Strasbourg, le 26 octobre 2020

T-PD(2020)02Rev

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

CONVENTION 108

Traitement des données à caractère personnel par et pour les organisations chargées des campagnes politiques : application de la Convention modernisée 108 du Conseil de l'Europe

préparé par

le professeur Colin J. Bennett

Direction générale Droits de l'homme et État de droit

Table des matières

Introduction *2*

Les tendances en matière de campagnes politiques numériques *5*

L'utilisation des données à des fins électorales : mythes et réalités *9*

Les campagnes politiques, les partis politiques et la Convention 108+ *11*

1) L'identification et la réidentification des données sur les opinions politiques 12

2) La définition des « opinions politiques » en tant que forme de données sensibles 13

3) Les règles encadrant les communications politiques consenties 17

4) Les questions de proportionnalité à la lumière des objectifs légitimes 19

5) Le traitement des données à caractère personnel rendues « publiques » 20

6) La transparence 22

7) Les règles encadrant la prise de décisions automatisée et le profilage des électeurs 23

Conclusions *24*

Résumé

Dans de nombreux pays, les campagnes électorales sont désormais guidées par des analyses de données complexes et par une série de nouvelles technologies mises en œuvre par l'industrie de l'"influence politique". Au centre des efforts visant à contrôler ces pratiques et à lutter contre la manipulation et la propagande électorales se trouve la question de savoir comment les données personnelles des électeurs sont traitées dans le cadre des campagnes politiques, et si cela se fait légalement et éthiquement. Des questions familières sur la vie privée sont aujourd'hui au centre d'un débat international animé sur l'intégrité démocratique et sur les droits à des élections libres et à l'autonomie des électeurs consacrés par la Convention européenne des droits de l'homme.

La Convention 108 modernisée du Conseil de l'Europe a un rôle unique à jouer pour limiter la surveillance des électeurs en mettant en avant des pratiques de campagne éthiques. Elle est explicitement conçue comme un instrument universel qui peut être appliqué dans différentes parties du monde, ainsi que dans les sociétés démocratiques établies comme émergentes. Elle est explicitement enracinée dans les droits de l'homme et les principes démocratiques plutôt que commerciaux. C'est un instrument technologiquement neutre qui peut relever les nouveaux défis posés par les nouvelles technologies d'analyse des campagnes et des électeurs. Il offre une norme de base pour la promotion des meilleures pratiques à destination des divers responsables de traitement de données et sous-traitant au sein des réseaux mondiaux de l'industrie de la campagne. Enfin, il contient également des normes fondées sur des principes pour la coordination des règles relatives à la protection de la vie privée dans les domaines de la protection des données et du droit électoral.

Les orientations du Conseil de l'Europe concernant le traitement des données à caractère personnel par et pour les campagnes politiques devraient aborder certaines questions clés en référence aux récentes décisions des autorités de protection des données, notamment l'étendue de la signification des "opinions politiques" en tant que forme de données sensibles, le caractère identifiable et ré-identifiable des données à caractère personnel relatives aux opinions politiques, les règles en matière de consentement et de communication politique, les questions de proportionnalité à la lumière des objectifs légitimes des campagnes politiques, le traitement des données qui ont été rendues "publiques" par le biais des plateformes de médias sociaux, les responsabilités en matière de transparence sur les réseaux de campagne, et les règles appropriées pour la prise de décision automatisée et le profilage des électeurs.

Le Conseil de l'Europe occupe une place unique pour traiter les implications en matière de protection de la vie privée des élections basées sur des données. Un document d'orientation sur la Convention 108+ et les campagnes politiques pourrait être avoir une réelle influence. Il pourrait aider les pays à trouver un équilibre entre la protection de la vie privée et les obligations plus larges des organisations politiques de faire participer l'électorat. Il pourrait également être adapté à différents environnements juridiques, traditions constitutionnelles et administratives, systèmes de partis et systèmes électoraux et cultures politiques.

Introduction[1]

Il existe une riche tradition qui consiste à essayer de comprendre la valeur sociale de la protection de la vie privée dans les sociétés démocratiques[2]. En effet, la protection de la vie privée encourage la mobilisation et la participation des citoyens qui peut ainsi voter librement, s'exprimer, s'affilier à des groupes d'intérêt, signer des pétitions, participer à la société civile, militer et protester. Elle favorise l'autonomie individuelle et renforce ainsi notre liberté de faire des choix en toute connaissance de cause et dans le respect équitable des préférences, des valeurs et des intérêts d'autrui[3].

Cependant, jusqu'à encore récemment, les nombreux ouvrages sur la vie privée, la protection des données et la surveillance des personnes publiés encore récemment ne comprenaient quasiment aucune analyse ou examen de la manière dont les données personnelles sont saisies, utilisées et traitées *dans le cadre* du processus démocratique. Ces publications ne s'intéressent pratiquement pas au suivi de l'électorat par les acteurs politiques, notamment les partis politiques, leurs candidats et le réseau de consultants et d'entreprises qui travaillent pour eux. Or nous savons que le respect de la vie privée est important *pour* la démocratie. Jusqu'à très récemment, nous savions très peu de choses sur la façon dont la vie privée est menacée *par* la démocratie, par les agents qui cherchent à nous mobiliser, à nous inciter et à nous encourager à voter ou à ne pas voter[4].

À l'évidence, cette situation a évolué de façon aussi rapide qu'alarmante. La médiatisation concernant les activités de Cambridge Analytica (CA), de la société canadienne (Aggregate IQ) et la collecte de données de Facebook au moyen d'applications tierces a pris des proportions extraordinaires. Ces scandales ont fait l'objet d'enquêtes dans plusieurs juridictions et nous en savons plus désormais sur l'étendue de « l'industrie de l'influence politique »[5] et sur les risques que représentent pour la démocratie le profilage de masse de l'électorat et la diffusion de messages microciblés à des catégories de plus en plus étroites d'électeurs[6] : les « bulles de filtre » et une volonté accrue de diffuser des messages sur des questions clivantes, la discrimination et la privation du droit de vote, un effet dissuasif sur la participation politique, un renforcement du sectarisme et de la polarisation ainsi que l'ambiguïté des mandats politiques des

[1] Je suis très reconnaissant à Sophie Kwasny et Bohumila Ottova, du Conseil de l'Europe, pour leur aide dans la préparation de ce rapport. Graham Greenleaf, Charles Raab et Lee Bygrave ont fait des observations très utiles sur les premiers projets. Je remercie aussi les membres des délégations qui ont posé des questions et formulés des observations sur les versions précédentes présentées lors des Vues sur la Protection des données du 3 juillet 2020 et lors de la réunion du Bureau du Comité de la Convention 108 (29 septembre 2020).

[2] A. Lever (2015). *Privacy and democracy: What the secret ballot reveals*. *Law, Culture and the Humanities*, *11*(2), 164-183.

[3] C. J. Bennett & S. Oduro Marfo (2019). *Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities* (Document publié lors de la Conference of International Privacy and Data Protection Commissioners de 2019), voir : https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf

[4] Ibid.

[5] Tactical Tech. (mars 2019). *Personal Data: Political Persuasion – Inside the Influence Industry. How it works.* Berlin: Tactical Tech. https://tacticaltech.org/#/projects/data-politics/

[6] C. J. Bennett and D. Lyon eds. (2019) Data-Driven Elections. *Internet Policy Review*, Vol. 8, No. 1, voir : https://policyreview.info/data-driven-elections

représentants élus[7]. L'opacité d'un grand nombre de messages politiques contemporains bloque les avantages présumés du processus d'autocorrection des droits à la liberté d'expression et érode le débat démocratique plus large sur le bien commun[8]. L'utilisation de données à des fins électorales et le microciblage ont clairement des effets « macro »[9].

La question de savoir comment les données à caractère personnel des électeurs sont traitées dans les campagnes politiques et si leur traitement est légal et éthique est au cœur des initiatives de lutte contre la manipulation et la propagande électorales. Et la question bien connue de la protection des données est désormais au centre d'un âpre débat international sur l'intégrité démocratique et sur le droit à des élections libres consacrés par la Convention européenne des droits de l'homme[10]. Les instruments internationaux relatifs à la protection des données, notamment la Convention 108 modernisée du Conseil de l'Europe[11], occupent une place de plus en plus importante dans la réglementation de l'utilisation des données à des fins électorales et dans le soutien des grands principes démocratiques du pluralisme et de l'autonomie individuelle

Les travaux du Conseil de l'Europe dans le domaine de la protection de la vie privée reposent sur l'article 8 de la Convention européenne des droits de l'homme. Depuis les années 1970, le Conseil s'emploie à promouvoir des normes de protection des données qui ont abouti à la Convention 108 originale adoptée en 1981[12]. S'appuyant sur cette longue tradition, la Convention 108 modernisée de 2018 (Convention 108 +) s'inscrit explicitement dans un large objectif, qui est « de garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne ». Elle évoque « l'autonomie personnelle, fondée sur le droit de toute personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait ». Elle rappelle que « le droit à la protection des données à caractère personnel est à considérer au regard de son rôle dans la société et qu'il est à concilier avec d'autres droits de l'homme et libertés fondamentales, dont la liberté d'expression[13]. »

Le traitement des données à caractère personnel dans les campagnes politiques nécessite précisément ce type de conciliation. Les partis politiques jouent un rôle unique et essentiel dans les sociétés démocratiques. Ils éduquent et mobilisent les électeurs. Ils sont les mécanismes essentiels qui relient le citoyen à son gouvernement. A cet égard, il serait peut-être bon que les partis et les candidats qui traitent des données à caractère personnel à des fins de « participation

---

[7] E. Pariser (2012). *The filter bubble: How the personalized web is changing what we read and think.* New York: Penguin Books; D.S. Hillygus, D.S. & T. Shields, (2008). *The persuadable voter: wedge issues in presidential campaigns*. Princeton, NJ : Princeton University Press ; S. Barocas (2012). The price of precision : Voter microtargeting and its potential harms to the democratic process. In *Proceedings of the first edition workshop on Politics, elections and data*, 31-36.

[8] S. Vaidhyanathan. (2018) *Anti-Social Media: How Facebook Disconnects us and Undermines Democracy*. Oxford: Oxford University Press. p. 164

[9] S. Hankey, S. J.K. Morrison & R. Naik. (2018). *Data and democracy in the digital age*. The Constitution Society. URL: https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie- Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital- Age.pdf

[10] Article 3 du Protocole n° 1 de la CEDH. « Chacun a le droit de participer aux élections du gouvernement de son pays dans un scrutin libre à bulletin secret. Sans ce droit il ne peut y avoir d'élections libres et équitables. Ce droit garantit la libre expression des citoyens, la juste représentativité des élus et la légitimation des instances législatives et exécutives, et, par là même, il contribue à la confiance populaire dans les institutions. »

[11] Conseil de l'Europe (2018). Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (2018). Voir : https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (ci-après Convention 108 +)

[12] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 1981, article 6, voir : https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680078b37

[13] Convention 108 +, Préambule.

démocratique » disposent d'une plus grande marge de manœuvre pour traiter ces données aux fins d'éduquer et de mobiliser les électeurs[14]. En revanche, un grand nombre des activités actuelles des partis politiques se distinguent à peine de celles des sociétés de marketing actuelles : ils font de la publicité en ligne et hors ligne, emploient des sociétés d'analyse de données, achètent des espaces sur les réseaux sociaux afin d'atteindre des publics ciblés et testent et retestent constamment leurs messages politiques. Désormais, ils sont sur « le marché des votes » et il est possible que les électeurs choisissent des partis de la même manière que les consommateurs achètent des produits[15].

Compte tenu de ces réalités, quel est le juste équilibre entre le droit au respect de la vie privée et les obligations qui incombent aux partis politiques et aux candidats d'éduquer et de mobiliser les électeurs ? En ce qui concerne les principes relatifs à la protection des données, qu'est-ce qui justifie de traiter les organisations politiques différemment des organismes publics ou des sociétés commerciales ? Comment la Convention 108 modernisée peut-elle contribuer à déterminer le juste équilibre ? Le présent document s'appuie sur les travaux antérieurs du Conseil de l'Europe consacrés aux technologies numériques et aux élections, notamment l'étude sur l'utilisation d'Internet dans les campagnes électorales[16] et, en particulier, les travaux de la Commission de Venise sur les technologies numériques et les élections[17].

La première partie souligne quelques-unes des tendances actuelles en matière de campagne politique dans les pays démocratiques modernes, selon des rapports élaborés par des autorités de protection des données et des études universitaires publiés récemment. La deuxième partie passe en revue certains mythes et réalités concernant l'utilisation de données pour les campagnes électorales et décrit brièvement le plus vaste ensemble de facteurs juridiques, institutionnels et culturels qui pourraient déterminer la surveillance de l'électorat dans une société donnée.

Le corps du document analyse les normes différentes mais néanmoins liées relatives à la protection des données qui s'appliquent directement au traitement des données à caractère personnel dans les campagnes électorales. Il est entendu que toutes les dispositions de la Convention 108+ peuvent s'appliquer au traitement des données personnelles par les organisations politiques. Le présent document met l'accent sur des questions portant sur la protection des données qui sont particulièrement épineuses et qui nécessitent une analyse singulière dans le contexte politique et sont plus générales dans tous les pays démocratiques. Il passe donc en revue les dispositions pertinentes de la Convention 108+ concernant les possibilités d'identification et de réidentification, la définition des « opinions politiques sensibles », les communications à contenu politique, les intérêts légitimes et la proportionnalité, le traitement de données publiques sur les réseaux sociaux, l'obligation de transparence et le traitement et le profilage automatisés. Il fait constamment référence aux dispositions parallèles du Règlement

[14] Bennett & Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, p. 4.
[15] S. Delacourt, (2015). *Shopping for Votes: How Politicians Choose Us and We Choose them*, 2nd ed. Madeira Park, BC: Douglas and McIntyre.
[16] Council of Europe, *Etude relative à l'utilisation d'internet dans le cadre des campagnes électorales*, DGI(2017)11 at: https://rm.coe.int/DGI(2017)11_Utilisation%20Internet%20dans%20campagnes%20e/09000016807c0e25
[17] Rapport conjoint de la Commission de Venise et de la Direction de la société de l'information et de la lutte contre la criminalité, Direction générale Droits de l'homme et État de droit (DGI) sur les technologies numériques et les élections, adopté par le Conseil des élections démocratiques lors de sa 65e réunion (Venise, 20 juin 2019) et par la Commission de Venise lors de sa 119e session plénière (Venise, 21-22 juin 2019). Voir : https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-f

général de l'UE sur la protection des données (RGPD)[18] et aux récentes enquêtes sur les pratiques utilisées dans les campagnes électorales menées par les autorités chargées de la protection des données au Royaume-Uni, en France et au Canada[19].

En conclusion, je soutiens que la Convention 108 + a un rôle unique à jouer dans la promulgation des bonnes pratiques de protection des données applicables aux campagnes politiques, et donc dans le renforcement des droits démocratiques. L'histoire du Conseil de l'Europe et son expérience en matière de promotion de ces droits fondamentaux en font le lieu idéal pour aborder des questions aussi cruciales, tant dans les sociétés industrialisées avancées que dans les pays aux démocraties émergentes plus fragiles.

Les tendances en matière de campagnes politiques numériques

Le scandale Facebook/Cambridge Analytica a été le reflet et l'aboutissement d'une série de tendances qui remontent à une vingtaine d'années[20]. Un rapport comparatif de 2019 du collectif Tactical Tech a tenté de cartographier ces tendances et de dresser un portrait de l'« industrie de l'influence politique » d'aujourd'hui dans le monde. Il établit une distinction utile entre les données en tant que *ressource politique*, en tant que *renseignement politique* et celles qui servent à exercer une *influence politique*.

Les données à caractère politique constituent une *ressource* dans la mesure où elles sont stockées dans des bases de données traditionnelles ou des systèmes de gestion des relations avec les électeurs dont les sources sont notamment les registres électoraux, les résultats de sondages, les informations provenant de courtiers en données commerciales, et les données recueillies par les partis eux-mêmes pendant leur campagne (par le porte à porte, au téléphone, en ligne). Les systèmes de gestion des relations avec les électeurs offrent aux partis des solutions intégrant tous les aspects de leurs campagnes : sensibilisation des électeurs, démarchage au porte-à-porte, télémarketing, affichage, gestion d'événements, présence sur les réseaux sociaux, suivi des problèmes et activités d'incitation au vote. Nous savons que ces systèmes existent non

[18] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif au règlement général sur la protection des données (JO L119 1). Voir : http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[19] UK Office of the Information Commissioner (July 2018). *Democracy Disrupted: Personal Information and Political Influence.* Voir : https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf (July 2018); UK, ICO, *Investigation into Data Analytics in Political Campaigns: Investigation Update.* https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf ; Office of the Privacy Commissioner of Canada (OPC) (2019) *Joint Investigation of Aggregate IQ Data Services Ltd. By the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia.* Report of Findings #2019-004 November 26, 2019. Voir : https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-004/; Office of the Information and Privacy Commissioner of BC (February 2019). *Full Disclosure: Political Parties, Campaign Data and Voter Consent.* Voir : https://www.oipc.bc.ca/investigation-reports/2278; France, Commission nationale de l'informatique et des libertés (CNIL) (8 novembre 2016). *Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ?* Voir : https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

[20] C. J. Bennett, (2015). "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications", *Surveillance and Society*, vol. 13, no 3-4 http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/vote_surv

seulement aux États-Unis mais aussi au Canada, au Royaume-Uni et en Australie. Ils ont généralement été mis au point avec l'aide de consultants américains[21].

Un volume croissant de données personnelles est désormais recueilli en utilisant des nouvelles applications mobiles lors des visites de porte-à-porte. Ces données se retrouvent de plus en plus entre les mains de très nombreux bénévoles qui s'en servent pour alimenter les bases de données des partis avec les réponses collectées sur le terrain. Certaines autorités de protection des données se sont inquiétées de l'étendue des données personnelles qui pourraient être enregistrées pendant le démarchage électoral, par exemple concernant le sexe, l'origine ethnique ou la religion[22]. Leurs enquêtes suggèrent que des informations supplémentaires peuvent être saisies sans le consentement d'autres membres du foyer, voire de locataires, ou déduites de l'observation des lieux : voitures dans l'allée, enfants jouant dans le jardin, entretien général de la propriété, etc.[23]

Les données fonctionnent comme une source de *renseignement* lorsqu'elles sont accumulées à la suite d'essais et d'expérimentations. Sasha Issenberg a révélé l'étendue de ces pratiques dans *The Victory Lab* – « La science secrète des campagnes gagnantes »[24]. La comparaison systématique de l'impact des messages par le biais des tests A/B sont couramment utilisés par les organisateurs de campagne pour comprendre l'impact d'un site internet, des courriers électroniques, des textes, des éléments de conception, des slogans, du publipostage ainsi que des publicités à la télévision, à la radio et sur les réseaux sociaux.

Dans la plupart des pays, les partis savent de mieux en mieux utiliser les réseaux sociaux pour cibler les messages, recruter des bénévoles et des donateurs, et suivre les questions liées à la mobilisation politique. Contrairement au télémarketing plus traditionnel, la collecte de données sur les réseaux sociaux peut servir à créer des réseaux de contacts à des fins d'« organisation relationnelle » ou de « partage ciblé »[25]. Sur Facebook, par exemple, un parti peut télécharger une liste cryptée de numéros de téléphone ou de courriers électroniques pour déterminer des audiences personnalisées en fonction de la localisation, de la démographie, des intérêts, des comportements et des connexions. L'annonceur recevra un retour d'information en temps réel via des scores de pertinence sur l'efficacité de la campagne publicitaire et procédera alors aux ajustements nécessaires aux messages. Sur Facebook, une publicité politique est moins un message singulier qu'une machine complexe visant à produire d'autres messages au moyen desquels ses algorithmes apprennent et délivrent des messages subtilement différents qui dépendent de très nombreuses variables[26] diverses.

Il y a une diversité de mécanismes clandestins qui permettent de recueillir des informations sur les convictions politiques d'une personne pour produire des données de renseignement. Sur Facebook, par exemple, le fait d'appuyer sur le bouton « J'aime » peut faire apparaître l'icône d'un parti politique sur la page de l'utilisateur et révéler, peut-être involontairement, ses

[21] Je passe en revue ces systèmes dans : C. J. Bennett, "Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America?" *International Data Privacy Law*, Vol. 6, No. 4 (décembre 2016), 261-275.
[22] Office of the Information and Privacy Commissioner of BC, *Full Disclosure* (n 95) 15.
[23] Ibid 16.
[24] S. Issenberg, (2013). *The victory lab: The secret science of winning campaigns*. Portland : Broadway Books.
[25] Pierre-Olivier Pielaet, *Report on the Application of the principles of the modernised Convention 108 to the processing of data by political parties* (Strasbourg : Conseil de l'Europe, non publié 2020).
[26] Bogost, I. & A.C. Madrigal. (2020). How Facebook works for Trump. *The Atlantic.* https://www.theatlantic.com/technology/archive/2020/04/how-facebooks-ad-technolo gy-helps-trump-win/606403/

convictions politiques. Or, être « ami » d'un parti politique sur Facebook peut avoir des conséquences, notamment si l'utilisateur n'a pas appliqué les contrôles de confidentialité appropriés, car le parti concerné peut collecter son nom et sa photo à son insu et le « cibler »[27]. L'ONG Privacy International a critiqué l'utilisation clandestine d'autres identifiants uniques de publicité, de pixels et de « tags ». Elle a également examiné les différents paramètres de confidentialité des applications susceptibles de diffuser des annonces politiques, telles que TikTok, Snapchat et Pinterest, afin de déterminer leur conformité aux règles de transparence des annonces publicitaires[28].

Les données ont une *influence* lorsqu'elles sont utilisées pour micro-cibler les personnes afin de les inciter à voter (ou à ne pas voter) à faire des dons, du bénévolat, etc. Diverses pratiques de microciblage sont examinées par Tactical Tech : le géorepérage (diffusion d'un message visant uniquement des personnes situées à l'intérieur d'un périmètre géographique), le ciblage IP (utilisation d'informations fondées sur la localisation à partir d'adresses IP), le géociblage des téléphones portables ou des biens, les appels automatisés et les textos sur mobiles, la télévision adressable et le profilage psychométrique – la catégorisaion et l'attribution de traits de personnalité - pratique pour laquelle la société Cambridge Analytica est devenue célèbre[29]. L'application *WhatsApp* est devenue un instrument de campagne particulièrement puissant. Facile à utiliser, crypté de bout en bout et pouvant diffuser des messages à de larges groupes d'utilisateurs, ce logiciel est extrêmement répandu dans des pays comme l'Inde, le Brésil et d'autres pays du Sud[30]. Il permet non seulement aux partis d'adapter les messages à des groupes précis, mais offre également l'anonymat, ce qui permet de masquer facilement l'identité d'un expéditeur.

Aux États-Unis, Jeff Chester et Kathryn Montgomery suivent le « mariage de la politique et du commerce » en cours et la progression continue du marketing politique[31] effectué sur la base de données. Ils ont passé en revue sept techniques principales utilisées lors des campagnes de 2016 aux États-Unis et qui montrent toutes les consolidations massives de données effectuées dans l'écosystème du marketing numérique : le ciblage inter-appareils, la publicité programmatique, l'utilisation de modèles de jumeaux statistiques (une fonction proposée par Facebook), la publicité vidéo en ligne, la publicité télévisée ciblée ainsi que le ciblage psychographique, le neuromarketing et le ciblage émotionnel. Dès lors, rien ne permet plus maintenant de distinguer le microciblage politique des pratiques programmatiques contemporaines du secteur des technologies publicitaires, y compris le processus très

[27] Une analyse approfondie de l'utilisation de Facebook dans l'arène électorale est fournie dans U.K. Information Commissioner's Office, *Democracy Disrupted? Personal information and political influence* (11 juillet 2018) https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[28] Apart from Facebook and Google, what are other platforms doing about political ads? Voir : https://privacyinternational.org/long-read/3703/apart-google-facebook-and-twitter-what-are-other-platforms-doing-about-political-ads#TikTok-ad-targeting

[29] Tactical Tech. (mars 2019). *Personal Data: Political Persuasion – Inside the Influence Industry. How it works.* Berlin: Tactical Tech. https://tacticaltech.org/#/projects/data-politics/

[30] E. Hickok, 2018. *The Influence Industry: Digital Platforms, Technologies and Data in the General Elections in India*: https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-india.pdf; R. Evangelista and F. Bruno, "WhatsApp and Political instability in Brazil: targeted messages and political radicalisation," Internet Policy Review, Volume 8, n° 4 : https://policyreview.info/articles/analysis/whatsapp-and-political-instability-brazil-targeted-messages-and-political

[31] J. Chester J., & K.C. Montgomery (2017). The role of digital marketing in political campaigns. *Internet Policy Review*, *6*(4). https://doi.org/10.14763/2017.4.773

controversé des « enchères en temps réel » (RTB) qui a récemment fait l'objet d'un examen minutieux de la part des autorités chargées de la protection des données[32].

Dans une mise à jour de 2019 qui donne un aperçu des pratiques susceptibles d'être suivies lors du cycle électoral de 2020, les mêmes auteurs prédisent : un perfectionnement croissant des « technologies de résolution d'identité », un système commercial d'informations géospatiales qui arrive rapidement à maturité et qui améliore les stratégies de ciblage mobile et autres, l'expansion vers des plateformes de diffusion en continu et de vidéo numérique non réglementées et de nouvelles évolutions dans les techniques de personnalisation et de test[33].

En 2018, un rapport de l'organisation Demos commandé par l'ICO a passé en revue les techniques de marketing numérique au Royaume-Uni. Il s'agit probablement d'un des guides les plus fiables concernant les campagnes numériques dans les systèmes parlementaires. Demos a examiné les types de pratiques susceptibles d'être observées dans les campagnes politiques britanniques dans les années à venir[34], notamment :

- une segmentation plus fine du public ;
- un ciblage inter-appareils ;
- l'utilisation croissante des techniques psychographiques ;
- l'utilisation de l'IA pour cibler, mesurer et améliorer les campagnes ;
- l'utilisation de l'IA pour générer automatiquement du contenu ;
- l'utilisation de données à caractère personnel pour prédire les résultats des élections ;
- le contact par l'intermédiaire de nouvelles plateformes (par exemple, la vidéo numérique et les objets connectés).

Le développement de ces technologies a aussi des conséquences pour l'organisation des campagnes politiques. Alors qu'il était autrefois possible de distinguer les différents types d'organisations associées à une campagne politique, le réseau actuel d'institutions apparaît aujourd'hui plus complexe et opaque. On observe désormais que des alliances étroites se nouent dans plusieurs pays entre des courtiers en données politiques, des sociétés de publicité numérique, les plateformes de réseaux sociaux, des sociétés de gestion et d'analyse des données et des partis politiques et qu'elles forment un vaste « écosystème d'organisations chargées des campagnes électorales ». Ces organisations s'appuient de plus en plus sur un réseau ou un « attelage de campagne » afin de mener et d'intégrer toutes les activités considérées comme nécessaires à une élection : collecte de données, analyse de données, sondages, collecte de fonds, publicité numérique, publicité télévisée, messages électroniques et textuels, diffusion sur les réseaux sociaux, gestion d'événements, coordination de bénévoles et activités d'incitation à voter. Chacune de ces activités nécessite une coordination minutieuse[35].

C'est pourquoi, de manière générale, le volume de données collectées sur les électeurs est plus important que dans le passé, et ces données sont de plus en plus partagées à l'intérieur d'un

[32] ICO. (juin 2019). *Update report into adtech and real time bidding.* https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

[33] J. Chester & K. Montgomery (2019). The digital commercialisation of US politics – 2020 and beyond. Internet Policy Review. Volume 8, n° 4. Voir : https://policyreview.info/articles/analysis/digital-commercialisation-us-politics-2020-and-beyond

[34] J. Bartlett, J. Smith & R. Acton. *The Future of Digital Campaigning*. Demos, 2018. Voir : http://www.demos.co.uk/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf

[35] R.K. Nielsen, (2012). *Ground Wars: Personalized Communication in Political Campaigns*. Princeton : Princeton University Press; D. Kreiss, (2016). *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy.* Oxford : Oxford University Press.

réseau complexe d'organisations, impliquant certaines entreprises assez obscures, qui commencent à jouer un rôle important d'intermédiaires dans le processus démocratique. Ces tendances sont mondiales même si leurs incidences dans les différentes sociétés sont très variables.

L'utilisation des données à des fins électorales : mythes et réalités

Le discours actuel sur l'utilisation numérique de données à des fins électorales est souvent fondé sur l'impératif technique suivant : dans la mesure où elles sont disponibles, il est naturel d'utiliser des données sur l'électorat pour influencer les électeurs et les persuader de se présenter aux bureaux de vote. Cet impératif est au cœur des arguments de vente du secteur de l'analyse électorale et incite les acteurs à réclamer des données personnelles sur l'électorat qui soient encore plus nombreuses et précises. Ainsi, Cambridge Analytica a affirmé (à un moment donné) avoir recueilli jusqu'à 5 000 points de données sur plus de 220 millions d'Américains et utilisé plus de 100 variables de données pour modéliser des groupes cibles et prédire le comportement de personnes partageant les mêmes idées[36]. Certes, ces affirmations doivent être lues avec scepticisme mais elles s'appuient néanmoins sur une certaine logique. En effet, l'« industrie de l' influence politique » part du principe que persuader l'électeur américain, allemand, canadien, suédois, français ou britannique moyen n'est pas fondamentalement différent si l'on diffuse des messages personnalisés pertinents au bon moment, en utilisant le bon média, à condition que le candidat ou le parti ait suffisamment de données à sa disposition[37]. D'ailleurs, les partis politiques et les candidats en compétition dans les grandes démocraties considèrent désormais dans une large mesure que le microciblage politique est un moyen essentiel de prendre l'avantage sur leurs opposants.

Son efficacité suscite un débat permanent dans les milieux politiques et universitaires, d'autant que les ouvrages populaires publiés sur ces technologies, ainsi que les entreprises qui en sont friandes ont tendance à surévaluer leur impact réel. Il existe de nombreux mythes concernant l'utilisation des données à des fins de campagne électorale, et des études montrent que ces techniques sont bien plus efficaces pour mobiliser les militants que pour persuader les électeurs de changer d'attitude et de comportement[38]. Cela dit, il est également prouvé que les publicités ciblées peuvent faire appel à des préjugés et à des vulnérabilités et avoir pour effet d'écarter certains groupes du vote. Un reportage de Channel Four sur l'utilisation de techniques de microciblage lors des élections américaines de 2016 a montré clairement que les Afro-Américains avaient été classés de manière disproportionnée dans la base de données des électeurs républicains comme pouvant être « dissuadés ». La participation électorale a été nettement plus faible au sein de ce groupe dans les principales villes du Midwest par rapport à celle de 2012.[39]

Les entreprises qui commercialisent ces produits en vue de campagnes numériques sont majoritairement américaines, et les stratégies employées aux États-Unis se heurtent à des

[36] www.cambridgeanalytica.ca (consulté en mars 2017).
[37] Bennett, C.J. (août 2013). The politics of privacy and the privacy of politics: parties, elections and voter surveillance in Western democracies. *First Monday*, *Vol. 18*, No. 8.
[38] J. Baldwin-Philippi, J. (2017). The myths of Data-Driven Campaigning. *Journal of Political Communication, 34* (4); J. Baldwin-Philippi, (2019). Data Analytics: Between empirics and assumptions. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1437
[39] Channel 4 News (2020). Revealed: Trump Campaign strategy to deter millions of Black Americans from voting in 2016, septembre 28, 2020 at: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

contraintes fondamentales dans d'autres démocraties. En effet, les lois relatives à la protection des données et au respect de la vie privée en vigueur dans la plupart des autres démocraties limitent réellement les possibilités d'extraction des données à caractère personnel et, par conséquent, la portée et l'étendue de l'économie de ces informations. Des lois plus strictes sur le financement des campagnes électorales en application dans ces États limitent également l'achat de sources commerciales de données ainsi que les sommes dépensées dans les circonscriptions et à l'échelon national. Les analyses sophistiquées de l'électorat observées aux États-Unis ne sont pas aisément reproduites ailleurs.

S'agissant de l'application de la Convention 108 + aux campagnes politiques, il est donc important de ne pas oublier certaines réalités incontournables de l'environnement électoral qui prévalent aujourd'hui dans différents pays et que la nature et le niveau du ciblage des électeurs dans différentes juridictions seront déterminés par une interaction complexe de facteurs juridiques, politiques et culturels[40].

Outre les lois relatives à la protection des données au niveau national et international, il existe d'autres *facteurs juridiques* pertinents, notamment :

- les dispositions constitutionnelles et la jurisprudence en matière de liberté de communication, d'information et d'association, surtout en ce qui concerne les affaires publiques et politiques ;
- les lois électorales qui réglementent souvent la distribution des listes et registres électoraux et imposent des sanctions en cas d'utilisation et de divulgation illégitimes de ces listes ;
- les lois sur le financement des campagnes qui réglementent les sommes dépensées par les partis politiques et les candidats et qui imposent souvent la saisie de données sur les donateurs ainsi que les montants donnés ;
- les règles du télémarketing qui établissent les conditions dans lesquelles les spécialistes du marketing, les sondeurs et autres peuvent communiquer directement et de manière personnalisée ;
- les codes et règlements relatifs à la publicité en ligne ;
- les règlements relatifs à la transparence de la publicité électorale ;
- les règles antispams qui visent la communication non sollicitée par courrier ou texte électronique.

L'équilibre global sera également profondément affecté par les caractéristiques *institutionnelles* pertinentes du système politique qui façonnent la nature de la concurrence politique et le rôle qu'y jouent les données personnelles. Par exemple, le système électoral est-il fondé sur la représentation proportionnelle ou le scrutin uninominal majoritaire à un tour ? Le vote est-il obligatoire, comme en Australie et en Belgique ? Les partis organisent-ils des « élections primaires » internes comme certains l'ont fait récemment en France ? Quelle est la fréquence des référendums ?

Le système des partis est également essentiel. Combien de partis sont en concurrence pour l'obtention de sièges législatifs ? Les organisations des partis sont-elles centralisées ou décentralisées ? Les organisations chargées des campagnes locales sont-elles suffisamment autonomes pour décider les messages qu'elles ont élaborés elles-mêmes ? Quelles sont les sources de financement des campagnes pour les candidats et les partis locaux ?

[40] Bennett et Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, pp. 53-54.

Il y a aussi des variables *culturelles* plus larges, associées à l'expérience historique. Les pratiques de campagne directe de candidat à électeur, notamment le porte-à-porte ou le sondage par téléphone, sont-elles généralement acceptées ? Les électeurs font-ils confiance aux élites politiques ? Sont-ils généralement disposés à participer ouvertement à la vie politique et croient-ils que leur participation « fera une différence » ? Certaines cultures politiques, en particulier où les souvenirs de régimes autoritaires sont récents, n'acceptent absolument pas le niveau d'intrusion courant dans les campagnes politiques nord-américaines[41].

Il est donc important, s'agissant des risques pour la vie privée et de l'application des instruments réglementaires nationaux et internationaux relatifs à la protection des données, de fonder le travail d'analyse sur des pratiques réelles et d'être sensible aux nombreuses autres contraintes (extra-juridiques) qui limiteront l'importation d'analyses électorales et de techniques de campagne numérique en provenance des États-Unis. Partant de ces principes, comment la Convention 108 modernisée pourrait-elle être utilement appliquée à l'environnement des campagnes politiques dans les pays qui y ont adhéré, ou pourraient y adhérer à l'avenir ?

Les campagnes politiques, les partis politiques et la Convention 108+

En Europe, les campagnes politiques sont réglementées par des lois relatives à la protection des données depuis de nombreuses années. Les organisations politiques étaient couvertes par la Convention 108 originale et par la directive européenne de 1995 sur la protection des données. Il est entendu que l'ensemble des principes et des exigences s'applique dans son intégralité.

Cependant, certains de ces principes ont une signification particulière et nécessitent une analyse plus détaillée, notamment au regard de la Convention 108 + et de son rapport explicatif, des exigences du RGPD ainsi que des conclusions de certaines autorités de protection des données issues d'enquêtes sur les utilisations de données personnelles dans l'environnement politique. Un récent projet de code de conduite élaboré par l'ICO sur la prise en compte des normes de protection des données par les organisations politiques peut aussi être considéré.[42] Les principales questions de protection relatives à l'utilisation des données à caractère personnel dans le cadre de campagnes politiques ont également été abordées par le Comité européen de la protection des données (CEPD)[43].

Cette partie du document analyse les questions cruciales qui, au regard de la Convention 108 modernisée, influencent la conduite des campagnes politiques contemporaines. Il est important de noter que les campagnes politiques ne sont pas uniquement des campagnes électorales puisque de nombreuses sociétés organisent des référendums. Les campagnes ne sont donc pas seulement menées par des partis politiques formels. En effet, des organisations de campagne plus temporaires et informelles (du type de celles observées lors du référendum sur le Brexit de 2016) collectent et traitent les données personnelles de l'électorat. La campagne politique peut désormais mettre en jeu plusieurs acteurs qui ne sont ni des partis politiques ni des candidats (responsables du traitement) ; il s'agit notamment des plateformes de médias sociaux, des

[41] C.J Bennett (août 2013). The politics of privacy and the privacy of politics: parties, elections and voter surveillance in Western democracies. *First Monday*, *Vol. 18*, No. 8.

[42] UK, Information Commissioners Office (2019). Guidance on Political Campaigning: Draft Framework code for consultation at: https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf

[43] Comité européen de la protection des données (CEPD). (13 mars 2019). *Déclaration 2/19 sur l'utilisation des données à caractère personnel dans le cadre de campagnes politiques*. Voir : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

courtiers en données, des réseaux publicitaires, des sociétés d'analyse, des cabinets de sondage et des consultants.

1) L'identification et la réidentification des données sur les opinions politiques

La principale question concernant le seuil d'application du droit de la protection des données est celle de la définition des « données à caractère personnel ». En effet, l'étendue de cette notion a d'énormes conséquences sur le traitement des données dans le cadre des campagnes politiques.

La Convention 108 + s'applique aux données à caractère personnel concernant une « personne identifiée ou identifiable ». Une personne qui ne pourrait être identifiée qu'au moyen d'« opérations excessivement complexes, longues et coûteuses » ne pourrait pas être considérée comme identifiable. Les avancées technologiques et autres développements peuvent avoir une influence sur ce qui pourrait être considéré comme des délais et des efforts déraisonnables dans différents contextes[44].

Comme dans le RGPD, la possibilité d'identifier une personne ne dépend pas uniquement de son nom ou d'un autre identifiant légal. En effet, la variable critique tient à la capacité de l'individualiser ou de la « distinguer ». Ce processus peut se produire au moyen d'identificateurs d'appareils (ordinateurs, etc.), notamment les adresses IP ou les identités pseudonymisées. Dès lors, si une personne peut être « adressée » individuellement, même si ce n'est pas par son nom, ces données à caractère personnel sont identifiables. En outre, si elle peut être identifiée grâce à une combinaison de différentes sources de données, par exemple l'âge, le sexe, la géolocalisation, la situation familiale, etc., ces données ne devraient pas être considérées comme anonymes. Il existe donc un continuum d'identification, et les organisations devraient en déduire que si ces données peuvent être utilisées pour identifier ou réidentifier une personne concernée, alors la loi sur la protection des données s'applique et l'individu a des droits sur ces données[45].

Historiquement, le type d'analyse de l'électorat menée en Amérique du Nord n'a pas été possible en Europe, ni dans d'autres pays, en raison de l'interdiction stricte de traiter des données sur les opinions politiques. Les entreprises ont donc fait la promotion de divers produits utilisant des données géo-démographiques agrégées et/ou anonymisées pour établir le profil politique de circonscriptions électorales spécifiques. Ces données sont ensuite utilisées pour proposer une publicité électorale plus ciblée, des campagnes de porte-à-porte et des opérations d'incitation à voter (GOTV).

Dans le contexte européen, la société créée par Thomas Liegy et ses collègues (aujourd'hui eXplain) est un bon exemple. Cette société, qui a de nombreux clients politiques en Europe et au-delà, commercialise notamment un produit appelé Pivot, qui « permet d'identifier les circonscriptions dans lesquelles les électeurs sont les plus susceptibles de 'changer d'opinion' et de voter pour vous. Notre technologie permet alors de mener des campagnes de porte-à-porte efficaces et attrayantes dont l'expérience prouve qu'elles constituent le moyen le plus efficace de

[44] Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Strasbourg : Conseil de l'Europe, 2018)

[45] J.Polonetsky, O. Kene, K. Finch (2016). Shades of Grey: Seeing the full spectrum of Practical data De-Identification, 56 Santa Clara Law review 593

gagner des électeurs[46] ». Les analyses sont appliquées à une base de données spécialisée d'informations socio-électorales qui a été structurée pour « identifier les circonscriptions les plus densément peuplées d'électeurs qui pourraient changer leurs habitudes de vote en votre faveur ». Ces applications ont été largement utilisées lors de la campagne « Grande Marche » lancée par Emmanuel Macron en 2016. Le logiciel a sans doute permis aux militants de la campagne de démarcher des électeurs français qui n'avaient peut-être pas été contactés auparavant[47].

Ces produits, ainsi que des produits apparentés, sont présentés comme étant respectueux de la vie privée et conformes à la protection des données. Pourtant, la question se posera toujours de savoir si les données d'un électeur qui ont été saisies sont effectivement « anonymisées » selon les normes en vigueur, et si les déductions qui en ont été tirées signifient en fait que ses données personnelles en matière politiques ont bel et bien été traitées.

2) La définition des « opinions politiques » en tant que forme de données sensibles

Il y a une considérable jurisprudence sur l'importance du débat et du pluralisme politiques en vertu de l'article 10 de la CEDH. La Cour européenne des droits de l'homme a déclaré à plusieurs reprises que l'expression d'opinions politiques a un statut privilégié, en tant que fondement de la liberté d'expression et de la liberté des élections[48]. En outre, le droit à des élections libres inscrit à l'article 3 de la CEDH entraîne une obligation positive pour les États membres d'établir les conditions dans lesquelles les individus peuvent librement former et exprimer leurs opinions et choisir leurs représentants sans discrimination. L'article 14 interdit la discrimination fondée sur les "opinions politiques ou autres", bien que la Cour ait rarement examiné des cas de discrimination fondée sur ces motifs[49]. Les opinions politiques ont également été définies comme une catégorie de données sensibles par la Convention 108 de 1981[50] comme par la Directive de l'UE de 1995 sur la protection des données[51].

De même, la Convention 108 + indique que le traitement « de données à caractère personnel pour les informations qu'elles révèlent concernant l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres, la santé ou la vie sexuelle, n'est autorisé qu'à la condition que des garanties appropriées, venant compléter celles de la présente Convention, soient prévues par la loi. » Elle ajoute que « ces garanties doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination[52] ». Le rapport explicatif qui l'accompagne met en évidence les dangers de discrimination découlant d'un traitement inapproprié de données à caractère personnel sensibles, mais il ne donne pas d'autres indications sur ce que signifie « opinions politiques » et ne

[46] https://explain-technology.com/our-products/pivot/
[47] Judith Duportail, The 2017 Presidential Election: The arrival of targeted political speech in French Politics. Tactical tech. Voir : https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-france.pdf
[48] Commission de Venise, Digital Technologies and Elections, p. 13.
[49] Cour européenne des droits de l'homme, Guide on Article 14 of the European Convention of Human Rights and on Article 1 of Protocol No. 12 to the Convention (31 août 2020), p. 30 disponible à : https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf
[50] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 1981, article 6 : https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680078b37
[51] Directive européenne sur la protection des données, article 8.
[52] Convention 108, article 6.

mentionne pas d'exemptions concernant le traitement des données personnelles à des fins électorales, ce qui est le cas dans le RGPD.

Selon l'article 9 (1) du RGPD, « le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits[53]. » Ces principes découlent également des principes de non-discrimination fondée sur l'opinion politique consacrés à l'article 21 de la Charte des droits fondamentaux de l'Union européenne. Le traitement de telles données peut comporter des risques particuliers de « probabilité variable et gravité » en ce qui concerne les droits et les libertés des personnes.[54]

Le RGPD énumère un certain nombre d'exemptions, dont deux sont directement liées au contexte politique. L'article 9.2 d) autorise le traitement lorsqu'il est effectué « dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ». L'article 9.2. e) permet également le traitement qui « porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée ». En ce qui concerne les partis politiques, le considérant 56 du RGPD énonce ce qui suit :

> « Lorsque, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique dans un État membre requiert que les partis politiques collectent des données à caractère personnel relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé pour des motifs d'intérêt public, à condition que des garanties appropriées soient prévues »[55].

Aucune de ces dispositions n'est sensiblement différente de celles de la Directive de 1995 sur la protection des données personnelles.

Nous avons constaté que des États membres profitent de ces dispositions pour donner une plus grande marge de manœuvre aux partis politiques et aux candidats dans le traitement des données personnelles. Dans la loi britannique sur la protection des données, par exemple, un parti politique enregistré peut traiter des données relatives aux opinions politiques « dans le cadre de ses activités politiques légitimes », à condition que cela ne cause pas « de dommage ou de préjudice important à la personne concernée » - c'est une norme relativement élevée et qui devra probablement être confirmée par la personne elle-même. En outre, le paragraphe 22 de l'annexe 1 prévoit une condition d'intérêt public particulière s'appliquant aux partis politiques qui sont engagés dans des « activités politiques[56] » et qui souhaitent traiter des données sensibles dans

[53] Règlement général de l'UE sur la protection des données, article 9 (1).
[54] Règlement général de l'UE sur la protection des données, considérant 75
[55] *Règlement général* de l'UE sur la *protection des données*, considérant 56.
[56] Royaume Uni, loi sur la protection des données (2018) c.12. annexe 1 (para 22) disponible à : http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted

ce domaine. Dans d'autres pays, des lois espagnoles et roumaines contiennent des dispositions d'une portée similaire qui ont motivé des plaintes émanant d'organisations de la société civile[57]. En Espagne, par exemple, la Cour constitutionnelle a annulé l'exception d'intérêt public dans la loi espagnole sur la protection des données mettant en œuvre le GDPR qui aurait permis aux partis politiques de saisir des données sur les opinions politiques sans consentement et de profiler les électeurs.[58]

Il n'y a pas eu, non plus, d'analyse significative du sens de l'expression « opinions politiques » comme catégorie de données sensibles dans le droit de la protection des données. Elle ne se définit pas elle-même bien que l'on puisse trouver des exemples utiles dans les orientations de l'ICO sur la campagne politique[59]. J'ai d'ailleurs soulevé un certain nombre de questions concernant l'étendue de sa définition dans des travaux antérieurs. Le sens de l'expression « dans le cadre des activités électorales » et la définition des « raisons d'intérêt public » sont également vagues[60].

La notion d'opinions politiques peut être interprétée à différents niveaux. De prime abord, il pourrait s'agir d'une *idéologie ou d'une conviction politique*, libérale, conservatrice, socialiste, communiste, etc. Il est intéressant de noter que c'est le sens que lui donne la loi japonaise sur la protection des données, désormais « adéquate ». Les « opinions politiques » n'y sont pas explicitement définies comme telles. En effet, la loi (art. 2, par. 3) utilise la notion plus large et plus informe de « croyance » (*shinjo*) qui englobe l'idéologie politique et d'autres systèmes de croyances, y compris la religion. Ces données « nécessitent une attention particulière afin de ne pas causer de discrimination injuste, de préjudice ou d'autres désavantages à l'intéressé[61]. »

Autre interprétation possible, celle de l'*affiliation* politique, voire de l'affiliation partisane, qui pourrait se rapporter à l'adhésion concrète à un parti dont les listes peuvent être légalement traitées. Cette notion pourrait également faire référence aux donateurs financiers que les partis doivent, dans de nombreux pays, enregistrer et déclarer en raison des règles de transparence du financement des campagnes. Il pourrait aussi s'agir d'une notion élargie de *l'identification partisane* pouvant être déduite des informations collectées sur les membres, mais aussi du profilage effectué au moyen des systèmes de gestion des relations avec les électeurs. Beaucoup de partis politiques connaîtront ainsi leurs vrais sympathisants et feront campagne pour les inciter à aller voter. La science politique comprend une branche qui analyse comment l'esprit partisan est corrélé avec différentes variables socio-démographiques dans le temps et l'espace : le sexe, la classe, la race, le lieu géographique, etc. Les modèles varient, mais ces facteurs donnent des indices très importants sur ce qu'est un comportement politique, voire des « opinions politiques ».

On trouve ensuite, bien entendu, les opinions sur les *politiques* : économique, sociale ou environnementale, ou concernant l'emploi, l'immigration, les droits des minorités, etc. Ces opinions seront également corrélées avec une idéologie ou l'adhésion à un parti. Elles peuvent

[57] Privacy International 30 avril 2019. "GDPR loopholes facilitate data exploitation by political parties". Voir : https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties

[58] Spanish Constitutional Court strikes down political profiling," GDPR Today, Vol. 4. No 11 (June 2019) at: https://www.gdprtoday.org/spanish-constitutional-court-strikes-down-political-profiling/

[59] ICO, Guidance on Political Campaigning, pp. 43-44

[60] C. J. Bennett (avril 2018). Cambridge Analytica and Facebook: a Wake-Up Call. *Privacy Laws and Business International Report,* numéro 152. C.J. Bennett, "Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America?" *International Data Privacy Law*, Vol. 6, No. 4 (décembre 2016), 261-275.

[61] Entretiens, Commission japonaise de l'information personnelle, mai 7, 2018.

aussi être sensibles, en particulier dans les pays qui présentent des tendances actuelles ou récentes à l'autoritarisme et qui souhaitent isoler et persécuter ceux qui ont des opinions anti-gouvernementales. Ainsi, une opinion politique sur les droits des homosexuels par exemple, dans un pays appliquant des lois homophobes, est sans aucun doute très sensible puisqu'elle peut révéler une préférence sexuelle et pourrait conduire au type de discrimination à laquelle s'oppose la Convention 108 +.

La Convention et le RGPD indiquent également que les données sensibles sont celles qui *révèlent* des opinions politiques[62], lesquelles peuvent être déduites de toute une série d'activités (par exemple, de la lecture de magazines ou de journaux), de conditions (telles que le voisinage ou le code postal) ou de convictions et préférences politiques.

Ces questions relatives à la collecte de données personnelles à des fins de campagne politique ont fait l'objet d'une enquête menée par l'ICO dans le contexte du Royaume-Uni et qui a fait l'objet d'un rapport de 2018 intitulé *Democracy Disrupted*. Toute entreprise qui fournit des données à des partis politiques (plusieurs d'entre elles sont mentionnées dans le rapport) « ne peut pas réutiliser ces données à caractère personnel pour une campagne politique sans d'abord l'expliquer à la personne concernée et obtenir son consentement[63] ». Des déclarations d'intention vagues et générales ne seront vraisemblablement pas suffisantes. De même, les partis politiques qui obtiennent des informations à caractère personnel auprès d'organisations tierces (courtiers en données, etc.) doivent veiller à ce qu'un consentement approprié ait été obtenu. Cet exercice de « diligence raisonnable » doit pouvoir être vérifié.

En outre, certains partis politiques utiliseraient un logiciel qui associe une ethnicité et un âge aux noms des individus au motif que ces données « supposées » ou « déduites » ne sont pas nécessairement des informations à caractère personnel sur la personne concernée. L'ICO a contesté ce point de vue. En effet, ces données, dès lors qu'elles sont liées à un individu, constituent des données à caractère personnel et sont soumises aux exigences relatives au traitement de catégories spéciales de données. Il existe un risque important que les hypothèses ou les prévisions concernant l'origine ethnique (fondées, par exemple, sur l'héritage du nom) soient inexactes et comportent des risques importants pour la personne concernée[64]. Cette interprétation est cohérente avec des précédentes orientations émises par le Groupe de travail de l'article 29 sur la prise de décision individuelle automatisée et le profilage qui relevait que « le profilage peut créer des données de catégorie spéciale inférées à partir de données qui, elles-mêmes, ne sont pas des données de catégorie spéciale mais le deviennent lorsqu'elles sont combinées avec d'autres.[65]

Ainsi, les « opinions politiques » peuvent être une catégorie très large pouvant englober l'idéologie, l'affiliation, l'identification ou les convictions politiques. Ces « opinions » peuvent être dérivées ou déduites d'un large éventail d'activités ou de conditions. L'étendue de la définition de l'expression « opinions politiques » a d'énormes conséquences sur les règles régissant la saisie des données personnelles dans le cadre des campagnes politiques.

[62] Règlement général sur la protection des données de l'UE, article 9(1)
[63] ICO, *Democracy Disrupted*, p. 15.
[64] ICO, *Democracy Disrupted*, p. 31.
[65] Groupe de travail de l'article 29, Lignes directrices sur la prise de décision individuelle automatisée et le profilage à des fins de règlementation, 2016/679, 6 février 2018, p. 15, disponible à : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

3) Les règles encadrant les communications politiques consenties

Les problèmes liés aux communications politiques inappropriées soulèvent des questions quant à l'application de règles concernant la possibilité d'accepter ou de refuser des communications diffusées par divers médias et plateformes traditionnels ou plus modernes. Ces questions ont préoccupé les autorités de protection des données par le passé et continueront de le faire à mesure que les moyens de diffuser des publicités politiques à des segments plus précis de l'électorat deviendront plus perfectionnés. En Europe, la plupart d'entre elles ont reçu des plaintes générées par des communications non sollicitées émanant de partis politiques, notamment des partis que la personne concernée ne soutiendra jamais, ce qui soulève des interrogations indignées des plaignants sur la manière dont leurs coordonnées ont été obtenues. À cet égard, la communication politique touche parfois des sensibilités qui n'existent pas dans le monde commercial[66].

La principale question est de savoir si la communication de contenus politiques doit être traitée d'une manière fondamentalement différente de la diffusion de messages commerciaux. Historiquement, les règles relatives au « marketing direct » ou au « télémarketing » avaient tendance à ne faire aucune distinction. L'exposé des motifs accompagnant la Recommandation n° R (95) 4 sur la « protection des données à caractère personnel dans le domaine des services de télécommunication » indique explicitement que la Convention 108 originale s'appliquait non seulement au marketing commercial, mais aussi au marketing politique[67]. Cette recommandation trouve son origine dans une recommandation de 1985 relative à la *protection des données à caractère personnel utilisées à des fins de marketing direct*, qui contenait une définition très large du marketing direct et ne faisait aucune distinction entre messages commerciaux et messages politiques.[68]

S'agissant de la Convention 108 +, le droit de contrôler des communications intrusives émanant de partis politiques ou de candidats est inscrit dans : l'article 5 sur la légitimité du traitement et la qualité des données, l'article 8 sur la transparence et l'article 9 sur les droits des personnes concernées, en particulier le droit de s'opposer au traitement. Dans ce domaine, il est essentiel de trouver un équilibre approprié entre les droits et intérêts en matière de protection des données et les droits à la liberté d'expression énoncés à l'article 11, point b).

Plusieurs autorités européennes de protection des données ont publié des orientations sur le marketing politique inapproprié qui s'appuient sur la directive de 1995 sur la protection des données et la directive de 2002 sur la protection de la vie privée dans le secteur des communications électroniques[69]. On peut citer à titre d'exemple une série d'orientations émanant

---

[66] Bennett, *Voter databases, micro-targeting and data protection law*, p. 270.

[67] Conseil de l'Europe (1995). Exposé des motifs de la Recommandation n° R (95) 4 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques, paragraphe 85. Voir : https://rm.coe.int/16806846cc

[68] Conseil de l'Europe,1985. Recommandation n ° R (85) 20 sur la protection des données à caractère personnel utilisées à des fins de marketing direct. Strasbourg : Conseil de l'Europe, octobre 1985. Voir : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336

[69] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »), (JL L201), voir : http://ec.europa.eu/justice/dataprotection/law/files/recast_20091219_en.pdf

de l'ICO[70] et de la CNIL[71]. La CNIL a également émis des règlements sur le spam en réponse au scandale « Sarkospam » de septembre 2005, lorsque des centaines de milliers de courriers électroniques non sollicités ont été envoyés au nom du candidat à la présidence Nicolas Sarkozy. Cette affaire a entraîné une série de recommandations de la CNIL sur l'utilisation de fichiers par les partis politiques, les groupes, les candidats et les élus[72].

Les règles nationales prévoient généralement que les organisations chargées des campagnes politiques doivent obtenir le consentement des personnes ciblées avant de leur envoyer des courriers électroniques ou des textos ou encore de les solliciter par des appels automatisés à des fins de marketing. L'appelant est tenu d'indiquer explicitement le parti qu'il représente, d'afficher clairement le numéro d'appel et d'enregistrer et respecter toute demande des personnes de ne pas être rappelées. Un parti qui utilise des listes à des fins de marketing doit tenir des registres pour démontrer ce à quoi la personne a consenti et comment elle y a consenti. Lorsqu'il existe une liste de personnes à ne pas appeler, l'organisation chargée de la campagne doit en tenir compte[73].

Les campagnes politiques sont également concernées par les règles relatives à la réception des « cookies ». L'article 5, paragraphe 3, de la directive « vie privée et communications électroniques » exige un consentement éclairé préalable pour archiver des informations stockées sur le terminal d'un utilisateur ou y accéder. Les responsables du traitement doivent demander aux utilisateurs s'ils acceptent la plupart des cookies et des technologies apparentées avant que le site ne commence à les activer. Pour que le consentement soit valide, il doit être éclairé, spécifique, donné librement et constituer une indication réelle des souhaits de la personne. Rien dans la directive ne suggère que cette disposition ne s'applique pas aux sites internet des partis politiques. En fait, certains partis politiques ont été pris à enfreindre ces règles[74].

Le RGPD précise que le traitement est autorisé pour les membres, les anciens membres ou ceux qui ont des « contacts réguliers ». Les orientations de la CNIL par exemple, partent du principe qu'une personne qui a pris des mesures positives pour une demande d'adhésion, faire un don ou se connecter régulièrement consent implicitement à une communication ultérieure. Au-delà de ces catégories étroites, un consentement explicite doit être obtenu. Cependant, la signification de l'expression « contacts réguliers » dans le contexte des différents réseaux sociaux fera certainement l'objet d'un litige permanent. Il est évident que les règles doivent être plus nuancées pour prendre en compte la diversité des différents médias sur lesquels les campagnes politiques se déroulent actuellement.

---

[70] U.K. Information Commissioner's Office, *Guidance on Political Campaigning* <https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

[71] France, CNIL. Communication politique : obligations légales et bonnes pratiques (janvier 2012). Les guides de la CNIL. Voir : http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Politique.pdf

[72] Délibération n° 2006-228 du 5 octobre 2006 portant recommandation relative à la mise en œuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques. Voir : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000459927

[73] ICO, *Guidance on Political Campaigning.*

[74] Bennett, *Voter databases, micro-targeting and data protection law*, p. 270.

4) Les questions de proportionnalité à la lumière des objectifs légitimes

La Convention 108 + énonce que « le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu »[75]. Le traitement des données est effectué soit sur la base du « consentement libre, spécifique, éclairé et non ambigu de la personne concernée », soit sur la base d'un autre fondement légitime prévu par la loi. Des exemples de tels intérêts légitimes sont fournis dans le rapport explicatif qui l'accompagne, et il n'est fait aucune mention du traitement des données par des organisations chargées de campagnes ou des organisations politiques. En outre, le responsable du traitement n'est pas autorisé à traiter des données « pour des finalités non définies, imprécises ou vagues[76]».

Cela étant, la Convention précise que la « liberté d'expression » est un intérêt légitime qui doit être mis en balance avec les droits de la personne concernée. Le rapport explicatif mentionne à cet égard « l'expression journalistique, académique, artistique ou littéraire ». Il n'est pas fait mention de l'expression politique. Quels sont donc les « objectifs légitimes » d'une campagne politique et comment faut-il les définir et les délimiter ?

Nul ne peut contester que les partis politiques et les candidats ont besoin de communiquer efficacement avec l'électorat. En effet, ils doivent présenter leur stratégiques politiques et les candidats, comprendre les besoins et les convictions des électeurs, encourager la participation au processus démocratique et mobiliser leurs partisans le jour des élections. La question la plus intéressante est de savoir quelle est la quantité d'informations dont les partis politiques et les candidats doivent disposer sur ces citoyens pour pouvoir jouer leur rôle essentiel ? D'une manière générale, que doit savoir l'orateur politique sur les membres de son auditoire afin de pouvoir lui parler efficacement et de leur permettre d'exercer leurs droits démocratiques ?

Sur cette question, les traditions culturelles façonnent les pratiques de campagne autant que les dispositions légales. Dans certaines sociétés, comme aux États-Unis, il existe une présomption générale en faveur d'une communication ouverte entre les électeurs et les acteurs politiques. Dans d'autres, notamment la société japonaise qui est un excellent exemple, les campagnes individualisées ainsi que le microciblage sont non seulement mal vus et mais parfaitement illégaux et associés à des problèmes historiques de corruption politique. Dans certaines sociétés, le démarchage au porte-à-porte est courant, voire attendu. Dans d'autres, en particulier aux souvenirs récents de régime autoritaire, l'idée qu'un homme politique puisse frapper à la porte pourrait suciter crainte et suspicion. Les « intérêts légitimes » des campagnes politiques évolueront donc énormément en fonction des attentes raisonnables de l'électorat et des contextes historiques et politiques[77]. L'ICO a déjà abordé les différentes activités qui font, ou non, la promotion de l'engagement politique et peuvent, en conséquence, être invoquées comme un « intérêt légitime » au titre de la loi britannique[78].

Dans la grande majorité des cas, le contact direct du parti ou du candidat avec l'électeur doit pouvoir faire l'objet d'un « consentement libre, spécifique, éclairé et non équivoque », que les

[75] Convention 108 +, article 5.
[76] Rapport explicatif, p. 9.
[77] Bennett et Oduro Marfo, *Privacy and International Democratic Engagement*, pp. ii.
[78] ICO, *Guidance on Political Campaigning.*

données personnelles soient recueillies sur le pas de la porte, au téléphone ou en ligne. Il y a un « contexte spécifique » à la campagne électorale qui devrait être clairement délimité par rapport à d'autres fins et situations commerciales ou publiques[79]. La question de savoir s'il existe ou non une « base légitime pour le traitement prévu par la loi » évoluera également d'une société à l'autre. Le fait que, dans certains pays, des listes électorales complètes soient partagées en toute légalité avec les partis et les candidats au début de chaque cycle électoral légitime le processus de communication avec les électeurs et sert de motif d'intérêt public à la participation démocratique. Les pratiques diffèrent quant à la manière dont ces listes sont transférées, au format de transmission (numérique ou non) et à la durée de leur conservation.

La situation est moins claire en ce qui concerne le traitement d'autres données sur l'électorat dans les bases de données de gestion des relations avec les électeurs. Le seul exemple européen est le Royaume-Uni, mais il en existe d'autres au Canada, en Australie et bien sûr, aux États-Unis. Dans ces sociétés, les partis utilisent la liste générale des électeurs, ou registre électoral, qui contient des données de base sur les ménages et les complètent avec des renseignements provenant d'autres sources : démarchage à domicile, sondages téléphoniques, pétitions, sources de données provenant de tiers, informations de recensement, etc[80].

Des autorités de protection des données ont parfois interdit à des partis ou des candidats d'utiliser des listes d'organisations apparentées (églises, clubs, associations, etc.) à des fins de communication politique.[81] Des problèmes se posent également lorsque des membres élus du corps législatif, qui peuvent accéder en cette qualité à des données à caractère personnel, les utilisent délibérément ou non, à des fins électorales. Dans les systèmes parlementaires, un « pare-feu » est censé exister entre les données personnelles collectées au titre des responsabilités liées aux circonscriptions ou législatives et celles qui sont utilisées pour les campagnes politiques. Mais cette distinction s'estompe souvent et la démarcation entre communication officielle, communication institutionnelle et campagne électorale n'est pas toujours claire. [82]

Enfin, se pose la question des listes achetées auprès *de courtiers en données*. En août 2018, l'ICO (Information Commissioner Office) a infligé une amende au courtier Emma's Diary pour avoir vendu des données au Parti travailliste sur les « nouvelles mères ». Cette société, qui fournit des conseils sur la grossesse et la garde d'enfants, a vendu à Experian Marketing Services, une filiale de l'agence de référence en matière de crédit, des informations réservées à l'usage exclusif du Parti travailliste. Experian a ensuite créé une base de données que le parti a utilisée pour dresser le profil des nouvelles mères et contacter celles qui vivent dans des circonscriptions dont les sièges sont marginaux afin de leur faire connaître ses politiques en matière de petite enfance lors de l'élection générale de 2017[83].

5) Le traitement des données à caractère personnel rendues « publiques »

[79] Rapport explicatif, p. 8.

[80] Bennett and Oduro Marfo, *Privacy, Voter Surveillance and Democratic Engagement*, pp. 21-27

[81] Bennett, "Voter databases, micro-targeting and data protection law", p. 267

[82] Ibid

[83] ICO News Release (09 août 2018). "Emma's Diary fined 140,000 pounds for selling personal information for political campaigning", voir : https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/

La Convention 108+ n'exempte pas de leurs obligations les responsables qui ont traité des données parce qu'elles étaient prétendument « disponibles ». Elle ne fait aucune distinction entre les « données à caractère personnel accessibles au public » et les autres formes de données personnelles. Le Comité européen pour la protection des données (CEPD) a également insisté sur le fait que les données personnelles qui sont rendues publiques ou partagées par les électeurs, même si elles ne révèlent pas des opinions politiques, sont toujours soumises au droit européen en matière de protection des données et protégées par lui. Ainsi, les données recueillies sur les réseaux sociaux pour contacter les électeurs ne peuvent être traitées que dans le respect des obligations en matière de transparence, de spécification des objectifs et de licéité[84].

La CNIL a rendu plusieurs arrêts sur l'utilisation de données collectées sur des réseaux sociaux dans le cadre de campagnes politiques et a établi des distinctions entre contacts réguliers et contacts occasionnels. Les premiers concernent « toute personne qui accomplit, auprès d'un parti politique, une démarche positive en vue d'entretenir des échanges réguliers et touchant directement à son action politique ». Dans la terminologie des réseaux sociaux, cela signifie suivre quelqu'un sur Twitter, devenir ami avec quelqu'un sur Facebook ou plus généralement, démontrer une volonté de maintenir un contact régulier avec le parti politique ou le candidat. En revanche, un « contact occasionnel » désigne « toute personne qui sollicite ponctuellement un parti politique ou un candidat, sans entretenir avec lui d'échanges réguliers dans le cadre de son activité politique » et, par exemple, qui « aime » ou « partage » sur Facebook, ou encore qui « retweete ». Un premier et unique message peut être adressé à un contact occasionnel pour savoir s'il consent à recevoir des messages de communication politique. Si elle répond positivement, la personne contactée devient un contact régulier. Mais en cas de réponse négative ou d'absence de réponse, ses données ne peuvent pas être traitées légalement et doivent être supprimées[85].

Des règles similaires s'appliquent au traitement de données issues de plateformes de réseaux sociaux dans le but de les rapprocher de certaines informations de contact, notamment les adresses de messagerie électronique, afin de personnaliser la communication avec les électeurs. En général, le droit européen ne permet pas l' « extraction » de données à caractère personnel des médias sociaux sans un consentement explicite. Au regard de ces normes, ces personnes ne sont pas considérées comme des « contacts réguliers ». Un programme géré par la société Nationbuilder (« Nationbuilder Match ») a été déclaré illégal par la CNIL. Cette société a dû interrompre ses services dans le monde[86].

Des normes analogues ont été appliquées aux partis politiques au Canada. Les partis politiques n'ont pas l'autorisation d'ajouter à leur base de données des informations à caractère personnel recueillies grâce à des réseaux sociaux uniquement parce que la personne avait interagi avec le

[84] CEPD, *Déclaration 2/2019 sur l'utilisation des données personnelles dans le cadre des campagnes politiques*. 13 mars 2019, disponible à : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

[85] Commission nationale de l'informatique et des libertés, « Élections 2016/2017 : quelles règles doivent respecter les candidats et partis ? » Voir : https://www.cnil.fr/fr/elections-2016-2017-quelles-regles-doivent-respecter-les-candidats-et-partis; Commission nationale de l'informatique et des libertés, « Communication politique : quelles sont les règles pour l'utilisation des données issues des réseaux sociaux ? » (8 novembre 2016). Voir : https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

[86]Nationalbuilder Match désactivée en France (31 mars 2017) voir : https://nationbuilder.com/nbmatch_france

parti en « aimant » un message ou un tweet[87]. L'ICO britannique a noté que le droit en matière de protection des données n'empêche pas les partis politiques d'obtenir et d'utiliser des données personnelles provenant de sources accessibles au public. Néanmoins, ils doivent toujours respecter la loi sur la protection des données et informer les électeurs de manière appropriée : « [l]'ICO s'inquiète du fait que des partis politiques utilisent cette fonctionnalité sans que les personnes concernées ne reçoivent d'informations appropriées. Les partis doivent donc inclure le déploiement de ces plateformes dans le cadre des futures évaluations d'impact sur la protection des données[88] ».

6) La transparence

Même lorsque le traitement est licite, les organisations doivent être transparentes quant à la base juridique du traitement, aux catégories de données traitées, aux destinataires de ces données et aux moyens d'exercer les droits à la protection des données[89]. Certaines informations essentielles sur le traitement doivent être fournies volontairement. Il s'agit notamment de l'identité du responsable du traitement, de la base juridique du traitement, des catégories de données traitées et des modalités d'exercice des droits. Les informations peuvent également comprendre la durée de conservation, le raisonnement qui sous-tend le traitement des données et des informations sur leurs transferts[90].

Il est entendu que le parti politique (ou en cas de référendum, les organisateurs de la campagne) est le responsable du traitement et assume toutes ces obligations. Il existe toutefois de nombreux contextes différents dans lesquels les partis et les campagnes peuvent communiquer avec les électeurs : en porte à porte, par téléphone, par l'intermédiaire de leurs sites internet, sur les réseaux sociaux, dans les réunions publiques et autres. Souvent, la collecte de données à lieu dans la frénésie d'une courte campagne électorale, lorsque les pressions pour frapper aux portes, démarcher par téléphone, mobiliser des agents et des bénévoles et collecter des dons sont très fortes. Les premières enquêtes ont révélé que les partis politiques contournent souvent ces exigences quand les campagnes sont très agressives.

De nombreuses conclusions du rapport 2018 de l'ICO, par exemple, ont trait au manque de transparence du « traitement équitable ». Le rapport critique les partis dont les politiques de confidentialité manquent de transparence et de clarté au regard des obligations imposées par le RGPD en matière de confidentialité. Les partis doivent également être particulièrement vigilents lorsqu'ils se procurent des informations auprès d'organisations tierces et veiller à ce qu'un consentement approprié ait été obtenu et que les exigences de transparence du RGPD soient respectées[91]. Il est urgent, au lendemain du scandale de Cambridge Analytica/Facebook, de renforcer la confiance dans le processus démocratique et le respect des normes de transparence dans le droit de la protection des données en est un moyen essentiel.

De récentes propositions visant à améliorer la transparence dans le secteur publicitaire, y compris par l'archivage numérique, offrent aux autorités de protection des données la possibilité de mieux comprendre la nature du microciblage politique dans leurs sociétés respectives, le niveau de sa

[87] OIPCBC*, Full Disclosure*, p. 21
[88] UK, ICO, *Democracy Disrupted*, p. 32.
[89] Convention 108+, article 8.
[90] Rapport explicatif, p. 13.
[91] ICO, *Democracy Disrupted*, p. 6.

granularité et la ou les sources de paiement. Dans le domaine des campagnes politiques, les infractions à la protection des données peuvent également être des infractions liées au financement des élections, et vice versa.[92].

7) Les règles encadrant la prise de décisions automatisée et le profilage des électeurs

La Convention 108+ stipule que « toute personne a le droit de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte[93] ». Selon le rapport explicatif, « la personne concernée doit avoir la possibilité de prouver l'inexactitude éventuelle des données à caractère personnel avant leur utilisation, l'inadéquation du profil qu'il est prévu d'appliquer à sa situation particulière ou d'autres facteurs qui auront un impact sur le résultat de la décision automatisée[94] ».

La prise de décision automatisée grâce à l'apprentissage automatique profond, à l'intelligence artificielle[95] et au traitement algorithmique secret peut être une cause de stigmatisation et de discrimination. La Convention prévoit qu'une telle prise de décision ne peut avoir lieu que si les droits de la personne concernée sont pris en compte. La formulation du paragraphe 1 de l'article 22 du RGPD apparaît plus ferme à cet égard : « [l]a personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. » Les domaines typiques de discrimination mentionnées dans ce contexte sont l'octroi de crédits ou de prestations sociales.

Il est presque impossible de distinguer les questions relatives au traitement automatisé de celles qui concernent le profilage automatisé, défini comme suit : « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ». Selon un rapport récent sur le profilage et la Convention 108 +, le profilage peut être « à risque élevé » lorsqu'il a un impact significatif sur la personne ou le groupe de personnes, lorsqu'il présente un risque de manipulation, lorsqu'il vise des catégories particulières de données ou lorsqu'il est effectué par des services d'information en grande partie en ligne[96]. Dans le contexte électoral, certains craignent que le profilage électoral n'ait un « effet dissuasif » sur la liberté d'expression et de participation. Il est en effet largement reconnu que le sentiment d'être sous surveillance peut entraver l'exercice des libertés fondamentales, y compris la participation aux élections[97]. Le CEPD a déjà statué sur ce point :

---

[92] Bennett and Oduro Marfo, p. 57.
[93] Convention 108+, article 9.1.
[94] Rapport explicatif, p. 14-15.
[95] *Lignes directrices sur l'intelligence artificielle et la protection des données*, adoptées le 25 janvier 2019 par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Voir : https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8
[96] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. *Profilage et la Convention 108+ : Pistes pour une actualisation de la Recommandation 2010(13) sur le profilage*. Strasbourg, 7 novembre 2019.
[97] Rapport conjoint de la Commission de Venise, juin 2019, p. 20.

"La prise de décision uniquement automatisée, y compris le profilage, lorsque la décision affecte légalement ou de manière similaire et significative l'individu qui en fait l'objet, est limitée. Le profilage lié à des messages de campagne ciblés peut, dans certaines circonstances, entraîner des "effets significatifs similaires" et n'est en principe licite qu'avec le consentement explicite et valable de la personne concernée".[98]

Cela dit, le profilage des électeurs peut prendre différentes formes et il est souvent invisible pour les personnes[99]. Très simplement, de nombreux partis politiques ont adopté des systèmes de notation personnalisés très élémentaires pour prédire le soutien ou l'opposition probable d'un électeur[100]. Ces systèmes de classement permettent aux partis de concentrer leurs efforts sur les électeurs les plus susceptibles de les soutenir et d'améliorer la capacité d'un parti à recruter de nouveaux bénévoles et donateurs. Les tentatives visant à rendre ces systèmes de notation transparents ont rencontré une résistance dans certains pays au prétexte que révéler qu'un parti utilise un système de notation et de profilage exclusif porterait atteinte à sa position concurrentielle[101].

Un profilage plus perfectionné des électeurs est effectué sur Facebook grâce à la création d'un public de « semblables ». L'enquête de l'ICO 2017-2018 sur les partis politiques britanniques a montré que les partis comprenaient souvent mal la base juridique du téléchargement des coordonnées de contact sur les plateformes de réseaux sociaux, notamment les fonctions *Core, Custom et Look-Alike Audiences* de Facebook. Selon des enquêtes menées au Canada, la raison pour laquelle des adresses électroniques de sympathisants sont transmises à des fins d'analyse et de profilage des données pour atteindre de publics similaires grâce à l'outil « Lookalike » de Facebook est complètement différent du motif initial déclaré ou invoqué par les partis pour les collecter[102].

Un rapport récent sur le profilage et la Convention 108 + montre que l'application des principes du traitement équitable et proportionné est délicat car le profilage repose sur des catégories de données difficiles à prévoir avant leur traitement. Il recommande que le profilage soit limité aux catégories de données que la personne concernée peut raisonnablement s'attendre (légitimement s'attendre) à ce qu'elles soient prises en considération au vu des finalités légitimes[103]. Le profilage doit contribuer « au bien-être des individus et au développement d'une société inclusive, démocratique et durable » et ne doit pas entraîner de discrimination à l'égard d'individus, de groupes ou de communautés. Il ne doit « porter atteinte ni à la dignité des personnes, ni à la démocratie[104] ».

Conclusions

[98] Comité européen pour la protection des données*, Déclaration 2/2019 sur l'utilisation des données personnelles dans le cadre des campagnes politiques.* 13 mars 2019, disponible à : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

[99] ICO, Guidance on Political Campaigning, p. 65.

[100] C.J. Bennett (2015). "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications", *Surveillance and Society*, vol. 13, no 3-4 http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/voter_surv

[101] Cet argument a été rejeté par le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, *Full Disclosure*, p. 37.

[102] Ibid. 26.

[103] *Profilage et la Convention 108+ : Pistes pour une actualisation de la Recommandation 2010(13) sur le profilage,* 7 novembre 2019, p. 5.

[104] Ibid, p. 4.

Le traitement de données à caractère personnel illégal ou contraire à l'éthique dans les campagnes politiques soulève des questions fondamentales sur les pratiques démocratiques, la qualité du débat démocratique, l'ouverture de la concurrence démocratique et la nature de la participation politique. Les pratiques sont très variées et se développent rapidement et de manière organique au fur et à mesure que les différents acteurs et organisations politiques évaluent les avantages des campagnes numériques en fonction de leurs ressources, de leur cadre juridique, de leur environnement institutionnel et de leur culture politique.

Compte tenu de la complexité et de la dynamique de cet écosystème, comment la Convention 108+ peut-elle contribuer au règlement de ces questions de participation démocratique au sens large ? Comment peut-elle être appliquée aux campagnes politiques et aux organisations chargées des campagne sans compromettre le droit des acteurs politiques de communiquer avec l'électorat et de le mobiliser à aller voter ?

La présente analyse débouche sur les conclusions qui suivent.

- La Convention 108+ a été explicitement créée comme un instrument de portée mondiale. Elle est formulée selon des principes généraux qui lui permettent d'être appliquée dans différentes parties du monde et dans divers systèmes politiques. Elle a été élaborée en vue de produire un impact à l'échelon international et constitue un processus plutôt fondé sur le respect d'un traité que sur les forces du marché[105]. C'est la seule perspective réaliste d'un accord mondial sur la protection des données[106].

- La Convention 108+ est formulée explicitement sous l'angle des droits de l'homme et de la démocratie et non dans une optique commerciale. Ses racines, ancrées dans les droits de l'homme et la démocratie en font un instrument international plus adapté à l'harmonisation des pratiques dans le domaine électoral.

- Le Conseil de l'Europe a joué un rôle historique dans la promotion des pratiques et des droits démocratiques grâce à l'action de la Commission de Venise et d'autres organes. Les questions relatives à la manipulation électorale, à la propagande et à la désinformation sont indissociables de celles qui traitent de la protection des données. Le Conseil de l'Europe est parfaitement placé pour comprendre ces relations et comment le traitement légal et éthique des données à caractère personnel peut améliorer l'intégrité de la démocratie et le fonctionnement des institutions démocratiques.

- Le Conseil de l'Europe a, de façon impressionnante, déjà démontré sa capacité à identifier les enjeux technologiques et à élaborer des solutions réglementaires clairement définies. À une époque où les pratiques de campagne numérique progressent rapidement au niveau mondial, il est parfaitement adapté pour s'attaquer à ces problèmes. La modernisation de la Convention 108 visait à relever les nouveaux défis posés par les technologies contemporaines et ses principes sont particulièrement appropriés face à la manipulation en ligne et à l'utilisation abusive de données dans le cadre des campagnes politiques. Les questions abordées dans le présent document sont également étroitement liées aux recommandations antérieures sur les médias numériques et sociaux.

[105] L. Bygrave. 2020. "The Strasbourg Effect in Data Protection: Its Logic, Mechanics and Prospects in Light of the 'Brussels Effect'. Voir : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3617871
[106] G. Greenleaf. 2018. Convention 108+ et Cadre de protection des données de l'UE. Voir : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606

- Le Conseil de l'Europe a également une vaste expérience dans les secteurs réglementaires et politiques connexes. Une large diversité de règles constitutionnelles, statutaires et d'autorégulation peuvent encadrer le traitement des données à caractère personnel dans les campagnes électorales. Le Conseil de l'Europe fournit de longue date des orientations et des services de coordination aux différents régulateurs nationaux intervenant dans différents secteurs. La Convention 108+ constitue un ensemble précieux de normes fondées sur des principes permettant de comprendre les diverses règles en vigueur dans les pays et de les intégrer.

- Au-delà des autorités chargées de la protection des données, les organismes de régulation des élections et des télécommunications ont des responsabilités statutaires en matière de financement, de publicité et d'administration des élections dans de nombreux pays. La Convention 108+ peut offrir un cadre précieux à la coordination des travaux des différents organismes de réglementation, aux niveaux national et international.

- Les « intérêts légitimes » des organisations chargées des campagnes et des organisations politiques sont différents de ceux des organismes publics et des entreprises. Ici, l'intérêt public exige de concilier la participation démocratique avec le droit à la vie privée des électeurs. Le Conseil de l'Europe est particulièrement bien placé pour aborder les conséquences de l'utilisation des données à des fins électorales sur la vie privée dans ce contexte élargi, et pour comprendre la relation qui existe entre la protection de la vie privée et la promotion des pratiques démocratiques.

- Les « opinions politiques » sont définies comme des formes de données sensibles dans la Convention 108+. Cette classification est motivée par des préoccupations historiques concernant la suppression du droit de vote et la manipulation des électeurs. Toute orientation ou recommandation visant la protection de la vie privée et les campagnes électorales doit tenir compte des différentes pratiques de campagne concernant la relation candidat-électeur. Dans les pays avec une histoire récente de régime autoritaire, la sensibilité des données sur l'affiliation politique est particulièrement élevée. Le Conseil de l'Europe possède une expérience précieuse dans la promotion des pratiques démocratiques dans les États aux démocraties établie comme dans les démocraties plus récentes et plus fragiles.

- Les campagnes politiques contemporaines sont complexes, opaques et mettent en jeu un écosystème changeant d'acteurs et d'organisations qui peut varier considérablement d'une société à l'autre. L' « industrie de l'influence » politique opère dans les cultures en se souciant peu ou pas du tout des traditions de campagne, des réalités institutionnelles ou des pratiques politiques. La Convention 108 peut servir de norme de référence pour le traitement des données à caractère personnel dans le cadre de différentes élections démocratiques et pour l'amélioration des pratiques utilisées par les divers responsables du traitement et sous-traitants dans les réseaux mondiaux de lancement de campagnes. Elle peut également servir de base à des codes de bonne pratique analogues à ceux qui sont en cours d'élaboration au Royaume-Uni.

- Ces questions ont manifestement une portée mondiale qui exigent le plus haut niveau de collaboration internationale entre autorités chargées de la protection des données, en Europe et au-delà. L'impact national et international de cette collaboration demandera aux autorités, par le biais de leurs associations régionales et internationales, ainsi qu'au réseau des défenseurs et des experts internationaux de la protection de la vie privée au sens large, une attention et une vigilance des plus constantes aux évolutions

transnationales. La Convention 108 + est un instrument précieux dont les principes peuvent servir de base à cette coordination.