ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 10778	De **M. Julien Borowczyk** (La République en Marche - Loire)	**Question écrite**

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

Rubrique >gendarmerie	**Tête d'analyse** >Favoriser les outils techniques d'enquête de la gendarmerie	**Analyse** > Favoriser les outils techniques d'enquête de la gendarmerie.

Question publiée au JO le : **17/07/2018**
Réponse publiée au JO le : **18/02/2020** page : **1259**
Date de changement d'attribution : **16/10/2018**

Texte de la question

M. Julien Borowczyk interroge M. le ministre d'État, ministre de l'intérieur, sur les moyens techniques dont disposent les gendarmeries pour mener leurs enquêtes. Et notamment, les écoutes et extractions des données des téléphones portables. Actuellement, la gendarmerie dispose d'outils qui lui permettent de décoder une grande majorité des données téléphoniques comme les messages, les appels, les *mails*, les positions géographique, l'historique de navigation, les photos. Mais qu'en est-il des données sur les nouvelles applications en réseaux comme Snapchat, WhatsApp et même Instagram et bien d'autres ? Si depuis la loi n° 2015-990 pour la croissance, l'activité et l'égalité des chances économiques de 2015 (et notamment l'amendement n° 1565), l'ARCEP peut qualifier comme opérateur une entreprise qui « exploite un réseau ouvert au public ou fournit au public un service de communications électroniques », cette qualification n'est pas suffisante pour permettre le travail complet des services de gendarmerie. Si le fait d'être déclaré comme opérateur oblige l'entreprise concernée à accepter d'être mise sur écoute, deux problèmes se posent. D'abord, la durée de cette procédure, à l'heure du numérique l'utilisation de certaines applications devient vite dépassée alors que d'autres voient très vite le jour. Le moment où il est utile de déclarer une personne comme opérateur jusqu'au moment où cette déclaration est mise en œuvre peut être très long. Enfin, les services de gendarmerie ne disposent pas des moyens techniques pour extraire et exploiter les données qui se trouvent sur ces nouveaux « opérateurs de communications ». La question de la réactivité entre la législation et les moyens techniques qui sont donnés pour son application se pose. Avec pour conséquences éventuelles, des répercussions sur les enquêtes menées pour protéger la sécurité nationale et lutter contre le terrorisme, la criminalité et la délinquance organisée. Il souhaiterait donc connaître ses intentions pour améliorer les moyens d'enquête des services de gendarmerie.

Texte de la réponse

L'accès aux données des solutions de communication chiffrée de bout en bout est un défi pour les forces de l'ordre dans l'exercice de leurs missions régaliennes. En effet, ces solutions de messagerie instantanée ou de téléphonie telles que Whatsapp, I message ou Télégramme, ne permettent qu'aux utilisateurs, à partir du terminal (smartphone, tablette, etc) ayant part à la communication, d'accéder aux données échangées. Cependant, l'accès aux données de ces solutions de communication à l'insu de l'utilisateur peut s'effectuer par plusieurs approches, à disposition des forces de l'ordre :D'une part l'approche traditionnelle est celle de l'investigation sous pseudonyme, c'est-à-dire par la participation aux échanges sans faire état de son identité ni de sa fonction.Ensuite, l'accès aux données peut

s'effectuer au titre d'une saisie du terminal. Cela suppose que l'accès logique au terminal soit possible. Le régime procédural en vigueur permet ainsi de déverrouiller le code d'accès et d'effectuer le déchiffrement des données si le système est chiffré dans son ensemble.Une troisième approche réside dans la captation des données informatiques. Il s'agit d'implanter un logiciel de captation de données dans le terminal à l'insu de l'utilisateur. Les données qui s'affichent à l'écran, qui sont saisies au clavier ou qui sont stockées sur le support sont alors dupliquées et exportées avant qu'elles ne soient chiffrées. La loi du 16 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, a introduit cette capacité légale dans l'enquête judiciaire. De plus, ces dispositifs particulièrement intrusifs et susceptibles d'être décelés par des solutions de sécurité informatique, nécessitent un très haut niveau de technicité en matière de conception et d'emploi opérationnel. La concrétisation de cette ambition est classifiée et échappera encore durablement aux enjeux de lutte contre la criminalité de droit commun.Il convient cependant de noter qu'une quatrième approche consiste à introduire des backdoors, c'est-à-dire un moyen de déchiffrer les données lors de leur transit entre plusieurs terminaux. Cette évolution dépend cependant des négociations entre l'Etat et les concepteurs de ces solutions de communication. Ces négociations ne sont pas rendues publiques. De même cette approche nécessite des évolutions du cadre juridique existant qui doivent faire face aux divisions de l'opinion publique, opposant les exigences de sûreté nationale à la défense des libertés publiques.