuses, etc.

En matière de loyauté, il faudrait éviter que les comportements qui sont interdits dans le monde physique se reportent dans le monde numérique. S'il est par exemple impossible pour un candidat ou ses militants d'aller influencer les électeurs le jour du scrutin, faut-il accepter les envois de SMS ou les messages de ralliements sur les réseaux sociaux ? De même, s'il est interdit d'acheter de l'affichage dans la rue, comment réagir face à la publicité qui a été achetée *à l'avance* via l'acquisition de faux followers ou à l'augmentation artificielle du trafic ? Et surtout, comment se comporter alors même que ces fraudes se font au sus et au vu de tout le monde - n'importe qui pouvant par exemple constater par soi-même sur ses propres comptes que des milliers de militants copient-collent les mêmes messages - avec parfois les mêmes fautes d'orthographe, au même moment, de façon automatisée.

S'il fallait considérer que ces pratiques sont génératrices d'un trouble au scrutin, des procédures d'urgence existent déjà devant le juge civil des référés, mais c'est le juge de l'élection qui décide in fine des éventuelles conséquences des messages ainsi diffusés.

Quant à la dignité du scrutin, il s'agit d'un principe nouveau établi par le Conseil constitutionnel à l'occasion de la proclamation de l'élection présidentielle de 2002 - certaines personnalités avaient appelé les électeurs à exprimer leur mécontentement devant le choix qui leur était proposé.

Sur l'ensemble de ces points, il ne fait pas de doute que le numérique est d'ores et déjà saisi par le droit électoral puisque l'article L. 48-1 du code électoral précise que « les interdictions et restrictions prévues par le présent code en matière de propagande électorale sont applicables à tout message ayant le caractère de propagande électorale diffusé par tout moyen de communication au public par voie électronique ».

Des questions se sont par exemple déjà posées en ce qui concerne l'achat ou non de publicité par les candidats - laquelle est logiquement interdite pendant la période prévue par l'article L. 52-

1 du Code, mais aussi en ce qui concerne le maintien d'un site internet pendant cette période - lequel a logiquement été autorisé car ne présentant pas le caractère d'une publicité. Dès 2002, le Conseil constitutionnel avait été obligé de contredire une décision de rejet du compte de campagne par la CNCCFP parce que les candidats avaient utilisé un site web gratuit qui risquait d'être qualifié d'avantage en nature venant d'une personne morale[21]. Seule est aujourd'hui interdite l'actualisation du site du candidat la veille et le jour du scrutin. De même, les candidats sont aujourd'hui incités à « bloquer » les discussions entre internautes se déroulant sur leur site Internet la veille du scrutin à zéro heure, et ils doivent eux-mêmes cesser de s'exprimer sur leurs comptes *via* les réseaux sociaux.

Reste qu'il n'est pas certain aujourd'hui que le dispositif de sanction du droit électoral soit adapté et efficace. Mis en place sous la IIIe République dans le contentieux des élections locales, combinant sanction légale de l'élection et sanctions pénales, il montre ses limites face à la souplesse des pratiques en ligne.

En effet, pour limiter l'impact du pouvoir judiciaire sur le droit électoral, celui-ci est relativiste, il ne permet de prononcer des sanctions que dans l'hypothèse où la triche a eu des conséquences graves sur le scrutin. Le premier critère de sanction concerne l'ampleur et le nombre des irrégularités constatées. Il n'y aura pas d'annulation de l'élection s'il s'agit d'un fait isolé ou qui ne concerne qu'un nombre limité de personnes. Le deuxième critère vise à punir le dépassement des limites « admissibles » de la polémique électorale - alors même que celles-ci sont étendues afin de permettre le débat durant cette période. Le troisième critère tient au moment de survenance de l'irrégularité et part du principe que la proximité avec le scrutin renforce l'impact sur celui-ci - ce qui est particulièrement faux dans l'univers numérique où beaucoup de choses s'organisent longtemps en amont.

Que faut-il penser par exemple de la récente pratique dite de #radiolondres par laquelle des membres des équipes de campagne, des journalistes et des passionnés de politique diffusent sur Twitter ou par SMS des résultats de sondages sortis des urnes largement avant l'horaire autorisé ?

Que faut-il penser par exemple d'un candidat qui améliorerait son audience en ligne par l'utilisation de faux *followers* payants au cours des deux ou trois années précédant le scrutin ? Ceux-ci ayant déjà été payés, faudrait-il considérer que leur usage pendant la campagne devrait encore être interdit ?

Ces pratiques sont interdites dans le monde physique. On ne peut pas déclamer les résultats avant l'horaire prévu à cet effet. On ne peut pas non plus acheter à l'avance une publication ou un affichage qui serait effectué pendant la campagne. Enfin, il ne fait aucun doute non plus qu'un contentieux est appelé à se créer en ce qui concerne les simples mensonges proférés par un candidat quand ils auraient eu un impact sur le scrutin sans pour autant constituer une injure ou une diffamation.

[21] https://legimobile.fr/fr/jp/c/ce/an/2003/2002-2937_2958/#

Mais malgré la force des principes en cause, leur violation n'entraîne que très rarement l'annulation de l'élection. De façon un peu cynique, le Conseil constitutionnel est aujourd'hui peut-être plus garant de la sincérité du scrutin que de sa moralité - dans la mesure où il se contente de sanctionner les actes blâmables par des réprimandes symbolique sans pour autant annuler les élections concernées. C'est donc logiquement qu'on a laissé la liberté primer dans le monde numérique pour autant qu'on supposait que ces pratiques n'avaient qu'un impact très faible ou inexistant. Il ne faudrait pas en conclure trop rapidement que le numérique est une zone de non-droit. Seule se pose la question de son impact réel sur les élections.

UN IMPACT NUMÉRIQUE PARTICULIÈREMENT SENSIBLE EN FRANCE

Si ces débats ont déjà eu lieu à l'étranger, ils prennent une importance toute particulière en France en raison du mode de scrutin majoritaire uninominal à deux tours de l'élection présidentielle, et du pouvoir important qui est accordé au Président de la République. Selon une récente étude de Stanford, les fausses informations diffusées sur les réseaux sociaux auraient dû influencer le vote de 0,7% des électeurs pour être considérées comme ayant eu un impact sur l'élection de Donald Trump. Compte tenu du régime électoral américain, ce chiffre est souvent présenté comme exonérant les plateformes numériques de leur responsabilité. Il prend une toute autre importance en France où une différence même plus infime 0,5%, 0,2% ou 0,1% au premier ou au second tour de scrutin serait parfaitement susceptible de transformer radicalement le résultat du vote. Il pose également question en ce qui concerne les élections législatives où l'investissement est peut-être moindre d'un point de vue financier, mais où le plus grand nombre de scrutins multiplie le problème autant de fois qu'il y a de candidats.

Ces questions de triche numérique prennent également une importance toute particulière dans le cadre de la perte de confiance des citoyens envers les politiques. Au-delà de la fraude relative à la propagande électorale, il semble évident que le climat de la campagne est profondément transformé sans qu'on puisse facilement en évaluer le résultat en termes de démobilisation, d'abstention, ou de radicalisation. Le sentiment assez général que les débats de fond ne sont pas vraiment abordés au cours d'une campagne pourtant toujours considérée comme le moment décisif de notre vie politique vient en partie du "bruit" entretenu par les réseaux sociaux et la dispersion des enjeux de la campagne.

Ces pratiques ne sont pas forcément nouvelles. Il est bien sûr déjà arrivé que les médias traditionnels diffusent des informations erronées, ou qu'il y ait des controverses en ce qui concerne les chiffres de l'économie, les résultats des sondages ou le niveau de participation aux meetings et aux manifestations. Mais le passage au numérique ne consiste pas seulement en la transposition de ces problèmes traditionnels dans un nouvel environnement. Il s'agit d'une métamorphose et d'un changement de nature. Face à des Français qui passent en moyenne 1h20 par jour sur un assistant personnel qu'ils ont presque tous au fond de leur poche et auquel ils confient leur vie la plus personnelle, les défenses cognitives et la pensée critique ne sont pas sollicités de la même façon. En outre, ce n'est pas la même chose de recevoir une fausse

information par le biais d'un journal ou dans le contexte d'une émission, et de la voir relayée par ses amis ou par ses connaissances - surtout dans la mesure où le modèle économique et la technique des plateformes sont conçus pour maximiser et tirer profit de ces échanges. La métamorphose de l'information provoque une amplification de certains travers, mais aussi une amplification des biais cognitifs - le biais de confirmation, le biais d'échantillon, etc. Les opinions militantes se trouvent sur-représentées car il y a une prime à ceux qui promeuvent une opinion plutôt qu'à ceux qui la contestent.

Sur tous ces points, les règles relatives à la propagande électorale ne semblent pas adaptées. Et elles le seront de moins en moins. Aujourd'hui, Facebook est le premier média d'information des jeunes, mais sa cible démographique s'étend chaque année un peu plus. Son influence politique ne semble pas non plus avoir atteint son apogée. Si la révolution tunisienne avait bénéficié d'un porte-voix grâce à Facebook, le réseau social est demeuré au coeur de la vie politique du pays dont il constitue la principale source d'information - éteignant l'impact des médias traditionnels comme la radio.

UN BESOIN DE FORMATION ET D'ACCOMPAGNEMENT

Au-delà des révélations sur les élections sud-américaines, la question du piratage a été au coeur de la précédente campagne américaine - pourtant la mieux financée et la plus surveillée du monde. C'est par le biais de courriels piégés que les démocrates ont dévoilé leurs mots de passe à deux groupes de *hackers* dénommés Fancy Bear et Cozy Bear. D'autres actions ont été repérées lors des votes en ligne à Honk Kong en 2014, ou contre le site de la Commission Centrale des Elections en Ukraine l'année dernière. La France n'est pas à l'abri et la trace de ces groupes a déjà été repérée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Reste que beaucoup de campagnes utilisent au quotidien des outils de messageries supposément « cryptées » mais en réalité pleines de failles connues et exploitées.

Ces problèmes ne sont pas aujourd'hui intégrés par les candidats, notamment aux législatives. Il devient nécessaire de prendre en compte la question de leur formation et d'assurer une meilleure fluidité entre les pratiques et les règles des deux mondes. L'émergence du sujet comme une préoccupation des équipes de campagne est extrêmement récente.

Du côté de l'administration aussi, la prise en compte est récente mais réelle. L'ANSSI a par exemple pu réunir les partis politiques français, les alerter, et déboucher sur une réflexion au niveau du Conseil de Défense. Autre exemple, la CNIL - dont le rôle n'est pas de protéger l'équité - a organisé un Observatoire des Élections depuis les premières primaires en 2011[22]. Aujourd'hui pérenne, il poursuit plusieurs objectifs : permettre aux candidats de poser des questions à la CNIL, créer une compétence transversale au sein de l'autorité - permettant par exemple d'avoir un regard terrain par les plaintes ou les témoignages, réflexion sur l'évolution des pratiques, de la doctrine de la CNIL, voire de la législation.

[22] https://www.cnil.fr/fr/elections

Le Chef de l'Etat lui-même s'inquiète des menaces numériques sur l'élection, au point de consacrer un Conseil restreint de défense à ce sujet et de permettre à l'ANSSI d'être saisie par la Commission Nationale de Contrôle de l'Election Présidentielle ainsi que par le Conseil Constitutionnel. Reste que les candidats semblent peu équipés pour faire face à ces questions. La législation électorale est déjà difficile à prendre en main. Les nouveaux outils de l'industrialisation numérique de la politique sont riches de promesses mais rajoutent encore une couche de complexité et forcent les candidats à se former ou à faire appel à des fournisseurs de solutions de sécurité dans le secteur privé. Il n'est certes pas du ressort de l'ANSSI de protéger leurs systèmes d'informations, leurs messageries ou leurs sites internet. Mais il serait sans doute utile que cette administration soit dotée d'une compétence de conseil dans ce domaine afin de disposer d'un référentiel sécurité qui serait un peu l'équivalent du guide préparé par la CNIL en ce qui concerne les données.

Mais au-delà des problèmes de triche eux-mêmes se pose également la question nouvelle des éditeurs d'outils de gestion de la relation client à finalité politique - c'est-à-dire les logiciels permettant aux candidats de gérer leurs militants, de leur envoyer des informations, de les mobiliser pour du porte à porte, etc. En France par exemple, le logiciel "Cinquante plus un" permet de gérer le porte-à-porte, mais également de prévoir quelles circonscriptions seront les plus efficacement travaillées. Sur ce point, il ne faut ni sur-estimer, ni sous-estimer le pouvoir de ces outils qui tendent surtout à ramener le candidat au réel en accélérant le regroupement de ses contacts. Reste que ces outils, dont le plus connu est le logiciel "Nation Builder" ont été conçus dans un cadre américain où les dépenses de campagne ne sont pas plafonnées. Leur coût est élevé. Leur modèle économique n'est pas celui de la limitation et du contrôle des dépenses de campagne. Ils créent une dépense supplémentaire qui n'est pas forcément accessible à tous les candidats - que ce soit en termes de moyens, ou en termes d'expertise.

UNE PRISE EN COMPTE DIFFICILE PAR LE BIAIS DES COMPTES DE CAMPAGNE

Se pose dès lors - et ce de façon plus urgente encore, la question des comptes de campagne vis-à-vis du numérique. Faut-il intégrer les faux comptes ou les faux *likes* dans les comptes de campagne ? Qu'en est-t-il si l'on ne peut pas démontrer qu'ils ont été payés par le candidat ? Le Conseil d'Etat a récemment eu l'occasion de traiter une question similaire à l'occasion de l'arrêt dit « Huchon » dans une situation où Jean-Paul Huchon avait fait afficher sans le savoir des panneaux publicitaires du Conseil Régional pour un montant de 1,5 millions d'euros en pleine période réservée. Le Conseil d'Etat avait alors rejeté ses comptes de campagne - l'empêchant ainsi d'être remboursé - tout en maintenant son élection[23].

Si l'on dresse le parallèle avec les pratiques en ligne, la question sera par exemple de savoir s'il faut réintégrer, ou non, dans les comptes de campagne l'acquisition de faux *followers* ou de faux

[23] http://www.conseil-etat.fr/Actualites/Communiques/Elections-regionales-d-Ile-de-France4

likes par un candidat. À suivre cette jurisprudence, pour immorale qu'elle soit, la pratique ne serait donc sanctionnée qu'à condition qu'elle ait finalement altéré la sincérité du scrutin. Ce qui ne serait pas évident à démontrer.

L'impact du numérique sur les élections est réel et arrive désormais à maturité. La multiplication des outils numériques entraîne des possibilités de fraude à tous les niveaux. Pour la majorité des comportements illicites, le droit électoral semble d'ores et déjà capable de les appréhender à condition d'en adapter l'interprétation. Pour le reste, il s'agit à la fois de s'adapter à l'industrialisation numérique croissante des campagnes électorales qu'à de nouveaux usages. Les critères traditionnels de sanction de la triche électorale sont adaptés à un environnement connu et maîtrisé depuis des décennies. Grâce à la bonne éducation du public, à la vigilance des médias et à la sévérité des peines, cela fait longtemps que personne ne bourre plus massivement les urnes en France. Mais la triche numérique est porteuse de nouveaux dangers. Attendre qu'elle ait un impact sur le scrutin pour commencer à la prendre en compte reviendrait à nier les problèmes qui ont pu être observés à l'étranger au cours de ces dernières années. Il faut au minimum que l'Etat garantisse la bonne tenue du scrutin en développant un rôle de conseil auprès des candidats - comme il le fait déjà en ce qui concerne certains autres aspects de l'élection. Mais il faut également adapter certaines sanctions, comme par exemple celles qui concernent la diffusion de fausses nouvelles. Il faut réunir les acteurs du secteur pour les accompagner dans leur volonté positive d'autorégulation, tout en étant capable de leur demander aussi un effort réglementaire supplémentaire quand c'est nécessaire, par exemple en matière de réactivité aux signalements ou de transparence de leurs algorithmes. Enfin, il faut sans doute prévoir des évolutions du droit électoral. La triche étant plus simple et moins coûteuse, la contrainte pénale qui est la seule à véritablement cibler les individus devrait être renforcée. Le critère de l'impact sur le résultat du scrutin devrait être adapté au numérique en prenant en compte les impacts directs, mais aussi indirects. La bataille du symbolique ne doit pas être gagnée par ceux qui croient que le numérique devrait échapper à toutes les règles. Face à la puissance de l'industrialisation numérique de la politique, il est nécessaire de rappeler la transcendance et la primauté des règles de la démocratie.