DONNÉES PERSONNELLES

RGPD et consentement, un malentendu handicapant pour les acteurs publics

Une idée largement répandue voudrait que le nouveau cadre de protection des données personnelles posé par le RGPD implique un recueil, sinon systématique, du moins très fréquent, du consentement des personnes concernées avant de pouvoir mettre en œuvre un traitement. Un présupposé erroné qui peut entraver l'action des personnes publiques.

1 LE CONSENTEMENT, UNE DES SIX BASES JURIDIQUES

Lorsque les acteurs publics décident de réaliser un traitement de données à caractère personnel, celui-ci doit respecter les dispositions relatives à la législation issue du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et au règlement général sur la protection des données (ci-après « RGPD ») du 27 avril 2016.

Pour rappel, un traitement correspond à toute utilisation de données à caractère personnel, tous les procédés étant pris en compte. Pour que ce traitement soit valide, il faut qu'il repose sur une base légale. Cette base légale est le fondement juridique du traitement et conditionne sa licéité.

L'article 6 du RGPD a posé les six bases légales sur lesquelles un traitement peut se fonder. Il s'agit des cas où le traitement est nécessaire au respect d'une obligation légale, à l'exécution d'un contrat, à la sauvegarde d'intérêts vitaux, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, qu'il est justifié par des intérêts légitimes et enfin qu'il repose sur le consentement de la personne concernée.

Le consentement n'est donc qu'un fondement au traitement parmi d'autres. En conséquence, il peut souvent arriver qu'un acteur public telle une collectivité traite des données personnelles sans avoir à recueillir le consentement de ses administrés (pourrait-on imaginer, par exemple, que l'établissement d'un rôle fiscal dépende du bon vouloir des assujettis ?).

Quatre critères fondent le consentement

La Commission nationale de l'informatique et des libertés (Cnil) est venue apporter des précisions sur la notion de consentement, qu'elle définit comme « 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 ». Les quatre critères du consentement (libre, spécifique, éclairé et univoque) sont appréciés très rigoureusement par les agents de la Cnil.

Du traitement spécifique au droit de retrait

Schématiquement, la liberté se définit comme l'absence de contraintes pesant sur la personne dont les données sont collectées. La spécificité suppose que le consentement ne soit pas mélangé entre plusieurs traitements différents. L'aspect éclairé implique que des informations élémentaires sur le traitement soient transmises à la personne avant que celle-ci ne fasse son choix (identité du responsable de traitement, finalités poursuivies, catégories de données collectées, l'existence d'un droit de retrait du consentement par exemple).

La dernière caractéristique, l'aspect univoque, induit la réalisation d'un acte positif clair de la part de la personne concernée.

2 LE RECOURS INAPPROPRIÉ DES ACTEURS PUBLICS À LA NOTION DE CONSENTEMENT

Au moment de l'entrée en vigueur du RGPD, les choses semblaient claires. Les obligations légales, la sauvegarde des intérêts vitaux et l'exécution de missions d'intérêt public ou relevant de l'exercice de l'autorité publique devaient servir de fondement légal aux traitements de données par les acteurs publics alors que l'intérêt légitime et le consentement de la personne devaient être plutôt utilisés par les acteurs privés (l'exécution d'un contrat étant mobilisé indifféremment par les uns et les autres). Toutefois, force est de constater qu'il existe un tropisme des acteurs publics pour le consentement comme base légale du traitement.

Ce tropisme semble tirer son origine dans des pratiques qui sont le reflet de celles des acteurs privés et d'une croyance selon laquelle tout recueil de données à caractère personnel doit forcément découler de l'acceptation de la personne concernée, en particulier depuis l'entrée en vigueur du RGPD. Or, le choix du consentement comme base légale du traitement est peu adapté à la réalité des missions réalisées par les acteurs publics et emporte deux conséquences principales.

Commune, département, bailleur social… des situations ubuesques

La première conséquence est que ce choix peut mener à des situations ubuesques. L'exemple d'un centre de santé public est particulièrement éclairant. Lorsqu'une personne se présente au guichet d'accueil et qu'elle a besoin de soins, lui fournir un formulaire de recueil de consentement peut sembler être une bonne solution pour réaliser une collecte de données légale. Sauf que, comme évoqué précédemment, la Cnil a une conception très rigoureuse de la validité du consentement avec ses quatre caractéristiques.

Si le centre de santé fonde sa collecte de données nécessaires aux soins sur le recueil du consentement et que la personne refuse, il ne sera pas possible de disposer d'informations élémentaires (groupe sanguin, allergies par exemple) permettant de réaliser les prestations de soin.

Par ailleurs, si le recueil de données conditionne la prise en charge de la personne, la question du consentement n'est plus réellement « acceptez-vous expressément que vos données soient collectées par le centre de soins ? » mais plutôt « voulez-vous être soigné ? Auquel cas, il faut consentir à la transmission de vos données ». Dans cette situation, le consentement qui a été obtenu ne pourra valablement être considéré comme libre même s'il était éclairé, univoque et spécifiquement donné pour le traitement.

En fin de compte, pour les acteurs publics, cet exemple est reproductible à l'infini. Pour les bailleurs sociaux, fonder l'attribution de logements sur le consentement à la collecte de données ne pourrait pas fonctionner car le consentement ne serait pas libre. Pour les communes, la situation serait identique, par exemple, pour ses missions d'accompagnement scolaire et périscolaire. Pour les départements, il en irait de même pour ses missions sociales. Ces situations aberrantes pourraient entraver le bon fonctionnement de leurs services en empêchant la collecte valide des données qui en sont le support indispensable.

Si un centre de santé public fonde sa collecte de données nécessaires aux soins sur le consentement et que la personne refuse, il ne sera pas possible… de la soigner.

Prouver… et documenter

La seconde conséquence est que le choix du consentement impose de lourdes formalités. Dès lors qu'il est décidé de fonder un traitement sur cette base légale, cela va rajouter une charge de travail supplémentaire au personnel administratif en plus de celui pesant sur le délégué à la protection des données. En effet, outre la préparation du recueil de consentement et des mentions d'information qui se doivent d'être particulièrement précises et adaptées, le consentement nécessite d'être prouvé et documenté. Tout responsable de traitement doit être en mesure de démontrer à tout moment que la personne a bien consenti au traitement, dans des conditions valides, et il doit documenter les conditions de recueil du consentement.

A l'inverse, lorsqu'un traitement est fondé sur l'obligation légale ou l'exécution de missions d'intérêt public, les obligations de preuve et documentation peuvent paraître moins lourdes puisque plus évidentes ; personne ne peut sérieusement contester les obligations incombant à une commune de collecter des données pour la gestion de l'état civil, par exemple.

Le consentement en dernier recours

Le choix du consentement comme base légale des traitements de données à caractère personnel présente de nombreux inconvénients, en plus de présenter des risques juridiques en matière de protection des données. Il s'agit d'un écueil dans lequel les acteurs publics ne doivent pas tomber d'autant que de nombreux moyens ont été mis à leur disposition pour réaliser leurs missions. En définitive, les acteurs publics ne doivent recourir au consentement des personnes concernées qu'en dernier recours, lorsqu'aucun des cinq autres fondements à leur disposition n'est applicable en l'espèce.

Par David Conerardy et Aloïs Ramel, avocats à la cour, SCP Seban et associés

RÉFÉRENCES

- 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
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles