Premières mises en demeure de la CNIL en application du RGPD, quels enseignements peut-on en tirer ?

Categories : RGPD

Date : mardi 27 novembre 2018

Depuis l'entrée en vigueur du RGPD en mai 2018, plusieurs décisions ont été rendues par la CNIL sous l'empire de l'ancienne loi.

Leur analyse met en particulier en avant le fait que les manquements les plus fréquents concernent :

- la licéité des traitements de données personnelles illicites (données non minimisées, finalités détournées, défaut de consentement de la personne concernées),
- l'obligation d'information des personnes et l'obligation de sécurité (confidentialité des données).

Dans ces affaires, la CNIL a porté le montant des amendes entre 10 et 50K€ et accordé des délais de mise en conformité entre 1 et 3 mois. D'une manière générale, la CNIL décide de rendre publiques ses décisions en fonction de la gravité de l'atteinte, du nombre de personnes concernées et dans une volonté pédagogique de sensibiliser les acteurs du traitement de données personnelles.

Ceci étant, les premières décisions rendues sous l'empire du RGPD étaient attendues. Des amendes rendues publiques, qui permettraient d'apprécier la façon dont la CNIL va appliquer les montants prévus de 10 à 20 millions d'€ ou 2 à 4% du Chiffre d'affaires, n'ont pas encore été prononcées. En revanche, la CNIL a fait paraître deux mises en demeure déjà riches d'enseignements pratiques et concrets pour la mise en application du RGPD par les entreprises.

Les deux affaires portant sur le même type de traitements et ayant en commun plusieurs manquements, il est intéressant de les analyser conjointement.

Les affaires SingleSpot et Vectaury – Mises en demeure des 8 et 30 octobre 2018

La CNIL a contrôlé la société SINGLESPOT et la société VECTAURY qui utilisent des technologies permettant de collecter des données personnelles via smartphones et de réaliser des campagnes publicitaires sur les mobiles. Ces sociétés ont recours à des outils techniques dénommés « SDK » intégrés dans le code d'applications mobiles de leurs partenaires qui leur permettent de collecter les données des utilisateurs des smartphones (identifiant publicitaire des smartphones et données de géolocalisation des personnes, soit à des périodes de temps fixe (toutes les cinq minutes), soit

selon la distance parcourue (tous les deux cents mètres) même lorsque ces applications ne sont pas en fonctionnement. Ces données sont ensuite croisées avec des points d'intérêts déterminés par les partenaires (enseignes de magasins).

Les finalités de ces traitements concernent donc l'affichage de publicité ciblée sur les smartphones des personnes à partir des lieux qu'elles ont visités ainsi que l'établissement de profils commerciaux.

Plusieurs manquements ont été constatés par la CNIL qui a demandé pour une mise en conformité que soient prises sous 3 mois les mesures suivantes :

- Recueil du consentement effectif de tous les utilisateurs concernés,
- Mise en place des mesures de sécurité
- Suppression des données indûment collectées.

Vu le nombre de données concernées, (ayant notamment justifié les publications des mises en demeure, soit plus de 14 millions pour SingleSpot et plus de 47 millions pour Vectaury, il est évident que l'obligation de supprimer les données collectées illicitement aura un impact majeur sur le business model des entreprises.

Ce qu'on peut retenir de ces décisions, en pratique

- La CNIL considère que la collecte de données de géolocalisation constitue un risque particulier pour la vie privée puisque les données sont révélatrices des déplacements des personnes et de leurs habitudes de vie.

- Plusieurs critères ont été retenus par la CNIL pour confirmer la qualité de responsable de traitement, avec la détermination dans une large mesure des finalités et moyens des traitements :

- une déclaration préalable du traitement (si l'on se considère soit même comme responsable, il est difficile d'affirmer le contraire par la suite)

- un traitement pour son propre compte des données personnelles collectées pour vendre des services d'analyse ou de profilage à ses clients annonceurs (si les données sont exploitées pour une finalité répondant au besoin de l'entreprise elle-même, elle ne pourra être considérée comme sous-traitant)

- une intégration des données collectées via les différentes applications mobiles des annonceurs dans la même base de données (si les données avaient été répertoriées dans des bases différentes pour chaque annonceur, le traitement aurait peut-être pu être jugé comme destiné aux annonceurs et non à l'entreprise).

- Pour recueillir un consentement licite et remplir l'obligation d'information, encore faut-il :

- communiquer une information suffisante aux utilisateurs des applications avant la collecte et le traitement des données (la seule présence d'informations dans des CGU, CGV ou politique de confidentialité ne suffit pas) : qui est responsable de traitement, quelles données sont collectées, pour quelles finalités

- ne pas activer la collecte des données par défaut

- permettre à l'utilisateur de télécharger l'application mobile sans activer le « SDK » (donc sans collecter et transmettre ses données personnelles de manière automatique) et de refuser la collecte de certaines données pour certaines finalités

- demander (et obtenir) un consentement pour chacune des finalités distinctes (collecte des données de géolocalisation pour les finalités de fonctionnalités de l'application d'abord, de l'affichage publicitaire ensuite, de la constitution de profils commerciaux enfin.

La CNIL recommande d'obtenir un consentement préalable au traitement par exemple par la mise en place d'un pop-up contenant une information suffisante et une case à cocher dédiées ou un bouton de refus

- L'absence d'information des personnes concernées entraîne automatiquement un manquement à l'obligation de permettre l'exercice de leurs droits : si les traitements sont opérés sans que les personnes concernées n'en soient conscientes, elles ne peuvent exercer les droits prévus par le RGPD.

- Une durée de conservation proportionnée à la finalité du traitement doit être définie (en l'occurrence la CNIL a constaté que les données étaient conservées plusieurs mois après la fin du projet de l'annonceur concernant ces données.

Ici la CNIL recommande de supprimer les données de géolocalisation des utilisateurs collectées en

dehors des zones de points d'intérêt une fois la correspondance entre les données de géolocalisation et les zones de points d'intérêt effectuée. Elle rappelle aussi la possibilité de ne pas supprimer mais anonymiser les données anciennes.

- Concernant le manquement à l'obligation d'assurer la sécurité et la confidentialité la CNIL recommande que les mots de passe soient stockés sous une forme hachée (par exemple, à l'aide de l'algorithme SHA256 avec l'utilisation d'un sel) et que le compte administrateur permettant d'accéder à la base de données soit soumis à une politique contraignante de mot de passe.

Il s'agit, pour les comptes accédant aux bases de données ou à leurs plateformes d'administration d'adopter :

- soit des mots de passe composés d'au minimum 12 caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial

- soit des mots de passe composés d'au moins 8 caractères, contenant 3 des 4 catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et accompagnés d'une mesure complémentaire, telles que la temporisation d'accès au compte après plusieurs échecs, la suspension temporaire de l'accès dont la durée augmente à mesure des tentatives, la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum 10).

Pour préserver la sécurité des données, la CNIL rappelle également qu'utiliser des données réelles pour les phases de développement et de test présente un risque pour celles-ci, notamment en cas de perte, de modification non autorisée, d'erreur ou d'accès par des personnes non autorisées et que les équipes de développement n'ont pas nécessairement à connaître des données issues de la base de données de production et, dans l'hypothèse où des données réelles seraient néanmoins requises, celles-ci devraient être anonymisées.

Elle demande ainsi que soit mise en œuvre une politique de séparation entre les environnements de tests de développement (ou de recette) et les environnements de production.

Il est louable de constater que la CNIL abreuve ses décisions d'informations pragmatiques pour une bonne mise en application de la Réglementation, avec des exemples pratiques

parfaitement applicables par les autres acteurs des traitements de données personnelles.

Les suites qui seront données à ces affaires (clôtures ou sanctions) seront quant à elles certainement enrichissantes pour apprécier la tendance de la CNIL d'une application dure ou souple du RGPD, notamment sur le chiffrage d'éventuelles amendes.

Pour ne pas manquer la suite des évènements et la publication de nouvelles décisions de la CNIL, suivez notre fil d'actualité RGPD en cliquant ICI