Le Règlement Général sur la Protection des Données

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

Contenu

1. Introduction

À travers les présentes lignes directrices, 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 compagnes 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, 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.

Comme le montre les révélations de Cambridge Analytica et les controverses autour des phénomènes de la désinformation et de la manipulation[2], 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, des initiatives sont lancées pour garantir la tenue d'élections européennes libres et équitables. Depuis septembre 2018, la Commission européenne et les Etats membres œuvrent à l'application d'un « paquet de mesures concernant des élections

[1] Pour des informations générales, voir par exemple le guide pratique pour le monde associative : 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 sur la manipulation en ligne et les données à caractère personnel, 19 mars 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf

européennes libres et équitables »[3] afin de protéger les droits démocratiques des citoyens et leur liberté d'expression. Ce paquet comporte notamment des volets relatifs à la cyber sécurité, la lutte contre la désinformation et contre les contenus haineux. Le paquet promeut la transparence et contient des recommandations et mesures concrètes concernant la protection des données. Le Comité Européen de la Protection des Données (EDPB) a récemment adopté une déclaration sur l'utilisation des données à caractère personnel dans le cadre de campagnes politiques[4].

En réaction aux récents scandales, sous l'impulsion de la Commission européenne, les plateformes en ligne et le secteur de la publicité se sont engagés à respecter un code de bonnes pratiques lancé dans le cadre du plan d'action européen contre la désinformation[5]. Sans préjuger des nouvelles initiatives et règles nécessaires, ce code de conduite constitue une avancée pour renforcer la transparence, lutter contre la désinformation et contre les tentatives de manipulation.

Les révélations de Cambridge Analytica et les autres développements décrits ci-dessus illustrent comment une violation potentielle du droit à la protection des données à caractère personnel pourrait affecter d'autres droits fondamentaux, tels que la liberté d'expression, la liberté d'opinion et la possibilité de penser librement sans manipulation.

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.

---

[3] Voir notamment le dossier de presse sur le site de la Commission européenne : http://europa.eu/rapid/press-release_IP-18-5681_fr.htm. Voir également l'avis du Contrôleur européen de la protection des données concernant ce paquet : Avis nº 10/2018 sur le paquet de mesures de la Commission concernant des élections européennes libres et équitables, https://edps.europa.eu/sites/edp/files/publication/18-12-18_opinion_on_election_package_fr.pdf

[4] EDPB, Déclaration 2/2019 sur l'utilisation des données à caractère personnel dans le cadre de campagnes politiques, adopté le 13 mars 2019: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

[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 .

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.

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 de 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 sont pertinentes. 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 de traitement doivent impérativement observer les principes découlant du RGPD pour tous leurs traitements de données, à savoir

- le principe de licéité, loyauté et transparence (articles 5 paragraphe (1) lettre (a), 6 et 9 du RGPD),
- le principe de limitation des finalités (article 5 paragraphe (1) lettre (b) du RGPD),
- le principe de minimisation des données (article 5 paragraphe (1) lettre (c) du RGPD),
- le principe d'exactitude (article 5 paragraphe (1) lettre (d) du RGPD),
- le principe de limitation de la conservation (article 5 paragraphe (1) lettre (e) du RGPD),

- le principe d'intégrité et de confidentialité des données (articles 5 paragraphe (1) lettre (f), 25 et 32 du RGPD), et
- le principe de responsabilité (article 5 paragraphe (2) du RGPD).

Le principe de licéité (articles 5 paragraphe (1) lettre (a) et 6 du RGPD) impose aux responsables de traitement de choisir la base juridique appropriée au traitement (aussi pour les données déduites (« inferred data »)).[6] Lorsque le traitement de données englobe des données dites « sensibles », comme des données révélant des opinions politiques, les responsables de 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.

Le principe de limitation de la finalité (article 5 paragraphe (1) lettre (b) du RGPD) exige que les responsables de traitement identifient une finalité licite pour chaque traitement, en veillant à ce qu'un traitement ultérieur n'est uniquement possible pour une finalité compatible.

Le principe de transparence (articles 13 et 14 du RGPD) requiert que les personnes concernées soient informées de chaque finalité du traitement, quel que soit la source des données collectées par le responsable de traitement.

Les responsables de traitement doivent vérifier si les données reçues de tiers ont été obtenues de manière licite. De plus, ils doivent veiller à ce que la finalité initiale utilisée pour légitimer la collecte soit compatible avec les finalités poursuivies (article 5 paragraphe (1) lettre (b) du RGPD) et ils doivent s'assurer que, si la collecte initiale a été légitimée par le consentement, que les personnes concernées ont donné leur consentement éclairé également pour la finalité ultérieure (article 6 paragraphe (4) du RGPD).

En vertu du principe d'exactitude (article 5 paragraphe (1) lettre (d) du RGPD), les responsables de traitement doivent garantir l'exactitude des données, en particulier pour les données provenant de sources différentes et les données déduites. A cet égard, le principe de minimisation des données exige que les responsables de traitement suppriment les données lorsqu'elles ne sont plus nécessaires à la finalité initiale pour laquelle elles ont été collectées (article 5 paragraphe (1) lettre (c) du RGPD).

Parmi les mesures à prendre en application du principe d'intégrité et de confidentialité (article 32 du RGPD), les responsables de traitement doivent établir clairement qui a accès aux données[7]. 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.

Les responsables de traitement doivent prévoir des mesures de sécurité adéquates, c'est-à-dire s'assurer des mesures techniques et organisationnelles appropriées[8]. 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

[6] Voir section consacrée aux conditions de licéité.
[7] Egalement en application des principes de la protection des données dès la conception et par défaut, défini à l'article 25 du RGPD, ainsi qu'aux obligations liées à la mise en place d'un niveau de sécurité adapté au risque, défini à l'article 32 du RGPD.
[8] Voir, pour plus d'informations, notre dossier thématique sur la sécurité informatique: https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/securite-informatique.html

d'intrusion. Parmi les mesures de sécurité, il convient également de sensibiliser les personnes susceptibles d'exécuter les opérations de traitement.

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. Il convient de cloisonner les fichiers de prospection 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.

De plus, les responsables doivent recourir uniquement à des sous-traitants présentant des garanties suffisantes et démontrant des connaissances spécialisées, une fiabilité et des ressources appropriées (article 28 du RGPD). Les contrats conclus avec les sous-traitants doivent clarifier leurs obligations respectives.

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 de 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 (voir article 33 du RGPD).

Lorsque les responsables de traitement envisagent de recourir au profilage ou à la prise de décision automatisé, 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 (article 22 du RGPD). En pratique, il est important d'obtenir le consentement explicite des personnes concernées, et le cas échéant, vérifier auprès du prestataire que ce consentement a été valablement exprimé. Selon le traitement envisagé, il peut être nécessaire d'effectuer en amont une analyse d'impact relative à la protection des données.

Finalement, les responsables de 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 (articles 12 à 21 du RGPD).

Le principe de responsabilité (« accountability ») signifie que les responsables de traitement doivent être en mesure de démontrer leur conformité à tout moment (article 5 paragraphe (2) du RGPD). Cela implique par exemple d'établir une documentation adéquate relative aux traitements de données effectués, y compris un registre de traitement des données 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 règlement général sur la protection des données. Leur traitement est strictement encadré par l'article 9 du RGPD.

Les finalités de l'utilisation des données à caractère personnel et l'identité du responsable de 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 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 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.

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 de s'appliquer. 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 (au sujet de ces conditions, voir ci-après, point 2.4.).

2.3. La provenance des données

2.3.1. 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 »[9] (au sujet du traitement de données de membres et de sympathisants, voir également ci-après, point 2.4.2.).

2.3.2. La réutilisation des listes électorales

Selon la législation en vigueur, les listes des électeurs constituent une source de données à laquelle les partis politiques et les candidats peuvent en principe avoir recours à des fins de publicité politique.

L'article 20 alinéa (3) de la loi électorale du 18 février 2003 prévoit 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 ». Les données contenues dans ces listes comprennent le nom, prénoms,

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

domicile, le lieu et la date de naissance des électeurs, et le cas échéant, la nationalité et le nom et prénoms du conjoint (article 13 et 14 de la loi électorale). Certains partis politiques luxembourgeois ont fait usage de ce droit et ont utilisé les données issues de ces listes à des fins de prospection politique pendant les précédentes périodes électorales.

Dans ce contexte, la CNPD précise que l'établissement de la liste des réclamations et des listes électorales constitue un traitement de données à caractère personnel au sens de l'article 4 point (2) du RGPD. Ce traitement est mis en œuvre par le collège des bourgmestres et échevins, qui répond donc à la définition de responsable de traitement au sens de l'article 4 point (4) du RGPD.

La loi détermine la finalité du traitement au sens de l'article 5 paragraphe (1) lettre (b) du RGPD en ce que les listes électorales ne peuvent être utilisées qu'à des fins électorales, c'est-à-dire en premier lieu la constatation de la qualité d'électeur des personnes physiques remplissant les conditions reprises dans le Titre I de la loi électorale. Les données des listes électorales peuvent également être utilisées pour des fins de prospection politique par des partis politiques, mais uniquement pendant les périodes électorales. Il convient de rappeler à cet endroit que l'article 32bis de la Constitution réserve aux partis politiques un rôle particulier dans le contexte électoral, en reconnaissant qu'ils « concourent à la formation de la volonté populaire et à l'expression du suffrage universel ».

La CNPD ne met pas en doute la licéité de la finalité de la prospection des électeurs inscrits, notamment pour leur adresser les programmes politiques, dans les limites de la finalité électorale posée par l'article 20 de la loi électorale. L'article 5 du RGPD érige la finalité d'un traitement de données en un principe essentiel dans le domaine de la protection des données en ce que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes. Les données à caractère personnel des listes électorales ne doivent pas être traitées ultérieurement de manière incompatible avec leur finalité électorale, p.ex. ne doivent pas faire l'objet d'une quelconque utilisation – par exemple à une finalité commerciale ou pour la promotion d'une association ou d'un syndicat. À cet égard, les partis politiques sont invités à prévoir une durée de conservation proportionnée à la finalité recherchée. Toutefois, les partis politiques devront veiller à garantir que les citoyens ayant fait usage de leur droit d'opposition ne soient plus contactés lors d'élections communales, européennes ou législatives futures.

. Pour des informations plus détaillées, la CNPD attire l'attention sur sa communication d'août 2018 au sujet de l'utilisation des listes électorales à des fins de prospection électorale (https://cnpd.public.lu/fr/actualites/national/2018/08/communication-administres.html).

2.3.3. 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.

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.

2.3.4. 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 »).

2.4. 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 (1) 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 de traitement sont dès lors amenés à fonder ces traitements sur les conditions de licéité 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.

2.4.1. Le consentement explicite de la personne concernée

Sur la base des articles 6 paragraphe (1) lettre (a) et 9 paragraphe (2) lettre (a) du RGPD, les responsables de traitement peuvent baser leurs traitements sur le consentement explicite des personnes concernées. Afin de garantir que le consentement soit fourni de façon libre et éclairée au sens de l'article 7 et du considérant 42 du RGPD[10], il est primordial d'informer les personnes concernées conformément à l'article 13 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 de traitement doit informer la personne concernée de cette possibilité et doit permettre un retrait facile du consentement.

Si les responsables de 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. Quoi qu'il en soit, il faut 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 de 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.

2.4.2. 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 (1) lettre (f) et 9 paragraphe (2) lettre (d) du RGPD.

En invoquant leurs « intérêts légitimes » pour légitimer ces traitements de données, les responsables de traitement doivent s'assurer à ce que les « intérêts ou les libertés et droits fondamentaux » des personnes concernées ne prévalent pas. Un parti politique a ainsi le droit

[10] Concernant les conditions relatives au consentement, voir notamment : Groupe de travail « Article 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, WP 259 rev. 1. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

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.

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

En combinaison avec l'article 6 paragraphe (1) 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.

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 de traitement devra respecter les conditions de licéité prévues par l'article 6 du RGPD.

En invoquant des intérêts légitimes prévu par l'article 6 paragraphe (1) (f) du RGPD, le parti politique devra continuer de les mettre en balance avec les intérêts et de la personne concernée. Concrètement, si la personne exprimant 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.

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

En principe, conformément aux articles 6 paragraphe (1) 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 »[11]. Les noms des personnes physiques[12] doivent dès lors être collectés sur la base d'une obligation légale et doivent également être communiqués aux autorités compétentes.

3. Les différentes modalités de communication

3.1. La prospection par des messages nominatifs directs

La prospection politique par la transmission de messages nominatifs directs est apparentée à du marketing direct. Ainsi, les partis politiques et candidats doivent respecter les dispositions particulières en la matière.

3.1.1. L'envoi de courriers postaux

En cas d'envoi de publicité politique par courrier postal, le RGPD confère aux personnes concernées un droit de s'opposer au sens de l'article 21 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. Tel est le cas si la législation autorise l'utilisation de certaines données, par exemple celles issues des listes électorales, à des fins de prospection politique en période électorale.

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 les listes électorales sur la base de l'article 20 de la loi électorale du 18 février 2003),

[11] Art. 6 de la *Loi modifiée du 21 décembre 2007 portant réglementation du financement des partis politiques*.
[12] 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 ».

- 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),
- 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.

3.1.2. L'envoi de messages électroniques

En cas d'envoi de publicité politique par voie électronique, la loi luxembourgeoise 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 libre, spécifique et informé. 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.

Il convient de préciser que l'envoi de messages 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 (1) 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. Par conséquent, le responsable de traitement doit recueillir le consentement de la personne concernée au sens des articles 6 paragraphe (1) lettre (a) et 7 du RGPD avant l'envoi de messages électroniques.

Eu égard au considérant 47 du RGPD, 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 marketing direct et doit avoir l'opportunité de s'opposer à une telle utilisation.

3.2. 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 de 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 « Blue Badge » auprès de Facebook) 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 publicité, 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.

3.2.1. Le micro-ciblage (« micro-targeting »), 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 publicité politique. Cet outil est puissant et de la même façon qu'une donnée personnelle est une donnée permettant d'identifier une personne, la limite qui fait qu'un micro-profilage dépasse un profilage classique et révèle une donnée sensible est qu'on puisse du fait d'avoir croisé les informations déduire par exemple l'opinion politique d'une personne. Le cas échéant, le seul fondement de licéité envisageable pour légitimer ce traitement de données est le consentement explicite. De plus, il convient de souligner que les responsables de traitement doivent veiller à ce que les prestataires (et donc les réseaux sociaux) ont recueilli valablement ce consentement explicite.

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 »[13].

Il apparaît que, selon la granularité du profilage, les messages publicitaires à des fins de publicité politique peuvent orienter les opinions des électeurs de façon à influencer le résultat du scrutin. Il peut être considéré que ce type de profilage a le potentiel « d'affect[er] [la personne concernée] de manière significative » en produisant des effets sur l'issu des élections ou du vote. Cette appréciation doit prendre en compte la vulnérabilité des personnes ciblées, notamment l'âge[14].

Or, suivant l'article 22 paragraphe (1) du RGPD, 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 ». Conformément au considérant 71 du RGPD, ce type de profilage doit être « assorti de garanties appropriées », dont une « information spécifique » et le droit « d'obtenir une explication quant à la décision prise ». Le considérant 71 du RGPD établit que « le profilage automatisé fondé sur des catégories particulières de données à caractère personnel ne devraient être autorisé que dans des conditions spécifiques ».

Dès lors, la CNPD est d'avis qu'il y a lieu d'éviter un profilage excessif des citoyens. La CNPD 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

[13] 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

[14] Voir, pour plus d'informations, Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP 251 rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

l'appartenance ou la non-appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée[15].

3.2.2. La nécessité d'effectuer une analyse d'impact en cas de recours au micro-ciblage

Si un parti politique ou un candidat considère recourir à des messages ciblés, il convient de vérifier si une analyse d'impact relative à la protection des données (AIPD)[16] est nécessaire.

L'article 35 paragraphe (3) du RGPD établit une liste de traitements pour lesquels les responsables de traitement doivent entreprendre une analyse. Trois cas de figure sont visés par cet article, et couvrent en particulier « le traitement à grande échelle de catégories particulières de données visées à l'article 9 ». De même, l'article prévoit qu'une AIPD doit être effectuée en recourant à un « profilage […] sur la base de laquelle sont prises des décisions […] affectant [la personne concernée] de manière significative de façon similaire ». En complément à la liste de l'article 35 du RGPD, la CNPD a par ailleurs adopté une liste nationale supplémentaire de traitements pour lesquels une AIPD est également nécessaire. Cette liste inclut notamment « les activités de traitement de dossiers susceptibles de contenir des données à caractère personnel concernant l'ensemble de la population nationale […] ». Il convient de souligner que cette liste n'est pas une liste exhaustive de tous les types d'opération de traitement nécessitant la réalisation d'une AIPD. Ainsi l'absence d'un type d'opération de traitement sur cette liste ne signifie pas nécessairement qu'une AIPD n'est pas requise. La liste se limite aux activités de traitement qui nécessiteront toujours la réalisation d'une AIPD. Pour les activités de traitement ne figurant pas sur cette liste, les responsables du traitement des données devraient s'appuyer sur l'article 35 (1) du RGPD et sur les lignes directrices WP248 du groupe de travail de l'article 29 pour évaluer la nécessité d'une AIPD.

Les traitements impliquant un micro-ciblage pouvant révéler des opinions politiques nécessitent probablement la conduite d'une AIPD avant la mise en place du traitement. De plus, si un parti politique ou un candidat envisage d'établir une base de données à partir de listes électorales, une AIPD paraît indiqué avant la mise en place de cette base de données. Conformément à l'article 36 paragraphe (1) du RGPD, le responsable de traitement doit effectuer une consultation préalable au traitement auprès de la CNPD pour avis sur l'AIPD si le traitement présente encore un risque résiduel élevé pour les droits et libertés des personnes après la mise en place de mesures pour atténuer le risque.

4. Conclusions

Tout traitement de données doit respecter les principes découlant du RGPD, être accompagné de mesures de sécurité adéquates et les responsables de 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 de traitement doivent veiller au respect des droits des personnes concernées, à savoir le droit à

[15] Voir Code penal, articles 454 ss.
[16] Voir notamment, sur les AIPD:
https://cnpd.public.lu/fr/actualites/national/2019/03/liste-DPIA.html

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.

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 publicité 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.

5. Pour en savoir plus

- 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

- 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

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

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

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

  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

- 27e Conférence internationale des commissaires à la protection des données et à la vie privée, *résolution sur l'utilisation de données personnelles pour la communication politique*, Montreux, 14-16 septembre 2005

  https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_political_communication_fr.pdf

- Autorité de protection des données (Belgique), Trai*tement 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/sites/privacycommission/files/documents/Note_elections_RGPD.pdf

- 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

  https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux

- Commission Nationale de l'Informatique et des Libertés, *Elections législatives : Six réflexes pour une campagne 2.0*, 15 mai 2017

  https://www.cnil.fr/fr/elections-legislatives-six-reflexes-pour-une-campagne-20-responsable

- Commission Nationale de l'Informatique et des Libertés, *Comment chiffrer ses documents et ses répertoires ?,* 3 mars 2017

  https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires