Nomos
société d'avocats

nomosnetcom.fr **Mai 2017**

Contrôle et sanction de la CNIL : une société de VTC sanctionnée pour manquements réitérés à la loi Informatique et Libertés

[DONNEES PERSONNELLES]
Délibération de la formation restreinte de la Commission Nationale de l'Informatique et des Libertés du 13 avril 2017

Le 13 avril 2017, la Commission Nationale de l'Informatique et des Libertés (CNIL) a publié une délibération faisant état d'une sanction prononcée à l'encontre d'une société de VTC pour manquements persistants aux obligations de la loi « *Informatique et Libertés* » (loi n°78-17 du 6 janvier 1978).

La procédure avait été initiée à la suite d'une plainte d'un client . A l'occasion d'un contrôle dans les locaux de la société, divers manquements avaient été constatés et la présidente de la CNIL avait alors mis en demeure la société d'adopter des mesures correctives dans un délai de trois mois.

A l'issue de ce délai, la formation restreinte a constaté la persistance de certains manquements et l'insuffisance des mesures adoptées. Une procédure de sanction a donc été ouverte.

La formation restreinte a prononcé une sanction pécuniaire de 15.000 euros, assortie d'une mesure de publication de la décision, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication .

Deux manquements principaux ont été retenus.

Le premier concerne la conservation des données dont la durée doit être préalablement définie en fonction des finalités visées par le traitement de données personnelles (article 6-5 de la loi « *Informatique et Libertés* »). Plus précisément, il avait été demandé à la société de veiller à ce que les données relatives au cryptogramme de la carte bancaire ne soient pas conservées au-delà du temps nécessaire à la transaction et de purger les données dont les personnes avaient demandé la suppression.

En défense, si les faits reprochés n'ont pas été contestés, la société a fait valoir qu'elle s'était montrée diligente pour appliquer les mesures correctives exigées par la CNIL mais qu'elle ne disposait que de faibles moyens humains et financiers. Aussi :

- Concernant la purge automatique que la société aurait dû mettre en place, elle faisait valoir que des mesures correctives avaient été aménagées et qu'à l'occasion du second contrôle de la formation, seuls dix comptes d'utilisateurs n'avaient pas été purgés.
- S'agissant des cryptogrammes visuels, la société a affirmé qu'elle avait été forcée de les stocker pour répondre à des exigences techniques imposées par son prestataire de paiement. Elle a en outre garanti qu'elle avait depuis changé de prestataire et qu'au jour de l'audience, plus aucun cryptogramme n'était stockéet en justifiait par la production d'un constat d'huissier.

La formation restreinte a rejeté ces deux arguments. Elle a estimé qu'il n'y avait pas lieu de minimiser le nombre de comptes non purgés ou de cryptogrammes conservés après le second contrôle puisque le délai de mise en conformité était à cette date, largement expiré.

Le second manquement visait l'obligation de garantir la sécurité et la confidentialité des données personnelles collectées par la société (article 34 de la loi « *Informatique et Libertés* »). A l'issue du premier contrôle, il avait été enjoint à la société de modifier les procédures de confirmation de création de compte et de récupération du mot de passe (afin qu'il ne soit plus communiqué en clair), et d'imposer pour chaque mot de passe une robustesse suffisante. A ce titre, la formation restreinte avait formulé des demandes précises, notamment la mise en place d'un stockage haché et de l'algorithme SHA 256 avec l'usage d'un sel stocké en dehors de la base de données.

En réponse, la société de VTC a fait valoir deux arguments principaux :

- Sur la procédure de création de mot de passe, elle a avancé que la Présidente de la CNIL avait manifestement anticipé une recommandation de la CNIL relative aux mots de passe publiée le 19 janvier 2017, soit bien après les deux contrôles.
- Sur la procédure de confirmation de création de compte, elle s'est fondée sur un constat d'huissier faisant état de la fin des manquements constatés. La société a également avancé que le stockage en sel du mot de passe dans un fichier distinct de celui où figure le mot de passe haché et encrypté suffit pour assurer la sécurité des données.

La formation restreinte n'a pas été convaincue par ces explications. Estimant que le dispositif de sa mise en demeure était suffisamment clair, elle a démenti que la Présidente de la CNIL ait appliqué par anticipation la recommandation précitée. Elle a par ailleurs observé que l'identifiant et le mot de passe de l'utilisateur étaient toujours transmis en clair lors du second contrôle, au mépris de la mise en demeure. Elle a enfin critiqué le choix du stockage du sel dans un fichier distinct des mots de passe, pour privilégier son stockage dans un espace distinct.

Si la formation restreinte a finalement condamné la société à une amende de 15.000 euros alors que le rapporteur recommandait une sanction de 50.000 euros, elle accompagne cette sanction d'une publication. Plus sévère, la publicité a pour objet de sensibiliser les personnes sur l'importance de mettre en œuvre les demandes de la CNIL, mais elle peut entraîner des conséquences dommageables pour la réputation de l'entreprise visée.

Kimberley BENISTI