



Par Grimaud VALAT

Avocat à la Cour
Cabinet DTMV Avocats

Et Julie BILLIEMAZ

Cabinet DTMV Avocats

→ RLDI 4574

Sanction d'Infogreffe par la CNIL à une amende de 250 000 euros

La récente condamnation d'Infogreffe par la Commission nationale de l'informatique et des libertés est l'occasion pour faire une ouverture sur l'importance de la mise en place d'une identité numérique fiable.

Délib. SAN-2022-018, 8 sept. 2022

Par délibération du 8 septembre 2022, la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL) a condamné Infogreffe à une amende de 250 000 euros au regard de la violation de l'obligation de conservation des données pendant une durée proportionnée à la finalité de traitement et de l'obligation d'assurer la sécurité des données à caractère personnel des utilisateurs de leur site.

Cette sanction a également été prise au regard de la nature d'officier public et ministériel de l'acteur concerné regroupant les greffes des tribunaux de commerce de France.

1.- Infogreffe a manqué à son obligation de conservation des données pour une durée proportionnée à la finalité du traitement de l'article 5, §1, e) du Règlement Général sur la Protection des Données (RGPD). La charte de confidentialité mentionnait un délai de conservation des données de 36 mois alors que pour 25% des utilisateurs les données personnelles étaient conservées au-delà de cette durée. Le manquement a été caractérisé par la conservation des données pendant une durée excessive au regard de la finalité de la collecte et de la politique de confidentialité d'Infogreffe. Cette conservation excessive découle manifestement de l'absence de procédure de suppression automatique des données. En défense, Infogreffe a invoqué notamment la finalité de traitement relative aux opérations de recouvrement. La CNIL a relevé que cette dernière n'était pas inscrite dans la charte de confidentialité, qu'aucun archivage intermédiaire ni aucune procédure d'anonymisation automatique n'étaient mis en œuvre. Ainsi, bien que constatant qu'une purge des comptes a été effectuée depuis le contrôle réalisé, la CNIL retient que le manquement reste caractérisé pour le passé.

2.- Infogreffe a manqué à son obligation d'assurer la sécurité des données à caractère personnel instaurée par l'article 32 du RGPD. Les mots de passe des utilisateurs d'Infogreffe n'étaient

pas suffisamment robustes puisqu'ils comprenaient seulement huit caractères, sans aucun critère de complexité et sans aucune mesure de sécurité complémentaire. A ce premier manquement s'ajoute le fait qu'Infogreffe transmettait en clair par courriel des mots de passe non temporaires et les conservait dans sa base de données avec les questions ainsi que les réponses secrètes de ré-initialisation des mots de passe. Les utilisateurs ne recevaient également pas de confirmation en cas de modification de leur mot de passe. En défense, Infogreffe indique notamment que l'obligation de sécurité n'est qu'une obligation de moyens qui doit être sanctionnée qu'en cas d'accès non autorisé, ce qui n'était pas le cas en l'espèce, et que les recommandations relatives au mot de passe ne sont que facultatives. La CNIL a tout d'abord rappelé que les recommandations concernant les mots de passe étaient des précautions élémentaires de sécurité, avant d'indiquer que les mesures de sécurité mises en place par Infogreffe étaient insuffisantes et que les risques encourus d'utilisation ou d'usurpation frauduleuse par des tiers des comptes étaient réels. Le manquement a ainsi été caractérisé, bien qu'une nouvelle fois certaines mesures aient été prises par Infogreffe pendant la procédure.

3.- De tels manquements à l'obligation de sécurité dans le traitement des données personnelles soulignent le besoin croissant d'une réelle identité numérique protégée et sécurisée.

L'émergence de l'identité numérique, dont des mises en œuvre sont déjà constatées en France (FranceConnect), dans l'Union Européenne, mais aussi en Inde (India Aadhaar), marque une nouvelle évolution du service administratif d'identification de la population, adaptée à la digitalisation de la société.

Cette évolution intervient à la faveur d'une innovation technologique qui consiste en la dématérialisation numérique d'informations autrefois regroupées sous des formes tangibles, dont le ni-



veau de sécurité est plus ou moins élevé en fonction du support utilisé, et dont l'utilité est limitée par la nature du support.

L'identité numérique doit permettre aux citoyens de reprendre possession de leurs données et de sécuriser leurs processus d'identification pour :

- d'une part, en utilisant la technologie pour centraliser les données d'identification et limiter au strict nécessaire les données divulguées en fonction des cas d'usage ;
- d'autre part, en autoriser la consultation à des tiers choisis pour des finalités approuvées.

Ce deuxième aspect est particulièrement intéressant, en ce que les caractéristiques même du support d'identité numérique permettent d'élargir la nature et la quantité des informations liées au dit support d'identification.

Ainsi, tandis qu'une carte d'identité est par nature immuable et limitée quant à son contenu, un coffre-fort ou portefeuille numérique d'identification permet l'adjonction de nouvelles informations, potentiellement compartimentées et affectées de divers niveaux de sécurité.

Ici, ce sont les meilleures techniques d'authentification et de sécurisation qui bénéficient potentiellement à des informations de moindre sensibilité et non l'inverse. ■