ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 54771	De **Mme Catherine Troallic** (Socialiste, républicain et citoyen - Seine-Maritime)	**Question écrite**

Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur

Rubrique >télécommunications	**Tête d'analyse** >Internet	**Analyse** > données personnelles. protection.

Question publiée au JO le : **29/04/2014**
Réponse publiée au JO le : **07/03/2017** page : **2106**
Date de changement d'attribution : **07/12/2016**
Date de signalement : **14/06/2016**
Date de renouvellement : **17/03/2015**

Texte de la question

Mme Catherine Troallic interroge M. le ministre de l'intérieur sur la protection des données personnelles numériques sur le territoire national. Le site internet du principal opérateur français de télécommunications a été la cible d'une intrusion le 16 janvier 2014. Près de 800 000 clients de l'opérateur auraient été victimes d'une violation de certaines de leurs données. Le même opérateur a, par ailleurs, été victime d'une intrusion de l'Agence nationale de sécurité américaine, révélée par Edward Snowden, qui aurait ainsi infiltré le câble sous-marin SEA-ME-WE 4 servant aux télécommunications entre l'Asie du sud-est, le Moyen-Orient et l'Europe. Outre le référentiel général de sécurité auquel les administrations sont soumises et qui doit garantir aux usagers un niveau de sécurité minimum par la mise en œuvre d'une analyse des risques, elle l'interroge pour savoir si des mesures complémentaires ont été prises par les services du ministère de l'Intérieur, notamment la Direction centrale du renseignement intérieur, afin de prémunir les institutions de la République française, Gouvernement, Parlement et hautes administration de telles attaques et assurer également à l'ensemble de nos compatriotes l'effectivité de la protection de leurs données privées inscrite dans notre droit. Elle lui demande par ailleurs si un renforcement de la responsabilisation des opérateurs de télécommunication notamment français prévue par l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électronique est une voie envisagée afin les inciter à mieux sécuriser les données des utilisateurs.

Texte de la réponse

Depuis 2014, l'ensemble des institutions publiques nationales et européennes s'est saisi de la question de la protection des données des citoyens et des entreprises. Il ne s'agit plus aujourd'hui de faire porter des obligations de sécurité uniquement sur les opérateurs de communications mais de les généraliser à l'ensemble des acteurs. Le ministère de l'intérieur s'est saisi de ces sujets, notamment en créant, en janvier 2017, la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), en charge notamment de l'élaboration d'une stratégie ministérielle en la matière, de la coordination de sa mise en œuvre, du pilotage de son évaluation et de son actualisation. Le ministère de l'intérieur inscrit ainsi pleinement son action dans le cadre de la stratégie nationale pour la sécurité numérique, élaborée avec l'ensemble des ministères et soumise par le secrétaire général de la défense et de la sécurité nationale à l'approbation du Premier ministre en octobre 2015. Pour sa part, la délégation générale de la sécurité intérieure (DGSI), qui a succédé le 12 mai 2014 à la direction centrale du renseignement intérieur (DCRI), « concourt à la prévention et à la répression de la criminalité liée aux technologies de l'information et de la communication », conformément aux termes du décret no 2014-445 du 30 avril 2014 relatif à ses missions et à son organisation. Depuis 2014, les menaces cyber se sont intensifiées caractérisées par

des attaques de plus en plus complexes et ciblées, des fuites d'informations massives et des actes de cybermalveillance rendus publics (TV5 Monde, élections présidentielles américaines, Shadowbrokers, Panama papers). La réponse normative couvre aujourd'hui de nombreux aspects de la vie des citoyens et des entreprises. Plusieurs textes sont ainsi venus renforcer les obligations des acteurs industriels et des fournisseurs de services en matière de protection des données des citoyens et d'encadrement de l'activité des services étatiques. Parmi ces textes figurent notamment : - dans le domaine de la vie privée : l'accord entre les États-Unis et la commission européenne Safe Harbour a été annulé par la cour de justice de l'Union européenne (CJUE) et remplacé peu après par l'accord Privacy Shield, qui a donné lieu à l'adoption du règlement UE 2016/679 du Parlement et du conseil européens du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; - en matière de dématérialisation : le référentiel général de sécurité évoqué a été profondément impacté par l'entrée en application du règlement eIDAS ; - dans le domaine de la cybersécurité : l'Union européenne a adopté la directive 2016-1148 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Les textes d'application de la loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et de programmation militaire ont également été publiés ; - enfin, en matière de renseignement, la loi no 2015-912 du 24 juillet 2015 relative au renseignement est également à mentionner. La définition des mesures de prévention et de protection des opérateurs de télécommunication est assurée, dès lors qu'ils sont opérateurs d'importance vitale (orange par ex…), par l'agence nationale de la sécurité des systèmes d'information qui peut faire appel aux compétences de la DGSI.