Le Règlement Général sur la Protection des Données

Les campagnes électorales dans le respect de la protection des données personnelles

Première publication : 2 octobre 2019

Mise à jour : 8 février 2023

Table des matières

1. Introduction

À travers les présentes lignes directrices, la Commission nationale pour la protection des données (ci-après la « CNPD ») souhaite sensibiliser les acteurs politiques sur les risques liés en particulier à la collecte et au traitement des données à caractère personnel des électeurs à des fins électorales[1]. La CNPD entend également émettre des recommandations et exposer les bonnes pratiques en matière de campagnes électorales numériques dans le respect de la protection des données personnelles.

Les traitements de données à caractère personnel effectués dans le contexte des campagnes électorales doivent bien entendu respecter le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ci-après le « RGPD »).

Des élections libres et équitables dans le respect des droits des citoyens sont essentielles à l'expression d'une démocratie saine. Pour une démocratie vivante, les échanges d'idées et la communication des opinions et positions politiques sont cruciaux. L'internet permet un accès facilité aux informations et les plateformes numériques permettent de nouvelles formes d'engagement et d'interaction. Avec l'émergence de ces nouveaux espaces d'échange et de débat, les campagnes électorales évoluent et la communication politique se déplace davantage dans l'espace numérique. Dans cette optique, pour compléter les vecteurs de communication plus classiques, les partis et candidats politiques utilisent différents canaux de communication électronique à l'attention des électeurs durant les campagnes électorales.

Pour que ces échanges permettent aux citoyens d'user pleinement de leurs droits fondamentaux comme la liberté d'expression, la protection de leur vie privée et la liberté de choix, ils doivent se dérouler dans un cadre légal, loyal et transparent. Ces garanties sont un gage pour que les échanges et les communications dans le contexte électoral continuent à être bénéfiques au processus démocratique.

Les révélations de Cambridge Analytica et les controverses autour des phénomènes de la désinformation et de la manipulation[2] ont montré que l'utilisation de ces outils et des nouveaux espaces de dialogue comporte également des risques, en particulier par l'utilisation de données à caractère personnel. En effet, dans l'affaire Cambridge Analytica, le non-respect de la protection des données personnelles a rendu possible des manipulations d'opinions qui ont mis en péril les processus démocratiques visés. De plus, dans ce contexte, les phénomènes de fausses nouvelles et de désinformation peuvent entacher la sincérité des débats en exposant les électeurs à de la manipulation.

1.1. Le contexte européen et international

Au niveau européen, plusieurs actions ont été entreprises depuis les révélations de Cambridge Analytica pour garantir la tenue d'élections européennes libres et équitables. Depuis septembre 2018, la Commission européenne et les Etats membres ont mis en œuvre plusieurs mesures visant à protéger les droits démocratiques des citoyens et leur liberté d'expression, y compris des mesures concernant la cybersécurité, la lutte contre la

[1] Pour des informations générales, voir par exemple le guide pratique pour le monde associatif : https://cnpd.public.lu/fr/dossiers-thematiques/guide-monde-associatif.html

[2] Voir à cet égard, Contrôleur européen de la protection des données, Avis n°3/2018 du 19 mars 2018 sur la manipulation en ligne et les données à caractère personnel

désinformation et contre les contenus haineux[3]. Ces mesures promeuvent la transparence et contiennent des recommandations et mesures concrètes concernant la protection des données. Le Comité Européen de la Protection des Données (en anglais European Data Protection Board, « EDPB ») et le Contrôleur européen de la protection des données (en anglais European Data Protection Supervisor, « EDPS ») ont également publié des guidances pour les acteurs impliqués[4].

Par la suite, les plateformes en ligne et le secteur de la publicité se sont engagés à respecter un code de bonnes pratiques en matière de désinformation, publié en 2022[5]. En collaboration avec le groupe des régulateurs européens des services de médias audiovisuels (« ERGA ») et l'Observatoire européen des médias numériques (« EDMO »), la Commission européenne évaluera régulièrement les progrès réalisés dans la mise en œuvre du code et adaptera, au besoin, les engagements au regard de l'évolution technologique, sociétale, du marché et de la législation[6].

1.2. Les risques associés à l'utilisation des nouvelles technologies dans les campagnes électorales

Avec l'avènement de nouvelles technologies de ciblage, les partis politiques se sont mis également à utiliser ces outils pour atteindre les électeurs avec des messages très personnalisés – en particulier sur les plateformes de médias sociaux – sur la base d'intérêts personnels, d'habitudes de vie et de valeurs. Les campagnes électorales luxembourgeoises ne sont pas à l'abri de ces développements, et les différents acteurs politiques, autorités et régulateurs doivent les prendre en compte afin de garantir des élections libres et équitables.

L'utilisation pour le ciblage des personnes à des fins de prospection politique, de l'intelligence artificielle et du « Big Data » en combinaison avec des données personnelles rend l'information opaque. En effet, les techniques actuelles, comme les outils prédictifs, permettent de formuler des hypothèses sur les opinions politiques et autres catégories particulières de données. À cet effet, ces outils déduisent des traits de personnalité profonde sur la base de caractéristiques relatives à l'humeur et d'autres informations sensibles des personnes concernées. Or, la transparence sur les traitements de données est l'un des garants des droits et libertés des citoyens, ce qui signifie dans ce contexte que les personnes ont le droit de savoir pourquoi elles ont étés ciblées et par qui.

De même, les techniques avancées de profilage rendent possible l'enfermement de personnes ciblées dans des bulles numériques polarisées sur des évènements spécifiques. Ceci va à l'encontre de la liberté de choix et de penser et constitue une entrave à l'exercice de liberté d'expression des citoyens. Il est donc important de savoir qui est l'auteur d'un message pour pouvoir librement faire ses choix politiques en toute connaissance de cause.

---

[3] Voir notamment les dossiers de presse de la Commission européenne disponibles sous : https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_6118, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/democracy-and-electoral-rights_fr et https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (liens vérifiés le 28 septembre 2022).

[4] Comité européen de la protection des données (EDPB), Déclaration 2/2019 du 13 mars 2019 sur l'utilisation des données à caractère personnel dans le cadre de campagnes politiques ; Comité européen de la protection des données (EDPB), Lignes directrices 8/2020 du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux ; Contrôleur européen de la protection des données, Avis n°3/2018 du 19 mars 2018 sur la manipulation en ligne et les données à caractère personnel.

[5] Voir notamment le dossier de presse sur le site de la Commission européenne: http://europa.eu/rapid/press-release_IP-18-6647_fr.htm (lien vérifié le 28 septembre 2022).

[6] Commission européenne, Communiqué de presse du 16 juin 2022 « Désinformation: la Commission se félicite du nouveau code de bonnes pratiques contre la désinformation, plus fort et plus complet », disponible sous : https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_3664 (lien vérifié le 28 septembre 2022).

Ainsi, l'extension de ces techniques de traitement de données personnelles à des fins politiques fait peser des risques graves, non seulement sur les droits à la vie privée et la protection des données, mais aussi sur la confiance dans l'intégrité du processus démocratique. Dans ce contexte, il convient de rappeler qu'une donnée personnelle garde son caractère personnel même si elle a été rendue publique, par exemple, sur un réseau social. De plus, une opinion politique est une donnée sensible sous le RGPD et est donc sujette à des règles d'utilisation plus strictes.

Par conséquent, les partis politiques doivent prendre conscience des risques inhérents à l'utilisation d'outils comme le profilage et le micro-ciblage à des fins de prospection politique et de leur responsabilité en matière de protection des données à caractère personnel. Il est à noter que cette responsabilité est partagée entre le demandeur et le diffuseur.

2. Quelques notions-clés

2.1. Un bref aperçu des obligations en matière de protection des données

La législation en matière de protection des données s'applique à tout traitement de données à caractère personnel quel que soit l'identité du responsable du traitement. A cet égard, il importe peu que ce dernier soit un parti politique reconnu en tant que tel, une association, un groupement de personnes physiques ou une personne physique. Par conséquent, si un candidat individuel traite des données en vue de leur utilisation à des fins de prospection électorale, les présentes lignes directrices s'appliquent. Ce candidat ne peut en principe pas invoquer l'exception des « *activités domestiques et personnelles* » lorsqu'il traite des données personnelles pour le bénéfice de sa campagne électorale. En effet, même si le RGPD ne s'applique pas aux traitements de données effectués « *dans le cadre d'une activité strictement personnelle ou domestique* », cette exception doit être interprétée de manière restrictive selon la jurisprudence de la Cour de justice de l'Union européenne. Dès lors que le traitement de données effectués par un candidat dépasse son cercle familial et ses proches, le traitement est soumis au RGPD.

En application de l'article 5 du RGPD, les responsables du traitement doivent impérativement observer les principes découlant du RGPD pour tous leurs traitements de données.

Le principe de licéité[7] impose aux responsables du traitement de choisir la base juridique appropriée au traitement (aussi pour les données déduites (« inferred data »)[8]). Lorsque le traitement de données englobe des données dites « sensibles », comme des données révélant des opinions politiques, les responsables du traitement doivent non seulement respecter les prescriptions de l'article 6 du RGPD, mais également les conditions spécifiques imposées par l'article 9 du RGPD encadrant les traitements de catégories particulières de données[9].

Le principe de limitation des finalités[10] exige que les responsables du traitement identifient une finalité licite pour chaque traitement. Réutiliser des données pour un traitement ultérieur est uniquement possible si la finalité de cette réutilisation est compatible avec la finalité initiale de la collecte des données.

[7] Articles 5, paragraphe 1er, lettre a), et 6 du RGPD.
[8] Voir ci-après, notamment points 4. et 5.2.
[9] Voir ci-après, point 2.2.
[10] Article 5, paragraphe 1er, lettre b), du RGPD.

Le principe de transparence[11] requiert que les personnes concernées doivent recevoir certaines informations concernant le ou les traitements entrepris, quel que soit la source des données collectées par le responsable du traitement[12].

Exemple

Un syndicat ou un groupement d'intérêts de citoyens pourrait être amené à solliciter de ses contacts le consentement à transmettre leurs données de contact à un parti politique afin que celui-ci puisse leur adresser des communications en matière de prospection politique dans le contexte d'une campagne électorale. Le parti politique en tant que responsable du traitement reçoit ainsi des données de tiers et doit vérifier si les données reçues ont été obtenues de manière licite. De plus, le parti politique doit veiller à ce que la finalité initiale utilisée pour légitimer la collecte soit compatible avec les finalités poursuivies et doit s'assurer que, si la collecte initiale a été légitimée par le consentement, les personnes concernées ont donné leur consentement éclairé également pour la finalité ultérieure[13]. Finalement, le parti politique doit encore informer les personnes concernées de la collecte de ces données, au plus tard à la première prise de contact.

En vertu des principes de minimisation des données[14] et d'exactitude[15], les responsables du traitement ne doivent collecter et traiter que les données nécessaires au regard des finalités pour lesquelles elles sont traitées et doivent garantir l'exactitude des données, en particulier pour les données provenant de sources différentes et les données déduites. Par ailleurs, le principe de la limitation de la conservation exige que les responsables du traitement suppriment les données lorsqu'elles ne sont plus nécessaires à la finalité initiale pour laquelle elles ont été collectées[16].

En vertu du principe d'intégrité et de confidentialité des données[17], les responsables du traitement doivent prévoir des mesures de sécurité adéquates, c'est-à-dire s'assurer des mesures techniques et organisationnelles appropriées[18]. Parmi ces mesures techniques, il convient par exemple de sécuriser les listes utilisées pour la prospection électorale et de les conserver sur des supports suffisamment protégés contre des tentatives d'intrusion.

Concrètement, il est recommandé de chiffrer les ordinateurs et supports qui contiennent des données personnelles ou confidentielles. De plus, il convient d'avoir des systèmes informatiques à jour, de se protéger des intrusions via des suites logicielles ad-hoc ou des équipements dédiés (pare-feux). Autant que possible l'authentification à double facteur doit être utilisée si disponible et les mots de passe doivent être complexes. Concernant l'utilisation de listes de diffusion par courriel, il est recommandé d'utiliser le champ « CCI » afin de garantir la confidentialité des adresses e-mail des destinataires. Les fichiers de prospection devraient être cloisonnés lorsque les conditions relatives à leurs traitements diffèrent, c'est-à-dire qu'il y a par exemple différentes sources, conditions de licéité ou durées de conservation.

[11] Articles 5, paragraphe 1er, lettre a), 12, 13 et 14 du RGPD.
[12] Groupe de travail « article 29 », Lignes directrices du 11 avril 2018 sur la transparence au sens du règlement (UE) 2016/679 (WP260rev.01), approuvées par le Comité européen de la protection des données.
[13] Article 6, paragraphe 4, du RGPD.
[14] Article 5, paragraphe 1er, lettre c) du RGPD.
[15] Article 5, paragraphe 1er, lettre d), du RGPD.
[16] Article 5, paragraphe 1er, lettre e), du RGPD.
[17] Articles 5, paragraphe 1er, lettre f), 25 et 32 du RGPD.
[18] Voir, pour plus d'informations, le dossier thématique de la CNPD sur la sécurité informatique, disponible sous : https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/securite-informatique.html

Parmi les mesures à prendre, les responsables du traitement doivent encore établir clairement qui a accès aux données[19]. Par exemple, les partis politiques doivent veiller à ce que seules les personnes au sein d'un parti politique qui ont besoin pour l'exécution de tâches particulières aient accès aux données personnelles en cause. Ils devraient également sensibiliser les personnes susceptibles d'exécuter les opérations de traitement.

En prévision d'une violation de données personnelles (telle que définie par l'article 4, point 12°, du RGPD, (attaques par des hackers, perte de la liste des membres, perte d'un ordinateur portable ou d'un stick USB), les responsables du traitement devraient prévoir des procédures de réaction rapide et de mitigation des conséquences sur les droits des personnes concernées et de notification à la CNPD et d'information aux personnes concernées[20].

Par ailleurs, les responsables du traitement doivent veiller au respect des droits des personnes concernées, à savoir le droit à l'information, le droit d'accès, le droit à l'oubli, le droit d'opposition et le droit de formuler une réclamation auprès de la CNPD[21]. Par exemple, lorsque les responsables du traitement envisagent de recourir au profilage, ils doivent prendre en compte les risques caractérisant ces techniques, adopter des garanties appropriées et se conformer aux conditions spécifiques encadrant ces moyens de traitement de données[22]. Selon le traitement envisagé, il peut être nécessaire d'effectuer en amont une analyse d'impact relative à la protection des données[23].

De plus, les responsables du traitement doivent recourir uniquement à des sous-traitants présentant des garanties suffisantes et démontrant des connaissances spécialisées, une fiabilité et des ressources appropriées[24] et doivent conclure des contrats avec eux clarifiant leurs obligations respectives.

Le principe de responsabilité (« accountability ») signifie que les responsables du traitement doivent être en mesure de démontrer leur conformité à tout moment[25]. Cela implique par exemple d'établir une documentation adéquate relative aux traitements de données effectués, y compris un registre de traitement des données, la documentation relative aux procédures mises en place, les contrats avec les sous-traitants et un registre interne des incidents et violations en matière de protection des données.

2.2. Les opinions politiques, une catégorie particulière de données

Les données à caractère personnel qui révèlent des opinions politiques constituent une catégorie particulière de données au titre du RGPD et leur traitement est strictement encadré par l'article 9.

Les finalités de l'utilisation des données à caractère personnel et l'identité du responsable du traitement peuvent entrer en ligne de compte quand il s'agit de déterminer si des données révèlent des opinions politiques. Par exemple, alors qu'une liste de clients d'une entreprise ou une liste de membres d'une association sportive ne révèle en principe pas les opinions

[19] Egalement en application des principes de la protection des données dès la conception et par défaut, définis à l'article 25 du RGPD, ainsi qu'aux obligations liées à la mise en place d'un niveau de sécurité adapté au risque, définies à l'article 32 du RGPD.
[20] Articles 33 et 34 du RGPD.
[21] Articles 12 à 22 du RGPD.
[22] Article 22 du RGPD.
[23] Articles 35 et 36 du RGPD.
[24] Article 28 du RGPD.
[25] Article 5, paragraphe 2, du RGPD.

politiques des personnes concernées, une liste de membres ou de sympathisants d'un parti politique révèle bien des opinions réelles ou supposées des personnes concernées.

Il est également important de noter que des *« opération[s] intellectuelle[s] de déduction ou de recoupement »* ou encore des techniques de profilage peuvent produire, via une combinaison de données *a priori* en dehors du champ de l'article 9 du RGPD, des données déduites pouvant révéler des opinions politiques au sens de cet article[26].

Dès que des données sont combinées, par exemple à des données statistiques ou démographiques, à des fins d'élaboration d'un profil d'électeur, l'article 9 du RGPD a vocation à s'appliquer. Si un responsable du traitement utilise les données observées pour catégoriser la personne concernée comme ayant certaines opinions politiques, que la catégorisation soit correcte ou non, cette catégorisation doit manifestement être considérée comme un traitement de données sensibles[27].Comme développé plus loin, cela signifie qu'il est en principe interdit de constituer un tel profil, à moins de remplir les conditions de l'article 9, paragraphe 2, du RGPD[28].

3. La provenance des données

3.1. Les listes de membres et de sympathisants

La principale source de données des partis politiques et des candidats constitue les listes de membres ou sympathisants établies au fil du temps lors de leurs activités.

L'article 9 du RGPD permet à « *une fondation, une association ou un autre organisme à but non lucratif et poursuivant une finalité politique* » de traiter ces données « *dans le cadre des activités légitimes* », « *à condition que le traitement porte exclusivement sur les membres ou les anciens membres […] ou sur des personnes entretenant avec lui des contacts réguliers* »[29] (au sujet du traitement de données de membres et de sympathisants, voir également ci-après, point 4.2.).

3.2. Les restrictions à la réutilisation des listes électorales

Dans le passé, les listes des électeurs constituaient une source de données à laquelle les partis politiques et les candidats pouvaient en principe avoir recours à des fins de prospection politique. Les données contenues dans ces listes comprennent le nom, les prénoms, le domicile, le lieu et la date de naissance des électeurs, et le cas échéant, la nationalité et le nom et prénoms du conjoint[30] (article 13 et 14 de la loi électorale).

En effet, avant la modification de loi électorale en 2022, l'article 20, alinéa 3, de la loi électorale du 18 février 2003 prévoyait que « *tout citoyen peut […] demander par écrit une copie des listes [électorales] actualisées […]. Les données des citoyens contenues dans les listes ne peuvent pas être utilisées à des fins autres qu'électorales* ».

---

[26] CJUE, arrêt du 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, ECLI:EU:C:2022:601. Voir aussi les lignes directrices 8/2020 du Comité Européen de la Protection des Données (EDPB) du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux et les lignes directrices du groupe de travail « article 29 » du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 (WP251rev0.1), approuvées par le Comité européen de la protection des données, pages 16-17

[27] Voir les lignes directrices 8/2020 du Comité Européen de la Protection des Données (EDPB) du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux, points 123 et 125.

[28] Voir ci-après, points 4 et 5.2.

[29] Voir plus loin, concernant les conditions de licéité.

[30] Article 13 et 14 de la loi électorale.

Cette disposition permettait avant tout aux partis politiques[31] d'utiliser ces listes électorales *« à des fins électorales »*, plus précisément pour la prospection politique, mais seulement pendant les périodes électorales.

Depuis 2022, l'alinéa 3 de l'article 20 de la loi électorale prévoit que « *tout citoyen peut prendre inspection des listes actualisées ainsi que des pièces mentionnées ci-dessus au secrétariat de la commune jusque et y compris le trentième jour avant le jour des élections* ». Ainsi, la disposition telle que modifiée ne permet plus d'obtenir une copie des listes électorales et par conséquent les listes ne peuvent plus être utilisées pour des finalités de prospection politique par les partis politiques. Au sujet de cette modification, la commission parlementaire explique dans son rapport que *« eu égard aux règles applicables en matière de protection des données à caractère général et à la tendance générale qui va de plus en plus vers un renforcement de la protection des données à caractère personnel, le maintien du droit au profit de tout citoyen de demander une copie intégrale des listes électorales n'est plus approprié de nos jours »*. Ledit rapport précise que le maintien du *« droit pour le citoyen de prendre inspection de la liste électorale au secrétariat de la commune […] satisfait à lui seul déjà à la finalité électorale poursuivie »*[32].

Accueillant favorablement cette modification, la CNPD précise dans son avis du 1er juillet 2022 au sujet de ladite modification et de la définition de la finalité électorale que

> *« La finalité de la tenue des listes électorales consiste notamment en la constatation de la qualité d'électeur des personnes physiques remplissant les conditions prévues par la loi électorale modifiée du 18 février 2003. La Commission nationale estime que le droit de prendre inspection des listes électorales rentre dans le cadre de cette finalité, notamment aux fins de vérifier l'exactitude des listes électorales, sans qu'il soit forcément nécessaire de prévoir, en plus, un droit d'en prendre copie. En supprimant la possibilité de demander une copie des listes électorales, le risque d'un traitement ultérieur incompatible avec la finalité électorale est réduit. »*[33]

Par conséquent, dès lors que les partis politiques ne peuvent pas obtenir copie des listes électorales et que l'article modifié restreint les finalités *« aux fins de vérifier l'exactitude des listes électorales »*, notamment par *« la constatation de la qualité d'électeur des personnes physiques »*, les partis politiques ne peuvent plus utiliser les données obtenues dans le cadre de la consultation des listes à des fins de prospection politique[34].

3.3. Les restrictions à la réutilisation de listes obtenues dans d'autres contextes

Si les candidats et leurs partis politiques ont bien évidemment un souci légitime d'approcher les électeurs et de leur exposer leurs programmes dans le cadre de leur campagne électorale, il convient de rappeler qu'ils ne doivent pas utiliser à cette fin des fichiers qu'ils se seraient procurés en dehors de toute base légale ou réglementaire auprès d'organismes privés ou d'institutions publiques ou qu'ils auraient collectés pour des finalités différentes.

---

[31] Cette possibilité, réservée principalement aux partis politiques, reflétait le rôle particulier que l'article 32bis de la Constitution réserve aux partis politiques dans le contexte électoral, en reconnaissant qu'ils *« concourent à la formation de la volonté populaire et à l'expression du suffrage universel »*.

[32] Projet de loi n° 7877, Rapport de la Commission des Institutions et de la Révision constitutionnelle, Doc. Parl. 7877/17, page 17.

[33] Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7877 portant modification : 1° de la loi électorale modifiée du 18 février 2003 ; 2° de la loi modifiée du 27 juillet 1991 sur les médias électroniques. Délibération n°28/AV12/2022 de la CNPD du 1er juillet 2022.

[34] Conformément au principe de la limitation des finalités au sens de l'article 5, paragraphe 1er, lettre b), du RGPD.

En effet, les partis politiques ou candidats pourraient être tentés d'utiliser des sources de données personnelles issues des activités d'institutions ou d'associations dans lesquelles ils sont actifs. Toutefois, le traitement ultérieur de données à caractère personnel pour d'autres finalités que celle(s) pour laquelle (lesquelles) ces données ont été collectées initialement n'est autorisé que si ce traitement ultérieur est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement, compte tenu du lien entre les finalités pour lesquelles elles ont été collectées et les finalités du traitement ultérieur envisagé.

Dès lors, dans la majorité des cas, la réutilisation de données à caractère personnel recueillies dans un autre contexte (fichier du personnel d'une administration ou d'une entreprise, données obtenues dans le cadre de l'exercice d'un mandat public, fichier clients d'une entreprise, liste des membres d'une association ou d'un syndicat, ...) n'est pas permise. Notamment, les associations à but non lucratif ne doivent communiquer la liste de leurs membres à des tiers sans le consentement de leurs membres. Outre le probable non-respect du principe de limitation des finalités, une telle réutilisation risque de rompre l'égalité entre les candidats.

3.4. Les limitations concernant l'utilisation de sources publiques

La collecte indirecte, sur la base de sources publiques, comme par exemple des informations publiées sur un annuaire en ligne, un site internet ou un réseau social à des fins électorales est en principe incompatible avec le principe de limitation des finalités.

Lorsqu'un parti politique ou un candidat entend recourir à un prestataire de services pour ses activités de promotion politique, celui-ci pourra utiliser des données personnelles collectées initialement pour des activités de marketing, pour autant que les personnes concernées ont exprimé un consentement libre et éclairé relatif à l'utilisation de leurs données personnelles à des fins de communication politique. Les acteurs actifs dans les campagnes électorales doivent par conséquent être particulièrement vigilants en recourant à des sous-traitants comme des revendeurs de données (« data brokers ») et des sociétés d'analyse de données (« data analytics companies »).

En ce qui concerne l'utilisation de données figurant sur les réseaux sociaux, l'EDPB a publié des lignes directrices sur le ciblage des utilisateurs de médias sociaux[35].

4. Les bases de licéité permettant l'utilisation des données personnelles

Tout traitement de données à caractère personnel doit être fondé sur une condition de licéité prévue à l'article 6 du RGPD, y compris les traitements portant sur des catégories particulières de données à caractère personnel (données dites « sensibles ») au sens de l'article 9 du RGPD. L'article 9, paragraphe 1er, du RGPD interdit le traitement des données qui « *révèle[nt] […] les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale* » sauf si l'une des conditions de l'article 9, paragraphe 2, est remplie.

Dans le contexte d'une campagne électorale, une grande partie de traitements de données concerne vraisemblablement des données dites « sensibles », et les responsables du traitement sont dès lors amenés à fonder ces traitements sur les conditions de licéité

[35] Comité européen de la protection des données (EDPB), Lignes directrices 8/2020 du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux. Voir aussi, points 4.3. et 5.2.1. des présentes lignes directrices.

combinées de l'article 6 et de l'article 9 du RGPD telles que exposées ci-dessous. En effet, tout traitement doit d'abord être légitimé par l'un des critères de l'article 6 du RGPD. Lorsque le traitement touche à une catégorie particulière de données (données dites « sensibles »), ce traitement doit en plus respecter les prescriptions spécifiques définies à l'article 9 du RGPD.

4.1. Le consentement explicite de la personne concernée

Sur la base des articles 6, paragraphe 1er, lettre a), et 9, paragraphe 2, lettre a), du RGPD, les responsables du traitement peuvent baser leurs traitements sur le consentement explicite des personnes concernées[36]. Pour être conforme aux exigences du RGPD[37], le consentement doit être « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »[38]. L'exigence que le consentement soit explicite implique que la personne concernée doit formuler une déclaration de consentement exprès par un acte positif[39]. Afin de garantir que le consentement soit fourni de façon libre et éclairée, il est primordial d'informer les personnes concernées conformément à l'article 13 ou, le cas échéant, l'article 14 du RGPD.

La personne concernée peut retirer ce consentement à tout moment, et elle doit pouvoir le retirer de manière aisée et compréhensible, avec la même facilité que lorsqu'elle a exprimé son consentement. Le responsable du traitement doit informer la personne concernée de cette possibilité dès le début du traitement et doit permettre un retrait facile du consentement.

Si les responsables du traitement envisagent de traiter des données qui n'ont pas initialement été collectées avec la finalité de la prospection politique, ils doivent veiller à recueillir le consentement des personnes concernées avant ce nouveau traitement conformément à l'article 6, paragraphe 4, du RGPD. Il faut encore veiller à ce que la personne concernée soit informée de telles autres finalités et de ses droits.

Certaines plateformes de réseaux sociaux permettent le déploiement d'applications intégrées dans ces plateformes (du type « jeux », « questionnaires », …). Ces applications peuvent être utilisées pour collecter des données sur leurs utilisateurs et potentiellement pour établir des profils révélant des opinions politiques réelles ou supposées. Dans la plupart des cas, ces profils sont ensuite utilisés pour cibler des messages publicitaires. Le consentement à ce traitement de données doit être donné de façon séparée et de façon explicite. Le consentement fourni lors de l'inscription à la plateforme n'est en principe pas suffisant.

Ainsi, lorsqu'un parti politique ou un candidat envisage l'utilisation d'une telle application, il devient responsable du traitement, et il est impératif de veiller à ce que le consentement ait été exprimé de façon séparée et de façon explicite, même si l'application a été développée et déployée par un sous-traitant.

[36] Concernant les conditions relatives au consentement et au consentement explicite, voir notamment les lignes directrices 5/2020 du le Comité européen de la protection des données du 4 mai 2020 sur le consentement au sens du règlement (UE) 2016/679.
[37] A savoir, aux articles 4, point 11, 6, paragraphe 1er, lettre a), 7 et 9 du RGPD
[38] Article 4, point 11, du RGPD.
[39] Comité européen de la protection des données (EDPB), les lignes directrices 5/2020 du 4 mai 2020 sur le consentement au sens du règlement (UE) 2016/679, section 4.

4.2. Les intérêts légitimes et les données de membres et de sympathisants

Lorsque les partis politiques effectuent des traitements de données, « *dans le cadre de leurs activités légitimes et moyennant les garanties appropriées* » qui « *se rapporte[nt] exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec [sa finalité politique]* », il est envisageable de fonder ce traitement sur les articles 6, paragraphe 1er, lettre f), et 9 paragraphe 2, lettre d), du RGPD.

En invoquant leurs « intérêts légitimes » pour légitimer ces traitements de données, les responsables du traitement doivent s'assurer à ce que les « *intérêts ou les libertés et droits fondamentaux* » des personnes concernées ne prévalent pas sur leurs intérêts légitimes[40]. Un parti politique a ainsi le droit de traiter les données de ses propres (anciens) membres et sympathisants, bien que celles-ci soient révélatrices de leurs opinions politiques.

Or, l'article 9, paragraphe 2, lettre d), in fine du RGPD exige que « *les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées* ». Ainsi, les données relatives aux membres et sympathisants ne peuvent pas être transmises à un tiers sans le consentement explicite de ceux-ci, même s'il existe des affinités politiques entre le parti et le destinataire.

4.3. Les intérêts légitimes des responsables du traitement et les données manifestement rendues publiques par la personne concernée

En combinaison avec l'article 6, paragraphe 1er, lettre f), l'article 9, paragraphe 2, lettre e), du RGPD permet de légitimer le traitement de données portant sur « *des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée* ».

Cette exception concerne principalement les candidats aux différentes élections. En effet, il est inhérent au fait de se présenter à des élections de se faire connaître et d'exprimer publiquement ses opinions politiques.

Toutefois, la simple divulgation d'opinions personnelles sur des réseaux sociaux ou sur d'autres plateformes par des électeurs potentiels ne peut pas, en tant que telle, être considérée comme une donnée « manifestement rendue publique » qu'un acteur politique pourrait traiter. A titre d'illustration, ce n'est pas parce qu'une personne interagit sur un réseau social avec un candidat ou un parti politique (la personne « aime », commente, partage ou « retweete » des contenus publiés sur les réseaux sociaux) que ceux-ci peuvent cibler cette personne avec des messages publicitaires ou autrement utiliser ces données d'interaction.

La personne doit clairement manifester sa volonté d'entretenir des contacts réguliers avec le parti politique ou le candidat, par exemple en devenant « follower » sur Twitter ou « ami » sur Facebook. Toutefois, ce type d'interaction ne permet pas nécessairement de déduire une opinion politique univoque.

---

[40] Les lignes directrices 8/2020 du Comité européen pour la protection des données du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux fournissent d'avantage d'informations quant aux exigences liées à l'article 6, paragraphe 1er, lettre f) du RGPD. Voir aussi l'avis du groupe de travail « article 29 » du 9 avril 2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP217).

S'agissant des réseaux sociaux, l'EDPB considère que les éléments suivants peuvent être pertinents pour évaluer si les données ont été manifestement rendues publiques par la personne concernée[41] :

i. les paramètres par défaut de la plateforme de médias sociaux (afin de savoir si la personne concernée a effectué une action spécifique pour changer ces paramètres de confidentialité par défaut en faveur de paramètres publics) ; ou

ii. la nature de la plateforme de médias sociaux, (afin de savoir si la plateforme est intrinsèquement liée à l'idée de mettre la personne concernée en relation avec des connaissances proches ou de créer des relations intimes (comme c'est le cas des plateformes de rencontre en ligne), ou si elle cherche à offrir un champ plus large de relations interpersonnelles, par exemple des relations professionnelles, ou encore s'il s'agit d'une plateforme de microblogging ou de partage de médias, d'une plateforme sociale pour partager des avis en ligne, etc.) ; ou

iii. l'accessibilité de la page où les données sensibles sont publiées (afin de savoir si les informations sont publiquement accessibles ou si, par exemple, la création d'un compte est nécessaire pour pouvoir accéder aux informations) ; ou

iv. la visibilité de l'avertissement signalant à la personne concernée la nature publique des informations qu'elle publie (afin de savoir si, par exemple, un bandeau continu apparaît sur la page ou si le bouton de validation d'une publication informe la personne concernée que les informations en question seront rendues publiques, etc.) ; ou

v. si la personne concernée a elle-même publié les données sensibles, ou si, à l'inverse, les données ont été publiées par un tiers (ex. une photo publiée par un ami qui révèle des données sensibles) ou sont déduites.

L'EDPB souligne que la présence d'un unique élément ne suffit pas toujours pour établir que les données ont été « manifestement » rendues publiques par la personne concernée. En pratique, il se peut qu'une combinaison de ces éléments ou d'autres éléments doive être prise en compte pour que les responsables du traitement puissent démontrer que la personne concernée a clairement manifesté son intention de rendre les données publiques. Une évaluation au cas par cas est dès lors nécessaire.

Le fait que les données aient été manifestement rendues publiques par les personnes n'exonère pas de justifier en amont d'une base légale (consentement ou intérêt légitime).

Ainsi, lorsqu'une donnée est manifestement rendue publique au sens de l'article 9 du RPGD, par exemple sur un réseau social, notamment parce que la communication est formulée de façon suffisamment explicite (par exemple : « je soutiens ce parti ») et est adressé à une audience qui dépasse largement le cercle privé, le responsable du traitement devra respecter les conditions de licéité prévues par l'article 6 du RGPD.

En invoquant des intérêts légitimes prévus par l'article 6, paragraphe 1er, lettre f), du RGPD, le parti politique devra continuer de les mettre en balance avec les libertés et les droits fondamentaux de la personne concernée. Concrètement, si la personne exprime ses opinions politiques, même de façon « *manifestement publique* », le parti politique ne pourra pas, sans autre élément, communiquer l'identité de cette personne vers l'extérieur (par exemple dans le contexte de ses publicités). La balance des intérêts doit se faire au cas par cas, et pourra prendre en compte le fait que la personne concernée est un personnage public, ou que le traitement prévoit de pseudonymiser la donnée avant sa réutilisation.

[41] Comité européen de la protection des données (EDPB), Lignes directrices 8/2020 du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux, points 127-129.

4.4. L'existence d'une disposition légale poursuivant un intérêt public important

En principe, conformément aux articles 6, paragraphe 1er, lettre c), et 9, paragraphe 2, lettre g), du RGPD, il est possible qu'une disposition légale qui « *constitue une mesure nécessaire et proportionnelle dans une société démocratique notamment pour la garantie de finalités importantes d'intérêt public* » puisse légitimer un traitement de données. Quoi qu'il en soit, il faut veiller à ce que la personne concernée soit informée de telles autres finalités et de ses droits.

Par exemple, en matière de financement des partis politiques, afin de pouvoir bénéficier d'un financement public, les partis politiques doivent déposer « *un relevé de ses donateurs* »[42]. Les noms des personnes physiques[43] doivent dès lors être collectés sur la base d'une obligation légale et doivent également être communiqués aux autorités compétentes.

5. Les différentes modalités de communication

5.1. La prospection par des messages nominatifs directs

La prospection politique par la transmission de messages nominatifs directs s'apparente au marketing direct. Ainsi, les partis politiques et candidats doivent respecter les dispositions particulières en la matière.

5.1.1. L'envoi de courriers postaux

En cas d'envoi de prospection politique par courrier postal, le RGPD confère aux personnes concernées un droit de s'opposer au sens de l'article 21.2 du RGPD (« opt-out ») à tout moment. Ainsi, un parti politique ou un candidat peut envoyer des communications via courrier postal à des électeurs potentiels. Evidemment, les adresses doivent être obtenues de façon légitime. Dans la mise en balance des intérêts légitimes du parti politique avec les intérêts des personnes concernées, il convient de prendre en compte si, au moment de la collecte des données, la personne concernée peut anticiper que ce traitement puisse avoir lieu.

Lorsque les envois sont préparés sur la base de données non collectées directement auprès des personnes concernées, la CNPD rappelle que, au titre de l'obligation d'information découlant de l'article 14 RGPD, les partis politiques doivent fournir, au plus tard au moment de la première communication, c'est-à-dire dans le courrier de prospection ou en annexe, les informations suivantes aux personnes concernées :

- l'identité et les coordonnées du responsable du traitement (le parti politique ou la section locale ou régionale du parti politique),
- l'origine des données traitées (par exemple si les données proviennent d'un organisme liée au parti politique ayant transmis les données sur la base du consentement explicite des personnes concernées),
- la finalité du traitement de données (la prospection politique dans le cadre de l'élection),
- la durée de conservation (l'effacement des données dans un délai raisonnable après les élections),

[42] Art. 6 de la loi modifiée du 21 décembre 2007 portant réglementation du financement des partis politiques.
[43] L'article 8 de la loi sur le financement des partis politiques prévoit que « *seules les personnes physiques sont autorisées à faire des dons aux partis politiques et à leurs composantes* ».

- l'existence des droits des citoyens en matière de protection des données (leur droit d'accès aux données, leur droit de rectification et d'effacement des données, leur droit de s'opposer au traitement de leur données à des fins de prospection électorale et leur droit d'introduire une réclamation auprès de la CNPD),
- les moyens de contact pour exercer leurs droits (adresse postale, lien vers un site internet et adresse électronique).

Il est primordial que toute communication contienne les informations relatives au droit d'opposition. Par exemple, les communications peuvent contenir un coupon-réponse ou indiquer une adresse mail spécifique permettant aux personnes concernées d'exprimer leur souhait de ne plus recevoir de tels courriers.

L'exercice du droit d'opposition doit être simple et efficace, et l'outil doit être facilement accessible. Il est ainsi recommandé d'instaurer une adresse électronique dédiée pour le traitement de ces demandes et de les traiter rapidement, en particulier lors de périodes électorales lorsqu'un nombre important de messages est diffusé.

5.1.2. L'envoi de messages électroniques

En cas d'envoi de prospection politique par voie électronique, la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques s'applique. La CNPD rappelle qu'une prospection politique par téléphone ou courrier électronique (ou tout autre moyen de communication électronique) ne peut se faire qu'avec l'accord préalable des personnes contactées.

Ainsi, si aucun lien entre le parti politique et la personne concernée n'existe, le consentement préalable doit être demandé avant l'envoi de communications électroniques (« opt-in »). Ce consentement doit être une manifestation de volonté par une déclaration ou par un acte positif clair et doit être libre, spécifique, et informé et univoque. Il faut encore qu'il soit recueilli avant l'envoi de messages électroniques[44]. Par la suite, chaque message de prospection doit informer la personne concernée de ses droits, en particulier de son droit de retirer son consentement à tout moment.

Lorsque les partis politiques communiquent avec des personnes dans le cadre d'une relation préexistante, typiquement avec leurs membres ou leurs sympathisants, ces communications peuvent avoir lieu sans récolter le consentement préalable des personnes concernées. En contrepartie, les personnes concernées doivent avoir le droit de s'y opposer à tout moment et être informées de ce droit lorsque les données sont recueillies, ainsi que lors de chaque message de prospection. Par conséquent, le membre ou sympathisant concerné doit, lors de la collecte de ses coordonnées électroniques, être clairement et distinctement informé de l'utilisation possible de celles-ci à des fins de prospection directe et doit avoir l'opportunité de s'opposer à une telle utilisation.

Il convient de préciser que l'envoi de messages électroniques personnalisés par un moyen de communication électronique ne peut pas être fondé sur les « intérêts légitimes » du parti politique en vertu de l'article 6, paragraphe 1er, lettre f), du RGPD puisque ce type de traitement ne permet pas une mise en balance adéquate entre ces intérêts et les intérêts des personnes concernées.

[44] Conformément à l'article 4, point 11, du RGPD.

5.2. Le ciblage publicitaire en ligne à des fins de prospection électorale

Outre les messages nominatifs, les partis politiques et les candidats peuvent être amenés à utiliser des publicités dans l'espace numérique pour promouvoir leurs programmes politiques. Or, contrairement aux espaces publicitaires physiques, relativement statiques par nature, les publicités en ligne peuvent impliquer d'une part une grande volatilité des messages publicitaires et d'autre part un ciblage basé sur un profil établi en recourant à un traitement de données à caractère personnel.

Bien que la communication politique présente des traits promotionnels, les communications en lien avec de la prospection politique présentent des caractéristiques particulières à cause précisément du contexte électoral. En effet, la circulation et la confrontation des idées et des convictions politiques sont l'essence même de ce débat. Contrairement à la commercialisation d'un produit ou d'un service, pour laquelle il est facile d'identifier le responsable du traitement, la promotion politique n'est pas toujours évidente à attribuer à un parti politique, à un candidat ou à un autre acteur actif dans la campagne électorale. Ainsi, il est important de faire preuve de transparence sur l'identité de l'auteur d'un message publicitaire à visée politique. Cette transparence a été identifiée comme l'un des vecteurs pour enrayer les risques de manipulation en ligne. Dans ce sens, il peut être recommandé que les candidats et les partis se dotent de comptes vérifiés sur les réseaux sociaux (par exemple la procédure « Verified Blue Badge » auprès de Facebook, TikTok ou Twitter) afin d'être clairement identifié et lutter en même temps contre des faux comptes et les tentatives de diffusion de désinformation.

Outre la transparence vis-à-vis du destinataire de la prospection politique, il conviendrait de rendre accessible au grand public et aux médias tous les messages publicitaires. De plus, ces messages pourraient être catégorisés par les diffuseurs en fonction des critères de ciblage utilisés et des profils auxquels ils ont été adressés. Cette pratique permettrait de pallier le risque d'opacité, de favoriser la tenue du débat contradictoire et public ainsi que la confrontation des idées et au final contribuer ainsi à la sincérité des campagnes électorales.

Les partis politiques et les candidats pourraient être tentés de concentrer leurs campagnes publicitaires à certains groupes de personnes jugés déterminants pour l'issue du scrutin. Cependant, de tels procédés peuvent entraver la libre circulation de l'information et enlever au reste de l'électorat la possibilité de faire leur choix en confrontant les points de vue défendus par les différents partis politiques. Ainsi, même si c'est techniquement possible et légalement défendable, il serait préférable, pour le bon fonctionnement du système électoral dans une société démocratique, de restreindre le recours à une trop grande segmentation des messages politiques et à un cloisonnement de groupes de personnes en fonction de leurs profils politiques.

Une attention particulière doit être apportée au micro-ciblage (« micro-targeting ») quand celui-ci est utilisé comme un révélateur de données sensibles. Le micro-ciblage est une forme de publicité ciblée en ligne qui analyse les données à caractère personnel pour identifier des intérêts d'un public spécifique ou d'individus afin d'influencer leurs actions. Le micro-ciblage peut permettre de déterminer la pertinence d'un contenu publicitaire, y compris d'un message envoyé à fins de prospection politique. Il s'agit d'un outil puissant, qui dépasse un profilage classique. En effet, le micro-ciblage croise une grande quantité d'informations qui, prises individuellement, ne seraient pas considérées comme des données sensibles, mais qui mises ensemble peuvent révéler des données sensibles, à savoir l'opinion politique d'une

personne[45]. Ce type de traitement peut « *comprendre des utilisations de données à caractère personnel qui vont à l'encontre ou au-delà des attentes raisonnables des individus et enfreignent ainsi les principes et règles applicables en matière de protection des données* »[46]. La pratique dans d'autres pays montre que des partis politiques ou leurs sous-traitants peuvent recourir à des « *techniques d'extraction de données capables de faire le lien entre les caractéristiques personnelles d'un individu et ses convictions politiques et de découvrir le comportement politique des électeurs* »[47].

Or, une 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* »[48]. Par ailleurs, ce type de prise de décision ne peut pas être fondé sur des données sensibles, à moins qu'une exception[49] s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place[50]. Comme l'indique le considérant 71 du RGPD, le traitement doit être « *assorti de garanties appropriées* », dont une « *information spécifique* » et le droit « *d'obtenir une explication quant à la décision prise* ». Les lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 fournissent d'avantage d'informations quant aux garanties appropriées[51].

Il apparaît que, selon la granularité du profilage, les messages publicitaires à des fins de prospection politique peuvent orienter les opinions des électeurs de façon à influencer le résultat du scrutin[52]. Il peut être considéré que ce type de profilage a le potentiel « *de produire des effets juridiques à l'égard d'une personne concernée* » ou *« d'affect[er] l[la personne concernée] de manière significative »* en produisant des effets sur l'issue des élections ou du vote[53]. Cette appréciation doit prendre en compte la vulnérabilité des personnes ciblées, notamment l'âge[54]. En fonction des traitements de données envisagés, le responsable du traitement doit vérifier si une analyse d'impact relative à la protection des données (AIPD)[55] est nécessaire lorsque celui-ci considère recourir à des messages ciblés. Les traitements

[45] Article 9 du RGPD. Voir, ci-avant, le point 2.2. CJUE, arrêt du 1er août 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, ECLI:EU:C:2022:601. Voir aussi les lignes directrices 8/2020 du Comité Européen de la Protection des Données (EDPB) du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux et les lignes directrices du groupe de travail « article 29 » du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 (WP251rev0.1), approuvées par le Comité européen de la protection des données, pages 16-17

[46] Voir aussi les lignes directrices 8/2020 du Comité Européen de la Protection des Données (EDPB) du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux, point 10.

[47] Conseil de l'Europe, Comité d'Experts sur le pluralisme des médias et la transparence de leur propriété, Internet et campagnes électorales - Étude relative à l'utilisation d'internet dans le cadre des campagnes électorales, Étude du Conseil de l'Europe, DGI(2017)11, avril 2018

[48] Article 22, paragraphe 1er, du RGPD

[49] Le traitement ne peut être mis en œuvre que sur base de l'article 9, paragraphe 2, lettres a) ou g) du RGPD.

[50] Article 22, paragraphe 4 du RGPD.

[51] Groupe de travail « article 29 », Lignes directrices du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 (WP251rev.01), approuvées par le Comité européen de la protection des données.

[52] Lignes directrices 8/2020 du Comité Européen de la Protection des Données (EDPB) du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux, point 13.

[53] Idem., page 23.

[54] Voir, pour plus d'informations, Groupe de travail « article 29 », Lignes directrices du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 (WP 251rev.01)

[55] Voir notamment, sur les AIPD: https://cnpd.public.lu/fr/actualites/national/2019/03/liste-DPIA.html. Voir également : Groupe de travail « article 29 », Lignes directrices du 4 octobre 2017 concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (WP248rev.01), approuvées par le Comité européen de la protection des données et Comité européen de la protection des données (EDPB), Lignes directrices 8/2020 du 13 avril 2021 sur le ciblage des utilisateurs de médias sociaux, section 7.

impliquant un micro-ciblage pouvant révéler des opinions politiques nécessitent probablement la conduite d'une AIPD avant la mise en place du traitement.

Le cas échéant, le seul fondement de licéité envisageable pour légitimer ce traitement de données sensibles est le consentement explicite. De plus, il convient de souligner que les responsables du traitement doivent veiller à ce que le consentement explicite ait été recueilli avant le traitement et conformément aux autres exigences du RGPD[56].

Dès lors, la CNPD est d'avis qu'il y a lieu d'éviter un profilage excessif des citoyens. Elle ne conteste pas la possibilité d'effectuer des opérations de tri et de sélection en fonction de l'âge ou de l'adresse des électeurs. Toutefois, la CNPD met en garde contre des critères pouvant cibler des personnes sur base de leurs origines réelles ou supposées, notamment par la consonance des noms ou le lieu de naissance ainsi que contre l'agrégation de données d'une personne concernée avec des données statistiques ou démographiques ou des données pouvant révéler sa situation socio-économique réelle ou supposée. Par ailleurs, la CNPD recommande de ne pas utiliser de données sensibles dans les modèles de publicité comportementale à cause des risques inhérents à ce type de traitements.

Finalement, la CNPD rappelle qu'il est pénalement répréhensible de discriminer des personnes, notamment sur base de distinctions fondées sur l'origine, le genre ou l'appartenance ou la non-appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée[57].

6. Conclusions

Tout traitement de données doit respecter les principes découlant du RGPD, être accompagné de mesures de sécurité adéquates et les responsables du traitement doivent s'assurer des mesures techniques et organisationnelles appropriées, notamment en recourant uniquement à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources. De même, les responsables du traitement doivent veiller au respect des droits des personnes concernées, à savoir le droit à l'information, le droit d'accès, le droit à l'oubli et le droit d'opposition et le droit de formuler une réclamation auprès de la CNPD.

Depuis 2022, la loi électorale limite strictement les finalités de la consultation des listes électorales *« aux fins de vérifier l'exactitude des listes électorales »*, notamment par *« la constatation de la qualité d'électeur des personnes physiques »*, ce qui implique que les partis politiques ne peuvent plus obtenir une copie des listes électorales pour les utiliser à des fins de prospection politique[58].

À cause des enjeux pour des élections libres et équitables, les partis et candidats politiques devraient attacher une grande attention à l'information et la transparence autour de leurs messages de prospection électorale. Cette transparence accrue permet de maintenir les bases d'un dialogue ouvert, nécessaire à une démocratie vivante.

Au-delà de la protection des données, il peut être considéré que la communication des partis politiques doit être transparente, c'est-à-dire que les citoyens et la presse puissent avoir accès aux contenus de prospection politique, que ces contenus soient diffusés par des messages personnalisés ou par des publicités personnalisées. Le respect de la législation en matière de protection des données est un vecteur parmi d'autres favorisant le déroulement d'élections libres et équitables.

[56] Voir ci-haut, point 4.1.
[57] Voir Code pénal, articles 454 ss.
[58] Conformément au principe de la limitation des finalités au sens de l'article 5, paragraphe 1er, lettre b), du RGPD.

7. Pour en savoir plus

- Groupe de travail « article 29 », Avis du 9 avril 2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP217)

  https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf

- Groupe de travail « article 29 », Lignes directrices du 4 octobre 2017 concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (WP248rev.01), repris par le Comité européen de la protection des données

  https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/wp248-rev01-fr.pdf

- Groupe de travail « article 29 », Lignes directrices du 6 février 2018 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 (WP 251rev.01) repris par le Comité européen de la protection des données

  https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

- Groupe de travail « article 29 », Lignes directrices du 11 avril 2018 sur la transparence au sens du règlement (UE) 2016/679 (WP260rev.01), repris par le Comité européen de la protection des données

  https://ec.europa.eu/newsroom/article29/items/612053

- Comité Européen de la Protection des Données (EDPB), Déclaration sur l'utilisation de données à caractère personnel dans le cadre de campagnes politiques, 13 mars 2019

  https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

- Comité Européen de la Protection des Données (EDPB), Lignes directrices 5/2020 du 4 mai 2020 sur le consentement au sens du règlement (UE) 2016/679

  https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_fr

- Comité Européen de la Protection des Données (EDPB), Lignes directrices 8/2020 du 13 avril 2021, sur le ciblage des utilisateurs de médias sociaux

  https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_fr

- Contrôleur européen de la protection des données (EDPS), Avis n°3/2018 du 19 mars 2018 sur la manipulation en ligne et les données à caractère personnel

  https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf

- Commission européenne, Orientations relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral : La contribution de la Commission européenne à la réunion des chefs d'État et de gouvernement à Salzbourg, 19 et 20 septembre 2018, COM/2018/638 final

  https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=COM:2018:638:FIN

- Commission Nationale de l'Informatique et des Libertés (France), Vie politique et citoyenne, 2022

https://www.cnil.fr/fr/vie-politique-et-citoyenne

- Information Commissioner's Office (Royaume-Uni), Enquête sur l'analyse de données à des fins politiques, 2018

  https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/

- Garante per la protezione dei dati personali (Italie), Enquête sur Facebook, l'application « Thisisyourdigitallife » et l'application « Candidati », communiqué du 7 février 2019

  https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9081475&zx=8ghzplmiahrr

- Autorité de protection des données (Belgique), Traitement de données à caractère personnel à des fins d'envois personnalisés de propagande électorale et respect de la vie privée des citoyens : principes fondamentaux, mai 2018

  https://www.autoriteprotectiondonnees.be/publications/note-juridique-sur-les-elections.pdf

- Conseil de l'Europe, Eleclab – le laboratoire électoral du Conseil de l'Europe

  https://www.coe.int/fr/web/electoral-assistance/eleclab

- Conseil de l'Europe, Lignes directrices relatives à la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre des campagnes politiques, février 2022

  https://rm.coe.int/lignes-directrices-protection-des-donnees-et-campagnes-politiques/1680a5afdd

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

15, boulevard du Jazz I L-4370 Belvaux
Tél. : (+352) 26 10 60 - 1 I Fax. : (+352) 26 10 60 - 6099

www.cnpd.lu