ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 947

De **M. Philippe Latombe** (Mouvement Démocrate et apparentés - Vendée)

Question orale sans débat

Ministère interrogé > Intérieur

Ministère attributaire > Intérieur

Rubrique >numérique

Tête d'analyse >Sécurisation des fichiers nationaux

Analyse > Sécurisation des fichiers nationaux.

Question publiée au JO le : **28/01/2020**
Réponse publiée au JO le : **05/02/2020** page : **660**

Texte de la question

M. Philippe Latombe attire l'attention de M. le ministre de l'intérieur sur la sécurisation des fichiers nationaux et notamment celle du système des titres électroniques sécurisés, plus communément appelé TES. Le fichier TES contient l'identité, le sexe, la couleur des yeux, la taille, l'adresse du domicile, les données relatives à la filiation, l'image numérique du visage et de la signature, l'adresse e-mail et les empreintes digitales de tous les détenteurs d'une carte nationale d'identité ou d'un passeport français. D'autres données sont également conservées, comme les informations relatives au titre en lui-même ainsi que les données relatives au fabricant du titre et aux agents chargés de la délivrance du titre. L'ensemble de ces données à caractère personnel et d'informations enregistrées sont conservées pendant quinze ans s'il s'agit d'un passeport, et vingt ans s'il s'agit d'une carte nationale d'identité ou respectivement de dix ans et de quinze ans lorsque le titulaire du titre est un mineur. Le choix de la centralisation pour un tel fichier expose un ensemble massif et précieux de données personnelles à la portée de puissances hostiles ou de criminels expérimentés. L'audit de la DINSIC de de l'ANSSI, rendu le 13 janvier 2017, a souligné le caractère perfectible du système, car il pouvait être techniquement détourné à des fins d'identification par reconstitution d'une base de données complète à partir du lien unidirectionnel existant. Devant de tels dangers, les entreprises privées dites stratégiques sont contraintes de disposer de serveurs de sauvegarde. Peut-il dire ce qu'il en est pour les grands fichiers nationaux stratégiques hors défense, à l'exemple de TES, afin de les sécuriser en cas de défaillance ou d'intrusion du système ? Peut-il indiquer s'il existe pour chacun des systèmes des serveurs de sauvegarde placés dans des lieux distincts de ceux d'exploitation ? Enfin, il lui demande s'il peut aussi garantir qu'il n'y a aucun projet en cours, ou aucun risque, que le *cloud* soit utilisé comme système de sauvegarde, ce qui constituerait un danger majeur pour la protection des données personnelles de l'ensemble des citoyens.

Texte de la réponse

SÉCURISATION DES FICHIERS NATIONAUX

Mme la présidente. La parole est à M. Philippe Latombe, pour exposer sa question, n° 947, relative à la sécurisation des fichiers nationaux.

M. Philippe Latombe. Le système des titres électroniques sécurisés, plus communément appelé TES, contient l'identité, le sexe, la couleur des yeux, la taille, l'adresse du domicile, les données relatives à la filiation, l'image numérique du visage et de la signature, l'adresse électronique et les empreintes digitales de tous les détenteurs d'une carte nationale d'identité ou d'un passeport français. D'autres données sont également enregistrées, comme les informations relatives au titre lui-même, ainsi que les données relatives à son fabricant et aux agents chargés de sa délivrance. Les données personnelles, ainsi que les autres informations enregistrées, sont conservées pendant quinze ans s'il s'agit d'un passeport, pendant vingt ans s'il s'agit d'une carte nationale d'identité, et respectivement pendant dix et quinze ans dans le cas d'un mineur.

Le choix de la centralisation d'un tel fichier expose un ensemble massif et précieux de données personnelles à la portée de puissances hostiles ou de criminels expérimentés. Le rapport d'audit de la DINSIC – direction interministérielle du numérique et du système d'information et de communication de l'État – et de l'ANSSI – Agence nationale de la sécurité des systèmes d'information –, rendu le 13 janvier 2017, a souligné le caractère perfectible du système, qui peut être techniquement détourné à des fins d'identification, par reconstitution d'une base de données complète à partir du lien unidirectionnel existant.

Face à ce danger, les entreprises privées dites stratégiques sont contraintes de disposer de serveurs de sauvegarde. Monsieur le secrétaire d'État, quelles mesures sont-elles prises afin de sécuriser les grands fichiers nationaux stratégiques hors défense, à l'exemple de TES, en cas de défaillance ou d'intrusion du système ?

Existe-t-il, pour chaque système, des serveurs de sauvegarde placés dans des lieux distincts de ceux de leur exploitation ?

Pouvez-vous nous garantir qu'il n'y a aucun projet en cours ou aucun risque que le *cloud* soit utilisé comme système de sauvegarde, ce qui constituerait un danger majeur pour la protection des données personnelles de nos concitoyens ?

Mme la présidente. La parole est à M. le secrétaire d'État auprès du ministre de l'intérieur.

M. Laurent Nunez, *secrétaire d'État auprès du ministre de l'intérieur*. Dans un rapport d'audit remis en janvier 2017, l'ANSSI a conclu que le système TES, utilisé à la fois pour la délivrance des passeports et des cartes d'identité, était compatible avec la sensibilité des données qu'il contient. Elle a formulé onze recommandations afin d'améliorer la protection de ce système contre les risques d'intrusion et, en particulier, de renforcer la robustesse du lien unidirectionnel permettant de lier les identités aux éléments d'identification biométrique.

Sur le fondement du rapport de l'ANSSI, une décision d'homologation du système TES au titre de la sécurité des systèmes d'information a été prise le 8 février 2017 pour cinq mois. Au regard des travaux menés ces dernières années, notamment pour renforcer le chiffrement des données et du lien unidirectionnel entre les données d'identité et les données biométriques, l'homologation du système TES a été renouvelée le 7 juillet 2017, le 6 juillet 2018 et le 6 juillet 2019 pour une durée d'un an.

Dans une démarche d'amélioration continue, la sécurité du système TES fait l'objet d'un suivi strict par un comité dédié. Actuellement, les travaux de ce comité portent essentiellement sur la résilience du système. Il a d'ailleurs été décidé, compte tenu de la sensibilité des données en cause, que l'homologation du fichier au regard des normes de sécurité devrait être renouvelée plus fréquemment.

Dans ce cadre, la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur, l'ANSSI et la direction du numérique du ministère de l'intérieur ont engagé la rédaction d'un plan de continuité et de reprise d'activité. La plateforme TES est hébergée sur un site hautement sécurisé, auquel seules les personnes dûment autorisées peuvent accéder. Les données font l'objet de sauvegardes très fréquentes, sur deux serveurs locaux distincts, également hébergés sur un site hautement sécurisé, à accès limité.