Allocab sanctionnée par la CNIL

L'entreprise de transport de particuliers avait été mise en demeure par la Cnil en novembre 2015 à la suite d'une plainte d'un de ses clients. Il lui était notamment reproché de ne pas assurer la sécurité des données de ses clients et de conserver les données relatives aux cryptogrammes des cartes bancaires au-delà du temps nécessaire à la transaction. Ne s'étant pas mise en conformité dans le délai imparti, Allocab a été condamnée, le 13 avril dernier, à une amende de 15 000 euros.

Bilan 2016 de la CNIL

La CNIL relève qu'elle a reçu 7 703 plaintes, ayant permis d'initier 15 % des 430 contrôles effectués en 2016, tant sur place, sur convocation qu'en ligne. Ces plaintes proviennent à la fois d'employés, de citoyens ou de clients, et visent majoritairement la diffusion de données personnelles sur Internet (sites, blogs, réseaux sociaux), la prospection ou la vidéosurveillance. De nouvelles tendances à surveiller ont également été identifiées, comme les objets connectés ou le Wi-Fi tracking.

Condamnation d'un forum en ligne

Par un arrêt du 22 mars 2017, la Cour d'appel de Montpellier a condamné la société éditrice d'un site internet pour avoir maintenu pendant 18 mois sur son forum de discussion des informations permettant d'identifier une personne qui s'exprimait de façon anonyme. Alors que des internautes avaient révélé son identité et divulguaient des informations malveillantes et diffamatoires touchant à sa vie privée, le site, qui disposait d'un modérateur, n'avait pas fait droit à sa demande de suppression.

Le rôle stratégique du délégué à la protection des données créé par le RGPD

LES FAITS

La création de la fonction de délégué à la protection des données (Data Protection Officier en anglais « DPO ») est au cœur du Règlement général de protection des données européen (RGPD) qui sera applicable dans tous les États membres d'ici un an, le 25 mai 2018. Les lignes directrices adoptées par le G29 dans leur version définitive le 5 avril 2017 clarifient ce nouveau cadre juridique.

Me PIERRE-RANDOLPH **DUFAU**

- **AVOCAT À LA COUR**
  Fondateur de la SELAS PRD avocats

En France, le DPO sera le naturel successeur de l'actuel Correspondant Informatique et Libertés (CIL). S'agissant de sa désignation, fini le seuil de 50 personnes. Elle sera obligatoire dans le secteur public, à l'exception des juridictions, quelle que soit la nature du traitement, comme pour les organismes privés, dès lors que les entreprises font des traitements à grande échelle de suivi régulier et systématique des personnes ou de données sensibles (religion, condamnations, santé, etc.). En dehors de ces cas, le G29 encourage fortement la désignation volontaire d'un DPO qui emportera sa soumission aux dispositions règlementaires le concernant. Le DPO sera le chef d'orchestre de la conformité des dispositifs internes au RGPD. À ce titre, il devra assister le responsable du traitement voire le sous-traitant, les conseiller, et émettre des recommandations sur toutes les problématiques liées à la protection des données à caractère personnel. Dans l'accomplissement de ses missions, le DPO appréciera les opérations de traitement eu égard aux risques associés à leurs nature, portée, contexte et finalités. Il réalisera à ce titre des analyses d'impact préalablement à la mise en œuvre d'un traitement, en se prononçant sur la méthodologie, les mesures de sécurité et de protection à mettre en place à l'aulne des risques encourus. Le Règlement exclut expressément la responsabilité personnelle du DPO en cas de non-conformité, qui pèse uniquement par principe sur le responsable du traitement. Il appartiendra aussi au DPO de contrôler l'application concrète des règles régissant la matière, en particulier à l'occasion d'audits. Sa mission sera facilitée par une coopération régulière avec l'autorité de contrôle. À la différence du CIL, le DPO n'est pas nécessairement un employé de l'organisme, il peut être externalisé (il peut s'agir par exemple d'un avocat), voire être mutualisé au sein d'un groupe d'entreprises, à condition de démontrer qu'il peut se rendre aisément disponible. En effet, le DPO doit être en mesure de communiquer facilement avec les personnes concernées, lesquelles doivent le soutenir dans sa mission. Son autonomie devra être garantie par une mise à disposition des moyens matériels nécessaires à la réalisation de sa mission. Ainsi, son rôle et ses missions en font le pivot dans la mise en place des principales dispositions novatrices du Règlement. À la fois facilitateur, contrôleur et conseil, son profil exige de fortes connaissances juridiques et techniques ainsi qu'une implication au niveau le plus élevé dans la structure qui l'a nommé. Précisons qu'en cas de non-respect de cette réglementation, les sanctions sont lourdes, celles-ci pouvant aller jusqu'à 10 M€ ou, pour les entreprises, à 2 % du chiffre d'affaires annuel mondial.

CE QU'IL FAUT RETENIR

À la lumière des lignes directrices du G29, nul doute que le DPO a vocation à occuper une place centrale au sein des organismes et entreprises et qu'il sera doté de moyens et de garanties bien supérieurs à ceux dont les CIL disposent aujourd'hui. Obligatoire dès mai 2018, il convient donc d'anticiper dès à présent leur arrivée.