JEAN-CHRISTOPHE LUBAC,
avocat associé SCP Sartorio et associés,
spécialiste en droit public, professeur à l'ICH

Nouvelle logique
Le règlement européen sur la protection des données personnelles (RGPD) opère, à compter du 25 mai 2018, un changement de culture en passant du contrôle à la responsabilisation.

Affirmation des droits
Le premier versant de cette révolution culturelle tient dans l'affirmation des droits des personnes physiques relatifs à la protection des données personnelles.

Obligations
La mise en œuvre du RGPD implique également un renforcement des obligations des acteurs privés et publics.

Droits et libertés

Le règlement européen des données personnelles arrive dans les collectivités

« Toute personne a droit à la protection des données à caractère personnel la concernant », déclare l'article 8 §1 de la Charte des droits fondamentaux de l'Union européenne.

Si depuis 1978, la loi informatique et libertés affirmait déjà les grands principes traduisant ce droit, à compter du 25 mai 2018, le règlement européen sur la protection des données personnelles (RGPD) opère un véritable changement de culture en passant d'une logique de contrôle à une logique de responsabilisation des acteurs privés et publics. Cela se traduira par une mise en conformité permanente et dynamique de la part des collectivités.

CHAMP D'APPLICATION

Le RGPD protège les libertés et droits fondamentaux des personnes physiques et en particulier leur droit à la protection des données à caractère personnel. Il s'applique ainsi à tout responsable du traitement, personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données.

Le traitement de données à caractère personnel est défini comme tout traitement automatisé en tout ou partie et appelé à figurer dans un fichier.

Les données personnelles regroupent toutes les informations se rapportant à une personne physique identifiée ou identifiable par un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou des éléments propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Ce traitement doit s'entendre notamment par les opérations telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission de données.

Le profilage de données se définit comme le traitement de données afin d'analyser et de prédire les éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

L'enjeu pour les collectivités est, pour l'essentiel, directement lié au développement de l'e-administration par les téléservices, l'open data, les systèmes d'information géographique, les réseaux sociaux, les compteurs intelligents, ou la lecture automatique de plaques d'immatriculation... Les collectivités doivent s'interroger sur les personnes pouvant accéder à un fichier, la durée de conservation de celui-ci, son utilisation à des fins autres que celles prévues initialement et la pertinence des informations qui y sont contenues, mais aussi sur la protection des fichiers des cyberattaques de plus en plus nombreuses.

L'enjeu se situe également pour les fichiers de ressources humaines, la sécurisation de leurs locaux, le contrôle d'accès par badge, la vidéosurveillance ou la gestion des différents services publics et activités dont elles ont la charge.

Ainsi, un maire ne se servira pas du fichier des inscriptions scolaires pour faire de la communication politique. La liste électorale pourra, en revanche, être utilisée à une telle fin. Seule la mention « personne en fauteuil roulant » sera enregistrée si la précision du handicap n'est pas nécessaire pour assurer une prise en charge adéquate de l'intéressé. Les agents doivent disposer d'un mot de passe individuel régulièrement changé et leurs droits d'accès aux fichiers sont définis en fonction de leurs besoins réels en lien avec l'exercice de leur mission.

DROITS DES PERSONNES PHYSIQUES

Le RGPD précise huit droits qui sont autant d'outils à disposition des citoyens pour protéger leurs données personnelles.

Le premier est le droit d'accès de la personne concernée aux données à caractère personnel détenues, ainsi que les informations relatives à la finalité du traitement,

aux catégories des données personnelles, la durée de conservation définie des données à caractère personnel et les destinataires auxquels les données ont été ou seront communiquées.

Le deuxième tient dans la possibilité de demander la rectification ou l'effacement de données personnelles au responsable du traitement.

Chaque personne physique peut aussi bénéficier de l'effacement des données personnelles, dit «droit à l'oubli», notamment lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées. La personne concernée pourra ainsi retirer son consentement ou s'opposer au traitement.

Le quatrième droit tient dans la possibilité de demander la limitation du traitement des données personnelles qui ne peuvent être traitées qu'avec le consentement de la personne concernée.

Le RGPD crée également le droit à la notification de la rectification ou de l'effacement des données à caractère personnel ainsi que le droit à la portabilité des données à caractère personnel par le responsable du traitement, dans un format structuré couramment utilisé et lisible par une machine. Cela lui permet de les transmettre à un autre responsable du traitement.

Le septième droit est celui du droit d'opposition, à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel y compris un profilage.

Le dernier droit tient dans la possibilité de demander à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques le concernant. Cela implique que la personne concernée a le droit d'obtenir une intervention humaine.

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

PRINCIPES DU TRAITEMENT

Les obligations se fondent sur des principes qui doivent guider le responsable du traitement de données personnelles dans son action.

Le premier principe rappelle que les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Cela implique que ladite personne a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.

RÉFÉRENCE

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).

Ainsi, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.

Néanmoins, les données pourront être traitées sans le consentement si elles remplissent les conditions du principe de finalité, qui implique que les données sont collectées dans un but déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial comme, notamment, l'objectif nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

À NOTER

Le RGPD concerne les fichiers de ressources humaines, la sécurisation de leurs locaux, le contrôle d'accès par badge, la vidéosurveillance ou la gestion des différents services publics.

Le règlement prévoit d'autres objectifs nécessaires:
- à l'exécution d'un contrat auquel la personne concernée est partie;
- au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
- à la sauvegarde des intérêts vitaux de la personne concernée;
- aux fins des intérêts légitimes poursuivis par le responsable du traitement.

RESPONSABLE DE TRAITEMENT

Dans toutes ces hypothèses, le responsable du traitement devra informer la personne physique que son contentement n'est pas requis pour l'un des fondements susévoqués.

Le principe de pertinence implique que seules les données strictement nécessaires à la réalisation de l'objectif poursuivi doivent être collectées.

Le RGPD affirme aussi un principe de durée limitée de conservation des données personnelles au seul temps nécessaire à la réalisation de l'objectif poursuivi. Elles devront, au-delà de cette durée, être détruites ou archivées.

Le dernier principe est celui de la sécurité de traitement de la collectivité qui doit prendre toutes les mesures utiles pour garantir l'intégrité et la confidentialité de ces données en s'assurant que les tiers non autorisés n'y auront pas accès.

Le responsable du traitement de données peut également avoir une obligation de réaliser une étude d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Elle est particulièrement requise en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, le traitement à grande échelle des catégories particulières de données (raciales, éthiques, relevant d'opinions politiques, de convictions religieuses, philosophiques, syndicales, génétiques, biométriques) et, en cas de surveillance systématique, à grande échelle d'une zone accessible au public.

L'analyse contient au moins une description systématique des opérations de traitement envisagées et des finalités du traitement, une évaluation de la nécessité et la proportionnalité des opérations de traitement au regard des finalités, et une évolution des risques pour les droits et libertés des personnes, ainsi que les mesures envisagées pour faire face aux risques.

En cas de risque élevé, le responsable du traitement saisit l'autorité de contrôle pour avis afin de vérifier si le règlement communautaire est bien respecté. Chaque responsable du traitement devra tenir

●○○ un registre des activités effectuées sous sa responsabilité comportant notamment le nom et les coordonnées du responsable du traitement, les finalités du traitement, une description des diverses catégories concernées (personnes, données à caractère personnel, destinataires auxquels les données à caractère personnel ont été ou seront communiquées), les délais prévus pour l'effacement des différentes catégories de données et une description générale des mesures de sécurité techniques et organisationnelles.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

A compter du 25 mai 2018, les collectivités territoriales devront désigner un délégué à la protection des données qui aura pour mission:

- d'informer et de conseiller le responsable de traitement de la collectivité;
- de diffuser une culture «informatique et libertés» au sein de la collectivité;
- de contrôler le respect du règlement et du droit national en matière de protection des données;
- de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution;
- de coopérer avec la Commission nationale de l'informatique et des libertés (Cnil) et d'être le point de contact de celle-ci.

À NOTER

A compter du 25 mai 2018, les collectivités territoriales devront désigner un délégué à la protection des données disposant d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace.

Ce délégué devra disposer d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace, notamment sur les droits et pratiques en matière de protection des données, être associé aux questions «informatique et libertés» et bénéficier de ressources et formations nécessaires pour mener à bien ses missions. Ce délégué peut être partagé entre plusieurs structures de mutualisation informatique ou au sein des EPCI.

L'article 32 du RGPD prévoit également une obligation de sécurisation des données. Il rappelle à cet effet que le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque comme le chiffrement des données à caractère personnel, les moyens garantissant la confidentialité, l'intégrité, la disponibilité des données, les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ainsi qu'une procédure visant à effectuer des tests.

Il devra aussi analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. L'objectif est de se prémunir contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises.

LES SANCTIONS

Le responsable de traitement peut faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement. Les autorités de protection peuvent notamment:

- prononcer un avertissement;
- mettre en demeure l'entreprise;
- limiter temporairement ou définitivement un traitement;
- suspendre les flux de données;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes;
- ordonner la rectification, la limitation ou l'effacement des données.

Les amendes administratives peuvent s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, à 2% et jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

L'article 82 du RGPD prévoit également un droit à réparation et responsabilité en précisant que toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Cette disposition peut se combiner avec celle relative à une action de groupe en matière de protection des données personnelles ayant pour objet de faire cesser les manquements tenant à ce que plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la loi de 1978 par un responsable de traitement de données à caractère personnel ou un sous-traitant.

L'action est engagée par les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel, les associations de défense des consommateurs représentatives au niveau national et notamment les organisations syndicales de fonctionnaires. Cette action de groupe pourrait permettre de lutter contre le traitement des données personnelles qui viendrait porter atteinte à l'identité humaine, aux droits de l'homme, à la vie privée, aux libertés individuelles ou publiques.

Si la Cnil a imposé ce changement de culture en passant d'une logique de contrôle à une logique de responsabilisation des acteurs privés et publics, alors une révolution pourrait bien naître dans les consciences des citoyens qui fournissent gratuitement leurs données personnelles à des algorithmes toujours plus puissants et intrusifs. ●