Hertz fait les frais de la loi Lemaire : 40 000 euros d'amende

Deux poids, deux mesures ? Non, plutôt les effets de l'entrée en application de la loi Lemaire, qui a renforcé les sanctions à l'encontre des entreprises qui ne sécurisent pas suffisamment les données personnelles de leurs clients. Hier, le site d'autopartage Ouicar recevait de la part de la CNIL un simple avertissement public malgré des erreurs de sécurité grossières, exposant les données de plusieurs centaines de milliers de personnes. Aujourd'hui, c'est le loueur de véhicules Hertz qui est sanctionné par cette même Commission de 40 000 euros d'amende pour un défaut de sécurisation des données des adhérents à son programme de fidélité.

Si la faille de sécurité chez Hertz – qui résulte d'une erreur d'un sous-traitant lors d'un changement de serveur – apparaît moins sévère que celle de Ouicar, la loi pour une République numérique est entretemps passée par là. « *C'est la première fois qu'une sanction pécuniaire est prononcée pour une violation de données sous l'empire de la loi pour une République numérique entrée en vigueur en novembre 2016. Avant cette loi, seul un avertissement pouvait être décidé dans un tel cas* », écrit la CNIL.

Hertz sanctionné et non son sous-traitant

L'affaire Hertz remonte au 15 octobre dernier quand la CNIL est alertée par nos confrères de *Zataz.com* (également à l'origine de la découverte des failles de Ouicar) d'un bug dans l'application Cartereduction-hertz.com. L'URL de création de cartes permettait d'accéder, adhérent par adhérent, aux noms, prénoms, dates de naissance, adresses postales, mails et numéros de permis de conduire des membres de ce programme. « *La délégation a ainsi pu accéder aux données à caractère personnel de 35 327 personnes* », écrit la CNIL dans sa délibération du 18 juillet. Résultant de la suppression involontaire d'une ligne de code en juin 2016 par un sous-traitant de Hertz, la faille est rapidement corrigée. Et le sous-traitant assure, sur la base d'une analyse des logs du serveur, qu'aucun téléchargement massif de données n'a eu lieu.

Malgré ces éléments rassurants et un audit rapidement commandé par Hertz sur la sécurité de son sous-traitant, la Commission a bien décidé de sanctionner financièrement le loueur de véhicules – et non son prestataire -, considérant que « *la violation de données résulte d'une négligence de la société dans la surveillance des actions de son sous-traitant* ». En particulier, la formation restreinte de la CNIL critique l'absence de cahier des charges rédigé par Hertz pour le développement du site et le fait que la société n'ait pas vérifié que la mise en production avait été précédée d'un protocole complet de test, alors qu'il s'agissait d'une opération touchant aux serveurs communiquant avec le prestataire de paiement. Soit un pan sensible de l'application.

L'épée de Damoclès du GDPR

Même si la CNIL relève « *la grande réactivité de la société* », elle n'en a pas moins décidé de rendre publique la sanction, « *au regard du contexte actuel dans lequel se multiplient les incidents de sécurité* ». Notons enfin que, pour sa défense, Hertz n'a pas cherché à se cacher derrière son petit doigt.

Contrairement à OuiCar qui, pour se dédouaner, a tenté de faire avaler à la CNIL que l'alerte donnée par nos confrères de *Zataz.com* « *avait un caractère frauduleux dès lors que ce dernier ne bénéficie pas du statut protecteur des lanceurs d'alerte* », comme le montre la délibération de la formation restreinte de la CNIL datant du 20 juillet.

Un argument rapidement balayé par la Commission, qui semble bien décidée à utiliser l'arme de la sanction pour pousser les entreprises à être plus rigoureuses dans la protection des données personnelles de leurs clients ou employés. Et l'entrée en vigueur du GDPR en mai prochain – règlement européen qui prévoit un nouveau renforcement des sanctions financières (4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros) – lui fournira bientôt des munitions supplémentaires.

A lire aussi :

CNIL : Facebook écope d'une amende symbolique de 150 000 euros