Protection des données personnelles

Les gestionnaires de flotte doivent s'imprégner de l'esprit du nouveau texte

Le 25 mai prochain, le RGPD (ou GDPR), nouveau règlement européen sur la protection des données personnelles, entrera en vigueur. Un dispositif que les gestionnaires de parc doivent comprendre afin de procéder à d'éventuels ajustements dans leurs pratiques quant à la gestion des données personnelles des conducteurs... Le prix de la sérénité, selon l'avocat spécialisé Hervé Gabadou.

Hervé Gabadou
est avocat inscrit au barreau de Paris depuis 1987 et spécialisé en droit de l'informatique et du numérique depuis 1990.

FleetMag : Le RGPD entre en vigueur le 25 mai prochain. Les gestionnaires de flottes automobiles ont-ils des raisons de s'en préoccuper ?

Hervé Gabadou, avocat à la cour, SEA-Avocats : Absolument. La philosophie générale du texte est de replacer la protection de la vie privée et donc des données personnelles au centre du jeu. Concrètement, cela signifie qu'à partir de l'entrée en vigueur du RGPD, toute entreprise devra être capable de démontrer qu'elle a mis cette protection au cœur de ses préoccupations.

Avec une déclaration à la CNIL ?

H. G. : Elle disparaît, et avec, le contrôle a priori. La situation antérieure qui se caractérisait par un manque de sanctions visibles risquait de laisser se développer un sentiment d'impunité « pas vu pas pris ».

Désormais, il va falloir être beaucoup plus précis dans l'information fournie aux individus concernés, documenter les processus pour démontrer le souci permanent de protection des données personnelles y compris, le cas échéant, à travers des études d'impact. Et surtout, demander la plupart du temps aux individus concernés, ici les conducteurs des véhicules de fonction ou de société, leur consentement explicite pour l'usage qui sera fait de leurs données.
Prenons un exemple : si l'entreprise décide d'utiliser des données remontées des boîtiers télématiques installés dans les véhicules de sa flotte pour effectuer des traitements statistiques de type Big Data, elle doit le prévoir dans le contrat signé avec le conducteur et lui expliquer notamment quels objectifs sont poursuivis.

Même si ces données sont anonymisées ?

H. G. : L'anonymisation est en soi un traitement de données personnelles. Il faut être absolument certain qu'il ne sera plus possible de remonter aux individus à partir des données ainsi dépersonnalisées. La CNIL a autorité pour valider les méthodes utilisées et permettre le traitement de ces données. Il existe pour cela des référentiels.
Sur ce point comme sur beaucoup d'autres, il faut que les acteurs de l'entreprise changent de prisme pour passer, chacun dans son propre domaine, à une logique de responsabilisation. Il ne s'agira plus, demain, de s'excuser parce que des données mal protégées se sont égarées dans la nature ou que les processus mis en place dans l'entreprise ne permettent pas aux individus d'exercer leurs nouveaux droits. Les sanctions prévues sont d'ailleurs particulièrement lourdes, pouvant aller jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise en faute.

Il y a là de quoi effrayer les responsables. Et leur faire croire que plus rien n'est possible, à moins de se lancer dans des montages techniques et juridiques compliqués ?

H. G. : N'exagérons pas. Il reste des latitudes et puis, bien compris, le RGPD est plutôt un facteur d'

lération de la transformation numérique des entreprises. Par exemple, les données recueillies dans le cadre de l'exécution d'un contrat sont réputées, d'une certaine manière, avoir fait l'objet d'un consentement implicite de l'utilisateur – à condition que l'entreprise n'en profite pas pour les utiliser à d'autres fins, par exemple publicitaires. Concernant un véhicule loué, les données permettant un bon entretien préventif du véhicule sont éligibles à cette notion. De même, la CNIL a depuis longtemps considéré que le recueil des informations de géolocalisation sur une flotte de véhicules utilitaires était licite dans la mesure où elles servent exclusivement à optimiser les délais et les frais de livraison, la sécurité des conducteurs et celle des véhicules, ou encore à contrôler le respect des règles d'utilisation du véhicule définies par l'employeur.

Quels conseils donneriez-vous aujourd'hui à un gestionnaire de flotte soucieux de se mettre en conformité ?

H. G. : Il pourrait commencer par s'interroger sur la nature des données qu'il recueille déjà ou souhaiterait recueillir, puis vérifier que ce recueil a fait l'objet d'un accord de la part des conducteurs. Le cas échéant, il devra éventuellement revenir vers eux pour leur faire signer une clause spécifique et explicite. Il pourrait également se demander si les données recueillies sont toutes nécessaires et indispensables aux traitements qu'il souhaite faire. Ce sont les principes de proportionnalité et de minimisation.
Sur le plan technique, il aura également intérêt à vérifier que les logiciels qu'il utilise – ceux du marché comme ceux développés en interne – sont suffisamment résistants à d'éventuelles attaques, et qu'ils sont conçus dès l'origine en tenant compte de la protection des données et de la vie privée. Leurs spécifications doivent pouvoir le démontrer.
Enfin, s'il a recours à des sous-traitants, par exemple un spécialiste de la location longue durée, il doit analyser les flux de données personnelles qui peuvent circuler pour que la sécurité des données soit maîtrisée de bout en bout. Le RGPD établit à cet égard un nouveau principe de responsabilité légale, et non plus seulement contractuelle, sur la tête du sous-traitant.

Y a-t-il de quoi craindre des retards dans la mise en œuvre du dispositif ?

H. G. : Je vais vous rassurer un peu. Il y a certes la date butoir du 25 mai et il s'agit d'un règlement européen qui devrait s'appliquer immédiatement. Sauf que, et je ne rentrerai pas trop dans les détails, il va tout de même y avoir un temps d'ajustement du fait des ouvertures qui sont laissées aux législateurs nationaux.
Deuxième point, la CNIL ne cherche pas à sanctionner mais plutôt à évangéliser. Tout dépendra en réalité de la nature des données collectées et de la finalité réelle de leur traitement. Si les données collectées (informations de conduite) se justifient par le but poursuivi (entretien personnalisé du véhicule) et que cela peut être démontré, alors tout va bien. C'est le détournement de ce but qui pourrait poser problème. Mon conseil est donc le suivant : mettez-vous au travail sans plus tarder, pour bien vous imprégner de l'esprit du nouveau texte. Et si vous avez, le 25 mai prochain, fait une grande partie du travail et que vous êtes surtout en capacité de le démontrer, vous ne devriez pas être inquiétés prioritairement. ■

Les 6 grands principes du RGPD appliqués à la gestion d'une flotte automobile

Le principe de transparence et de consentement
Les personnes (ici les conducteurs) doivent donner leur accord explicite à l'usage qui sera fait de leurs données personnelles, lequel doit leur être expliqué avec précision et transparence

Les principes de proportionnalité et de minimisation
Une donnée personnelle ne peut être collectée que pour une finalité précise et légale. La donnée doit donc être pertinente et indispensable au traitement. Il faut donc pouvoir la supprimer quand elle ne l'est plus.

Principe de sécurité
Le responsable du traitement des données est tenu d'informer la CNIL (dans les 72 heures) et le cas échéant, les personnes concernées en cas de violation de leurs données personnelles. S'il est en retard, il faudra qu'il en explique la raison. Les incidents n'arrivent pas qu'aux autres. Il faut s'y préparer.

Principe du « Privacy by design »
Ce principe consiste à mettre en place des dispositifs de protection de la vie privée et des données personnelles au stade de la conception d'un outil de gestion de flotte. La démarche de « Privacy by design » introduite par le RGPD donne également obligation de sécurité et d'intégrité des données consubstantielle à leur outil de traitement. Un principe à prendre en compte avant de choisir les outils qui les manipulent, par exemple les logiciels de gestion de flotte.

Principe de conservation limitée
Le règlement interdit, comme par le passé, de conserver indéfiniment les données personnelles. La durée de conservation choisie doit être justifiée par la finalité du traitement.

Principe « d'Empowerment »
Les personnes dont les données personnelles ont été collectées disposent de droits accrus : accès à une information plus complète, rectification, effacement, verrouillage, portabilité, etc.

Principe de responsabilisation
À ne pas confondre avec responsabilité. Le responsable de traitement et le sous-traitant, sur le périmètre qui lui a été sous-traité, seront comptables du respect du RGPD. Il faudra donc qu'ils puissent chacun en faire la démonstration.