



ASSEMBLÉE NATIONALE

14ème législature

protection

Question écrite n° 25205

Texte de la question

M. Jacques Cresta attire l'attention de Mme la ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, sur les incidences de la mise en place des technologies dite DPI (*deep packet inspection* ou inspection des paquets en profondeur) sur les réseaux de télécommunication français. Ces technologies peuvent être utilisées afin de censurer ou contrôler les flux émis par les citoyens, en dehors de tout cadre judiciaire. Ceci ferait courir un risque important pour la liberté et la confidentialité des données personnelles si des opérateurs privés utilisaient cette technologie. Il souhaite savoir si le Gouvernement est informé de telles pratiques de la part des opérateurs de télécommunication français ayant pour incidence d'étudier, d'expérimenter ou de mettre en place des moyens d'analyser le contenu détaillé d'un paquet réseau de façon à en tirer des statistiques, à filtrer ceux-ci ou à détecter des intrusions, du spam ou tout autre contenu prédéfini. Si tel est le cas, des mesures seront-elles mises en œuvre dans le cadre du projet annoncé d'un *habeas corpus* numérique, permettant de définir les règles garantissant la protection des données personnelles et de la vie privée sur Internet ?

Texte de la réponse

La garde des sceaux, ministre de la justice, est particulièrement sensible aux enjeux de démocratie liés à l'évolution et à l'utilisation des matériels de communication électronique. Le Deep Packet Inspection (DPI), ou inspection des paquets en profondeur, recouvre une large gamme de systèmes et d'applications qui peuvent notamment être utilisés pour la sécurisation et la protection des réseaux. Les opérateurs qui souhaitent utiliser une technologie, quelle qu'elle soit, doivent le faire dans le cadre des dispositifs législatifs et réglementaires applicables, indépendamment des solutions techniques employées. A cet égard, les articles 100 à 100-7 du code de procédure pénale et L.241-1 à L.245-3 du code de la sécurité intérieure encadrent le secret des correspondances émises par la voie des communications électroniques. L'article L. 241-1 du code de la sécurité intérieure dispose ainsi que : « Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci ». L'article 226-15 du code pénal institue par ailleurs des délits et des sanctions pour les atteintes au secret des correspondances, notamment celles qui sont émises, transmises ou reçues par la voie électronique. S'agissant des communications électroniques, les articles L.34-1 à L.34-6 du code des postes et des communications électroniques indiquent les obligations des opérateurs pour la protection de la vie privée des utilisateurs de réseaux et services de communications électroniques. Compte tenu de cet état du droit, les pouvoirs publics ne manqueraient pas de saisir les juridictions compétentes si des projets ou agissements contrevenant aux dispositions législatives et réglementaires en vigueur étaient portés à leur connaissance. Enfin ces éléments sont pris en compte dans le cadre des travaux sur le projet de règlement européen relatif à la protection des données personnelles et sur le projet d'*habeas corpus* numérique.

Données clés

Auteur : [M. Jacques Cresta](#)

Circonscription : Pyrénées-Orientales (1^{re} circonscription) - Socialiste, écologiste et républicain

Type de question : Question écrite

Numéro de la question : 25205

Rubrique : Télécommunications

Ministère interrogé : PME, innovation et économie numérique

Ministère attributaire : Justice

Date(s) clé(e)s

Question publiée au JO le : [23 avril 2013](#), page 4367

Réponse publiée au JO le : [19 novembre 2013](#), page 12131