Campagne électorale et utilisation des données personnelles : grands principes et points de vigilance

par Émilie **Seruga-Cau**
Chef du service des affaires régaliennes et des collectivités territoriales de la CNIL
et Tiphaine **Havel**
Conseillère pour les questions institutionnelles et parlementaires de la CNIL

L'utilisation de nouveaux moyens de communication, et en particulier des réseaux sociaux, en période électorale impacte nécessairement la vie démocratique et politique. Dans le même temps, la généralisation du recours à ces nouveaux modes de communication renouvelle les enjeux attachés à l'utilisation des données à caractère personnel dans le domaine politique. Quelques mois après l'entrée en vigueur du règlement général n° 2016/679 du 27 avril 2016 relatif à la protection des données (RGPD)[1] et alors même que l'année 2018 a été marquée par plusieurs affaires illustrant la nécessité d'empêcher l'utilisation abusive des données lors des campagnes politiques, un rappel des grands principes à respecter en matière de protection des données à caractère personnel et des principaux points de vigilance lors de l'utilisation de ces données dans le cadre d'une campagne électorale prend tout son sens, à quelques mois des élections européennes (26 mai 2019) et alors que se profile dans le courant de l'année l'ouverture de la campagne officielle des élections municipales.

Utilisation des données en matière politique : un encadrement de longue date par la CNIL

L'utilisation de fichiers à des fins politiques ayant toujours suscité des interrogations, la CNIL s'est très tôt emparée du sujet afin de préciser les règles applicables en matière de communication électorale et politique.

Recommandation – La première recommandation adoptée en cette matière remonte ainsi à 1991 et a fait, à plusieurs reprises, l'objet de modifications notamment afin de tenir compte de l'émergence de nouveaux usages (démocratisation de l'accès et du recours à des sites Internet, utilisation des messages électroniques, recours aux automates d'appel, etc.).

Observatoire des élections – Cet encadrement de l'utilisation des données à caractère personnel en matière politique s'est également illustré par la création, au sein de la CNIL et à l'occasion des élections présidentielle et législatives de 2012, d'un Observatoire des élections[2] chargé de mener des opérations de veille, de dialogue avec les partis politiques et d'information régulière du public.

Guide – Plus récemment, un guide a été élaboré conjointement par la CNIL et le Conseil supérieur de l'audiovisuel (CSA) afin de rappeler les compétences respectives des deux autorités ainsi que les règles applicables en matière de communication politique[3].

Auditions – Les conditions dans lesquelles les candidats et les partis politiques peuvent utiliser les données issues des réseaux sociaux ont également été précisées à la suite de plusieurs auditions menées auprès des principaux prestataires de logiciels de stratégie électorale, dans la perspective des échéances électorales de 2016 (primaires) et 2017 (élections présidentielle et législatives)[4]. L'utilisation croissante par les candidats de ces logiciels, gros consommateurs de données personnelles, souvent sensibles, suscite de nouvelles interrogations au regard de la protection de la vie privée.
La sensibilité particulière des données relatives aux opinions politiques, dont le traitement est susceptible par nature de porter atteinte aux libertés fondamentales ou à la vie privée, justifie en effet qu'une vigilance particulière soit portée aux conditions dans lesquelles il est possible d'utiliser de telles données. La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée[5] pose ainsi un principe d'interdiction de collecter et de traiter ce type de données. La levée de cette interdiction ne peut dès lors intervenir que dans des conditions particulièrement strictes. À ce titre, le nouveau cadre juridique tel qu'il résulte de l'entrée en vigueur du RGPD et tel qu'il est en particulier précisé à son article 9 (« Traitement portant sur des catégories particulières de données à caractère personnel ») concernant le traitement de données « sensibles », n'opère aucun changement de paradigme sur ce point, le traitement de telles données demeurant par principe interdit.

Opinions politiques : renforcement par le RGPD de la protection accordée aux personnes concernées

Historiquement, la réglementation relative à la protection des données à caractère personnel a été conçue autour du respect de

(1) Pour une présentation générale de ce texte, v. Dalloz IP/IT 2016. 566 ; Collectif, *Le RGPD*, Dalloz, coll. « Grand Angle », 2018.
(2) www.cnil.fr/fr/elections/les-missions-de-lobservatoire.
(3) CSA/CNIL, Campagnes électorales : tout savoir sur les règles CSA et CNIL, nov. 2016.
(4) www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.
(5) V. not. *RGPD / Loi informatique et libertés modifiée*, Dalloz, coll. « Les Textes », 2018.

plusieurs principes clefs, lesquels demeurent plus que jamais d'actualité sous l'empire de la nouvelle réglementation.

Principe de finalité des collectes – En particulier, il importe que les données relatives aux opinions politiques ne soient collectées que pour des finalités déterminées, explicites et légitimes (principe de finalité).

> Cela implique par exemple qu'un candidat n'utilise pas à des fins de communication politique un fichier qui aurait été constitué dans le cadre d'une activité professionnelle distincte.

De la même manière, il est indispensable que seules les informations adéquates, pertinentes et strictement nécessaires au respect des finalités poursuivies soient collectées, conformément au principe de minimisation des données prévu par le RGPD, et que les données ainsi collectées soient conservées pour une durée limitée ainsi que dans des conditions de nature à garantir leur sécurité.

Stockage des données – De même, les systèmes d'informations utilisés pour procéder au stockage de ces données doivent ainsi faire l'objet de mesures particulières correspondant au niveau de risque identifié et des procédés doivent être mis en place afin de pouvoir, par principe et en cas de violation de données, informer sans tarder les personnes concernées et l'autorité de contrôle.

Dans ce contexte, c'est sans doute sur la question du respect des droits des personnes que la nouvelle réglementation renforce de manière conséquente la protection accordée à chaque citoyen.

Obligation d'information – Le responsable de traitement[6] est ainsi désormais tenu à une obligation générale de transparence qui implique qu'une information soit délivrée aux personnes dont les données sont traitées et ce, de façon « concise, transparente, compréhensible, et aisément accessible, en des termes clairs et simples ». Si une information devait déjà être délivrée aux personnes concernées antérieurement au 25 mai 2018 dans le cadre de la mise en œuvre de traitements de données à caractère personnel, c'est désormais plus d'une dizaine d'éléments qui devront être fournis dans le cadre de la mise en œuvre d'un tel traitement.

Collecte directe ou indirecte – Le RGPD effectue par ailleurs une distinction selon que les données à caractère personnel ont été collectées directement ou non auprès de la personne concernée. Dans l'hypothèse où les données n'ont pas été collectées directement auprès de la personne concernée (collecte indirecte), cette dernière doit être informée de la « source » d'où proviennent ces données, c'est-à-dire de leur origine.

En matière de communication politique, ce point revêt une importance particulière dès lors que les usages recensés révèlent que certains acteurs n'hésitent pas à utiliser des données recueillies initialement à d'autres fins, y compris par des tiers.

Si de telles pratiques ne peuvent – par principe – être proscrites, il convient qu'elles soient strictement encadrées afin de ne se développer que dans un cadre qui soit respectueux de la réglementation et qui permette de garantir le droit au respect de la vie privée.

Prospection – Outre les nouveaux droits conférés aux personnes concernées et consacrés par le RGPD (droit à la limitation, à la portabilité, etc.), la nouvelle réglementation contient une disposition spécifique relative aux données à caractère personnel traitées à des fins de prospection. Il est ainsi expressément prévu que la personne concernée est en droit de s'opposer à tout moment au traitement de ces données pour une telle finalité. Une information spécifique doit être délivrée aux personnes concernées dans ce cas de figure dans des conditions de nature à garantir que ces dernières ont été explicitement informées de leur droit d'opposition en matière de prospection. Le RGPD impose à ce titre que la possibilité pour les individus de s'opposer au traitement de leurs données soit présentée « clairement et séparément de toute autre information »[7].
La délivrance de cette information est d'autant plus importante qu'aujourd'hui aucune disposition n'interdit à un parti ou à un candidat de procéder à la location de fichiers auprès de sociétés spécialisées à des fins politiques ; de même qu'aucune obligation légale spécifique n'impose de recueillir le consentement des personnes concernées au traitement de leurs données en matière de prospection politique, contrairement à ce qui existe par exemple en matière de prospection commerciale *via* les dispositions du code des postes et des communications électroniques (CPCE). Historiquement, le recueil d'un tel consentement demeurait néanmoins une bonne pratique encouragée par la CNIL et qui ne pouvait qu'être renforcée par l'étendue des moyens offerts par Internet et les réseaux sociaux.

Il convient par ailleurs de s'interroger sur les conditions de réalisation d'une telle prospection – à partir de fichiers commerciaux par exemple – au regard de l'ensemble des principes tels qu'ils figurent au sein du RGPD, en particulier sur la base légale susceptible d'être mobilisée pour de telles opérations[8].

Bonnes pratiques – Sur ce point, il y a lieu de rappeler que si l'entrée en vigueur du RGPD a conduit à la disparition de la plupart des formalités préalables auprès de la CNIL au profit d'une logique de responsabilisation des acteurs, les différentes formalités simplifiées adoptées antérieurement par la CNIL demeurent un ensemble de bonnes pratiques en termes de protection des données personnelles qui doivent permettre aux différents acteurs de bénéficier d'une base de référence pour la mise en conformité de leurs traitements avec la réglementation applicable en matière de protection des données à caractère personnel.
L'entrée en vigueur du RGPD doit également être l'occasion de clarifier la responsabilité de chacun des acteurs participant à la mise en œuvre de traitements de données à caractère personnel en matière électorale. La responsabilité « conjointe » est en effet désormais expressément prévue. De la même

(6) Défini aux termes de l'art. 4, 7) du RGPD comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».
(7) Droit d'opposition, art. 21 du RGPD.
(8) Par ex., le droit d'opposition préc.

manière, la nouvelle réglementation s'inscrit dans le cadre d'une dynamique de responsabilisation du sous-traitant qui se voit également imposer le respect de certaines obligations, ce dernier participant ainsi pleinement au respect de la réglementation applicable en matière de protection des données à caractère personnel.

■ Ciblage politique des personnes effectué au travers de l'utilisation des réseaux sociaux

Les révélations intervenues l'année passée dans l'affaire *Cambridge Analytica*, mettant en cause Facebook, témoignent des risques qui peuvent être liés à l'usage de technologies particulières dans le cadre du processus électoral.
L'utilisation de données à caractère personnel diffusées sur Internet ou *via* les réseaux sociaux à des fins politiques soulève en effet des enjeux juridiques forts du point de vue de la réglementation relative à la protection des données à caractère personnel s'agissant, en particulier :
- des conditions de licéité de la collecte réalisée ;
- du volume particulièrement important de données qui peuvent être recueillies ;
- ou encore du défaut d'information délivrée aux personnes concernées.

Si la législation européenne est particulièrement stricte quant aux conditions dans lesquelles un traitement de données relatives aux opinions politiques peut être mis en œuvre, les pratiques observées mettent en évidence les progrès qu'il reste à accomplir en la matière.

Sincérité du scrutin – De manière plus générale et au-delà des seuls principes rappelés, les abus constatés dans l'utilisation de données relatives aux opinions politiques sont susceptibles de porter atteinte à d'autres droits fondamentaux et, en particulier, à la sincérité du scrutin qui découle du mésusage lié à l'utilisation de données mises à disposition par les internautes. Outre les enjeux juridiques, c'est donc également des enjeux éthiques dont il est question afin de garantir une loyauté et une transparence dans le traitement de l'information qui s'avèrent indispensables au sein d'une démocratie.

La question du ciblage des personnes concernées au travers de divers contenus mis en ligne met par ailleurs en lumière la problématique de l'exploitation d'informations qui, bien qu'au départ ne renvoyant pas nécessairement à des données « politiques », le deviennent par leur croisement ou leur recoupement avec d'autres informations diffusées sur Internet ou les réseaux sociaux. De la même manière, la personnalisation de contenus en fonction des différentes informations qui peuvent être recueillies sur les sources ouvertes n'est pas sans poser question dès lors que cette personnalisation a pour effet d'orienter l'opinion des personnes concernées.
Dans ce contexte, il convient de faire preuve de la plus grande vigilance dans l'utilisation des informations ainsi collectées et de s'assurer, en tout état de cause, du respect de la réglementation relative à la protection des données à caractère personnel.

Le respect de principes élémentaires doit ainsi être observé : déterminer la base juridique appropriée pour traiter les données sensibles, informer les personnes concernées du traitement de leurs données, ne pas utiliser de sa propre initiative et sans garanties appropriées des données transmises pour une autre finalité, s'assurer que les données collectées sont toujours exactes, s'assurer de l'effectivité des procédures mises en œuvre afin de permettre l'exercice des droits, etc.

■ Vers un règlement sur la protection des données en matière électorale ?

À l'ère du numérique et de l'usage de nombreux médias sociaux en période électorale, garantir la régularité du processus électoral et la sincérité du scrutin constitue un enjeu majeur de souveraineté. À ce titre, il convient de souligner qu'outre l'application des seules dispositions du RGPD, un processus a été engagé au niveau européen – notamment dans la perspective des prochaines élections européennes – afin d'édicter des règles spécifiques pour éviter que des abus ne soient commis dans l'utilisation de données à caractère personnel afin d'influencer ces élections.
C'est en ce sens qu'un projet législatif qui introduirait des sanctions financières pour les fondations et les partis politiques européens qui enfreindraient délibérément les règles de protection des données pour influencer ou tenter d'influencer les résultats des élections européennes est en cours de négociation [9]. L'idée est ainsi de se prémunir contre les campagnes de désinformation éventuelles qui se fondent sur une utilisation abusive des données à caractère personnel des électeurs.

***

L'heure est donc plus que jamais au respect de la réglementation en matière de protection des données à caractère personnel et à l'appel à la vigilance individuelle afin que chacun des acteurs concernés, électeurs, acteurs de la vie politique, autorités de régulation, contribue dans la complémentarité au fonctionnement vertueux du processus électoral.

(9) Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE, Euratom) n° 1141/2014 en ce qui concerne une procédure de vérification relative aux infractions aux règles en matière de protection des données à caractère personnel dans le contexte des élections au Parlement européen (COM (2018) 636, 12 sept. 2018).