Sanctions CNIL 2020 : enseignements à retenir pour les TPE-PME

PAR **ALEXANDRA DECAUDIN**, JURISTE, CONSEIL SUPÉRIEUR

En 2020, la CNIL a condamné en France 11 entreprises au paiement d'une amende pour des manquements au RGPD[1].

QUELLES LEÇONS PEUT-ON TIRER DE CES SANCTIONS ?

En premier lieu, le contrôle et la sanction de la CNIL interviennent très souvent à la suite d'une plainte déposée par une personne physique dont les données personnelles ont été utilisées. Les sanctions ont été prononcées généralement entre 15 et 18 mois après les premiers contrôles diligentés après réception de plaintes.

En second lieu, la CNIL tient compte de plusieurs critères pour déterminer le montant de l'amende : la taille de l'entreprise, le nombre d'infractions et leur gravité, le nombre de personnes concernées par la violation de leurs données personnelles et les efforts de régularisation de l'entreprise à la suite de l'enquête de la CNIL.

Par exemple, *Carrefour France s'est vu infliger une amende de 2,25 millions euros[2] et sa filiale Carrefour banque une amende de 800 000[3] euros pour des manquements notamment à l'information délivrée aux personnes et au respect de leurs droits, tandis que la société Performeclic, une TPE dont l'activité consiste à envoyer des messages à des fins de prospection pour le compte d'annonceurs, a été condamnée à une amende de 7 300 euros[4] pour avoir adressé des courriels de prospection commerciale sans preuve du consentement préalable des personnes.*

En troisième lieu, de nombreuses décisions concernent le défaut d'information des personnes concernées sur la collecte de leurs données et l'exercice de leurs droits. Souvent, les informations fournies sont considérées comme incomplètes (informations manquantes dans la politique de confidentialité sur le web) ou inexistantes (lors de la création d'un compte sur une application mobile)[5].

En quatrième lieu, un certain nombre de décisions portent sur le manquement aux obligations de sécurité des données personnelles collectées.

Par exemple, *une société a été sanctionnée notamment pour ne pas avoir imposé aux internautes un mot de passe assez robuste[6]. Deux médecins ont été condamnés pour ne pas avoir veillé à ce que les données personnelles de leurs patients ne soient pas librement accessibles en ligne en raison d'une mauvaise configuration de leur box Internet et d'un mauvais paramétrage de leur logiciel d'imagerie médicale. Il leur a également été reproché de ne pas crypter systématiquement les données personnelles hébergées sur leurs serveurs. Ils ont enfin omis de notifier les violations de données à la CNIL, après avoir constaté que l'imagerie médicale était librement accessible en ligne. Ils ont été condamnés respectivement à une amende de 3 000[7] € et de 6 000 €[8].*

Les enseignements à tirer de ces décisions pour les cabinets d'expertise comptable :

- Il faut toujours informer sur la collecte des données réalisée par le cabinet et être transparent sur ses finalités et ses modalités ;
- il faut appliquer des règles de conservation des données préalablement définies par le cabinet (les plus courtes possibles dans le temps au regard de la finalité du traitement) et supprimer ou archiver les données, si nécessaire, à l'expiration du délai de conservation ;
- il faut garder toujours une trace des consentements obtenus et, au minimum, des exemples de procédures de collecte de consentements qui vous serviront de preuves ;
- il ne faut pas collecter plus de données personnelles que nécessaire ;
- il est indispensable de prévoir des règles de sécurité suffisantes telles que la mise en place d'un système d'authentification permettant de contrôler les accès informatiques aux données personnelles, protéger l'accès aux armoires et tiroirs contenant les dossiers papiers ;
- il faut apporter une attention particulière aux contrats signés avec les prestataires informatiques. Cette vigilance doit conduire les cabinets à choisir les solutions applicatives présentant le maximum de garanties en termes de sécurité informatique et de protection des données personnelles. La question du transfert des données personnelles hors d'Europe est un point très important[9].

POUR EN SAVOIR PLUS

Consultez le « Guide de la protection des données personnelles à l'usage des experts-comptables » sur Biliordre.fr

Téléchargez le rapport d'activité 2020 de la CNIL sur son site, www.cnil.fr.

1. Le règlement général sur la protection des données.
2. Délibération du 18 novembre 2020.
3. Délibération du 18 novembre 2020.
4. Cf. l'article Sanction d'une TPE pour défaut de conformité aux dispositions du RGPD publié dans le SIC mag n°402 daté de mars 2021.
5. Délibération du 8 décembre 2020.
6. Délibération du 8 décembre 2020.
7. Délibération du 7 décembre 2020.
8. Délibération du 7 décembre 2020.
9. Cf. l'article « Protection des données personnelles : la Cour de justice de l'Union européenne (CJUE) invalide le privacy shield » publié dans le SIC mag n°398 daté d'octobre 2020.