ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 41411	De **M. Bernard Perrut** (Les Républicains - Rhône)	**Question écrite**

Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Premier ministre

Rubrique >numérique	**Tête d'analyse** >Protection des données de santé et souveraineté numérique	**Analyse** > Protection des données de santé et souveraineté numérique.

Question publiée au JO le : **28/09/2021**
Réponse publiée au JO le : **03/05/2022** page : **2944**
Date de changement d'attribution : **05/10/2021**

Texte de la question

M. Bernard Perrut alerte M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques sur la sécurité des données de santé. Les données personnelles d'environ un million et demi de personnes dépistées contre la covid-19 mi-2020 ont été dérobées après une cyberattaque menée au cours de l'été 2021. Les informations compromises incluent l'identité, le numéro de sécurité sociale et les coordonnées des personnes testées, ainsi que l'identité et les coordonnées des professionnels de santé les prenant en charge, les caractéristiques et le résultat du test réalisé, avec les risques que ces fuites représentent en matière d'usurpation d'identité. Ce nouvel incident intervient deux semaines après la découverte par Mediapart de centaines de milliers de résultats de tests antigéniques étaient restés accessibles durant plusieurs semaines sur le site d'un prestataire de pharmacies non homologué par les autorités sanitaires coupable d'une série de négligences. Dans ce contexte, face à la multiplication des cyberattaques qui touchent de nombreux établissements de santé et alors que l'américain Microsoft héberge les données du *Health Data Hub* français, il souhaiterait connaître les mesures qui vont être prises pour la protection des données et pour permettre à la France de retrouver sa souveraineté numérique.

Texte de la réponse

Les données à caractère personnel présentent un attrait particulier pour les attaquants. Elles font donc l'objet d'actions malveillantes, à finalité lucrative ou d'espionnage. En raison de leur faible sécurisation, elles font l'objet de divulgations massives, répondant à des motivations diverses de la part des attaquants. Dans son Panorama de la menace 2021, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a classé ces divulgations en quatre grandes catégories : les divulgations de données dans le cadre d'attaques par rançongiciels ; les divulgations motivées idéologiquement (hacktivisme) ou dans le cadre d'opérations de déstabilisation ; les divulgations de données à des fins de revente ; et enfin les divulgations par négligence. Les données personnelles volées peuvent être réutilisées pour mener de nouvelles attaques, notamment par hameçonnage : elles fournissent des portes d'entrée aux attaquants et facilitent les cyberattaques. La protection des données personnelles est donc essentielle dans une optique de renforcement du niveau de cybersécurité. L'action de l'ANSSI, service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale, concourt à cet objectif dans le domaine de la

sécurisation des systèmes d'information hébergeant des données, notamment à caractère personnel, des individus, des entreprises (TPE/PME, grandes entreprises), des administrations et des collectivités auxquels elle fournit des ressources méthodologiques et pratiques, des recommandations et des outils. Elle met en œuvre diverses mesures visant à responsabiliser les acteurs privés et promouvoir les offres numériques sécurisées, notamment en qualifiant des prestataires de produits et de services. Les visas de sécurité délivrés par l'ANSSI permettent d'identifier facilement les offres dont la fiabilité a été reconnue à l'issue d'une évaluation rigoureuse. Au-delà de la sécurisation des données, la protection des données repose sur un ensemble de principes et pratiques tels que la transparence et la licéité, les droits des personnes physiques concernées, la limitation des finalités, la minimisation des données ou encore la pertinence et la durée de conservation d'une donnée. De nombreuses mesures visant à protéger les données des citoyens et des entreprises ont été mises en œuvre, tant au niveau européen que national. En particulier, le règlement européen sur la protection des données (RGPD), entré en application le 25 mai 2018, vise à harmoniser les règles et les pratiques européennes applicables en matière de protection des données à caractère personnel et complète d'autres dispositifs règlementaires concourant au renforcement de la sécurité numérique limités à un nombre restreint d'organisations. La Commission nationale de l'informatique et des libertés (CNIL), autorité indépendante de contrôle pour la protection des données à caractère personnel en France est ainsi chargée de veiller à la bonne application du RGPD et d'accompagner les entités engagées dans leur démarche de mise en conformité avec le règlement. Elle effectue un travail majeur au profit de nos concitoyens en contrôlant la protection de leurs données personnelles face à des utilisations non autorisées. Elle rend également obligatoire l'information des citoyens dont les données personnelles ont été divulguées.