Protection de nos données personnelles : La sécurité informatique en question...

Le 23 février le journal LIBERATION révélait qu'un fichier contenant les informations de 500 000 patients a fuité sur Internet et fait la une des médias ces derniers jours.

Ce fichier comporte 491 840 lignes. Et à chaque ligne, jusqu'à 60 informations différentes sur une même personne: numéro de Sécurité sociale, date de naissance, groupe sanguin, adresse, numéro de téléphone portable, médecin prescripteur, etc et même e-mail, mot de passe et données de santé.

Ce fichier, dans lequel 478 882 personnes sont identifiées par leurs noms de famille, est majoritairement constitué de résultats provenant de laboratoires de biologie médicale dans le Morbihan, l'Eure, le Loiret, les Côtes-d'Armor et le Loir-et-Cher.

Les données sont datées de 2015 à 2020, avec une large partie de 2018 et 2019. Plus inquiétant encore, d'après Damien Bancal, spécialiste de cybersécurité, ces quasi 500 000 profils médicaux ne constitueraient qu'un "*extrait*" d'un fichier plus large.

La presse nous apprend aussi que *le fichier n'était effectivement pas anonymisé et qu'il n'était nullement protégé par une couche de chiffrement ; des mesures pourtant fortement recommandées, et même obligatoires pour certaines informations de santé*.

La CNIL indique dans un communiqué de presse qu'elle procédait actuellement à des contrôles pour constater officiellement la mise à disposition du fichier.

« ***Les constatations préliminaires semblent indiquer qu'il s'agit effectivement d'une violation de données d'une ampleur et d'une gravité particulièrement importante, et laissent à penser que les données proviendraient de laboratoires d'analyse médicale.*** » explique la commission. « ***Si ces éléments devaient être confirmés, il incombe aux organismes concernés qui ne l'auraient pas déjà fait, de procéder à une notification auprès de la CNIL, dans les 72 heures suivant le moment où ils en ont pris connaissance. »***

La CNIL rappelle les obligations des entreprises concernées, surtout quand la fuite de données est susceptible d'engendrer un risque élevé pour les droits et les libertés : « ***Les organismes responsables ont l'obligation d'informer individuellement les personnes concernées du fait que leurs données ont été compromises et publiées en ligne***. »

Certes le risque zéro n'existe pas et des intrusions malveillantes dans un dispositif informatique sont toujours possibles, mais notifier les fuites à la CNIL et en informer les victimes ne suffit pas.

En qualité de client potentiel, d'un quelconque cabinet médical ou laboratoire d'analyses, on peut s'étonner que l'acquisition ou la location de logiciels, n'offrant pas toutes les garanties d'anonymisation et de chiffrement, puissent faire l'objet d'offres commerciales en leur direction et que ces offres puissent être retenues.

8 Mars 2021