Qui collecte moins collecte mieux : le principe de minimisation des données

les faits **Une société de maintenance informatique avait équipé ses véhicules d'un dispositif de géolocalisation permettant de collecter diverses données relatives aux incidents de conduite, aux horaires de ses techniciens et de mieux planifier leurs interventions. La CNIL l'a mise en demeure de cesser tout traitement des données issues de cet outil, aux fins de contrôle du temps de travail de ses salariés.**

Le Conseil d'État, alors saisi d'une demande d'annulation de cette décision, a rejeté le 15 décembre dernier la requête de la société en se fondant notamment sur l'article 6-3° de la loi Informatique et Liberté, repris quasiment à l'identique par le Règlement européen sur la protection des données (RGPD), qui impose également le respect du principe de minimisation des données.

Ainsi, pour être licite, le traitement doit porter sur des données « *adéquates, pertinentes et non excessives* », c'est-à-dire limitées à ce qui est strictement nécessaire au regard de la finalité pour laquelle elles sont traitées. Suivant ce principe, certaines données à caractère personnel ne doivent être collectées que si la finalité du traitement envisagé ne peut pas être atteinte par d'autres moyens, fussent-ils moins efficaces. Dans cette affaire, le Conseil d'État a estimé que la collecte et l'utilisation par la société des données issues de son outil de géolocalisation, afin d'assurer le contrôle de la durée de travail de ses salariés, étaient excessifs, la société disposant d'autres moyens et notamment de documents déclaratifs, pour assurer ce contrôle. Si la CNIL proscrit en conséquence à cette société tout usage de son système de géolocalisation pour contrôler

Me Pierre-Randolph Dufau
Avocat à la cour
Fondateur de la SELAS
PRD avocats

les horaires de travail de ses employés, elle ne lui interdit toutefois pas de traiter ces données pour d'autres finalités comme la facturation de ses prestations à ses clients.

Appliqué à tout type de traitement, il convient d'anticiper le principe de minimisation des données dès la conception de nouveaux services. À titre d'exemple, il incombe au responsable du traitement de s'assurer qu'un formulaire en ligne destiné à proposer des devis gratuits ou participer à un jeu-concours ne recueille que l'identité et les coordonnées de l'internaute, à l'exclusion de tout champ supplémentaire (carte bancaire, sexe etc.), même facultatif, et ce afin d'éviter d'obtenir plus de données que nécessaire. Ce principe de minimisation, qui s'entrechoque avec la logique même du big data, ne s'applique pas seulement à la quantité de données collectées, mais aussi à leur durée de conservation et à leur accessibilité. Il appartient aux entreprises de veiller à ce que les données ne soient accessibles qu'aux personnes qui en ont strictement besoin pour mettre en œuvre le traitement et conservées pour une durée n'excédant pas celle raisonnablement nécessaire au regard de sa finalité. De stricts délais de conservation doivent ainsi être fixés, associés à des processus automatisés d'accessibilité, de traçabilité et de sécurité pour chaque traitement. ■

ce qu'il faut retenir **La collecte de données personnelles, même effectuée dans le respect des obligations légales d'informations et avec le consentement de la personne concernée, se doit d'être limitée et proportionnée. Une véritable politique de sélection, d'utilisation, de conservation, d'archivage et de purge des données doit en outre être élaborée et documentée.**

Darty sanctionné pour atteinte à la sécurité de ses données clients

Une défaillance permettait l'accès à l'ensemble des réclamations renseignées via un formulaire en ligne de service après-vente, développé par un prestataire. Dans sa décision du 8 janvier 2018, la CNIL a considéré que le fait que Darty fasse appel à un sous-traitant ne l'exonérait pas, en tant que responsable de traitement, de son obligation de vérifier régulièrement et de préserver la sécurité des données. Elle l'a donc condamné à 100 000 € d'amende.

Informations privées et preuves aux prud'hommes

Le 20 décembre 2017, la Cour de cassation a confirmé la condamnation d'un employeur qui avait présenté comme preuve contre un salarié des informations extraites de son compte Facebook obtenues à partir du smartphone professionnel d'un autre salarié. L'accès à ces informations, bien que recueillies au moyen d'un téléphone professionnel, était restreint aux seuls « amis » Facebook du salarié, leur conférant ainsi un caractère privé.

Obsolescence programmée : ouverture d'une enquête contre un fabricant d'imprimantes

Le parquet de Nanterre a ouvert une enquête préliminaire contre un acteur majeur du marché de l'imprimante à la suite d'une plainte déposée le 18 septembre dernier par l'association HOP (Halte à l'obsolescence programmée). Ce délit, inscrit dans le Code de la consommation depuis juillet 2015, condamne les techniques visant à réduire la durée de vie d'un produit. L'enquête a ainsi été confiée à la DGCCRF.