

14ème législature

Question N° : 65915	De M. Damien Meslot (Union pour un Mouvement Populaire - Territoire de Belfort)	Question écrite
Ministère interrogé > Intérieur		Ministère attributaire > Intérieur
Rubrique > télécommunications	Tête d'analyse > appareils téléphoniques	Analyse > cryptage des données. lutte contre la criminalité.
Question publiée au JO le : 07/10/2014 Réponse publiée au JO le : 26/05/2015 page : 3975		

Texte de la question

M. Damien Meslot interroge M. le ministre de l'intérieur sur les risques d'entraves à la réalisation d'enquêtes de police visant à lutter contre la criminalité, suite à la mise en place par Apple d'une sécurité renforcée sur ses nouveaux iPhones 6 et 6 Plus. En effet, le directeur de la police de Chicago s'est sérieusement inquiété de la mise en place par le géant californien d'un degré de sécurité qui empêche même la marque à la pomme d'outrepasser le mot de passe des utilisateurs ou d'accéder à leurs données. En cela, il est rejoint par le Bureau fédéral d'investigations (FBI), l'Agence centrale du renseignement américain (CIA) ou encore l'Agence nationale de la sécurité étasunienne (NSA). Le directeur du FBI a estimé que ces nouvelles règles de sécurité entraîneront effectivement une préférence des personnes malveillantes qui se sentiront « au-dessus des lois ». Le nouveau cryptage de données utilisé par Apple pour ses derniers smartphones rend l'accès aux données quasiment impossible. Si les scandales liés à l'espionnage de données dévoilé *via* Wikileaks, ou le scandale du vol de photos intimes diffusées sur internet, ont réveillé l'opinion publique concernant les données privées, la police et les enquêteurs détiennent malgré tout, dans ces données, de précieux indices pour tracer les criminels, remonter des filières et démanteler des réseaux. Ainsi il souhaite connaître les mesures qu'il entend prendre pour empêcher que soit rendue plus difficile sinon impossible la lutte contre la criminalité passant par l'utilisation des nouveaux iPhones 6 et 6 Plus, un appareil que le directeur de la police de Chicago a déclaré dans une formule choc comme « un téléphone de choix pour les pédophiles ».

Texte de la réponse

Un certain nombre de téléphones récemment mis sur le marché mettent en oeuvre par défaut des technologies de chiffrement qui les rendent pratiquement inviolables, même pour les fournisseurs qui affirment ne pas disposer de la capacité technique de déchiffrement de leurs terminaux et ne pouvoir répondre aux demandes des autorités judiciaires souhaitant accéder aux informations contenues dans ces appareils. La commercialisation de ces nouveaux téléphones a donc suscité de fortes réserves de la part des services d'investigations américains, comme en France de la direction centrale de la police judiciaire qui craint de ne pouvoir accéder aux données contenues dans les téléphones portables des délinquants, souvent essentielles pour la résolution des enquêtes. La France toutefois, outre les moyens dont peuvent être dotées ses agences spécialisées telle que l'Agence nationale de la sécurité des systèmes d'information, dispose d'ores et déjà d'outils juridiques qu'elle pourrait mettre en oeuvre pour surmonter les difficultés posées par la sécurité renforcée des iPhone 6 et autres terminaux de cette génération. Si la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dispose que « l'utilisation des moyens de cryptologie est libre », le décret n° 2007-663 du 2 mai 2007 relatif aux moyens et aux prestations de cryptologie organise cependant un régime de déclaration ou d'autorisation auprès de l'Agence nationale de la sécurité des systèmes d'information pour les sociétés souhaitant mettre ces moyens à la disposition du public, dans le cadre de la

protection des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat. Par ailleurs, les sociétés sont légalement tenues de disposer d'une capacité de déchiffrement de leurs terminaux. Aux termes de l'article 434-15-2 du code pénal, « est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale. Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende ». Cette disposition semble applicable aux sociétés fabriquant des smartphones, qui auraient dès lors une obligation légale de disposer de la capacité de déchiffrement de leurs propres terminaux. Toutefois, les sociétés concernées n'ont pas nécessairement de filiales françaises sur lesquelles pourrait porter cette obligation. Elles sont par conséquent soumises à la loi de leur pays d'origine (loi américaine dans le cas d'Apple) et ne peuvent faire l'objet de poursuites pénales en cas de refus de mise en oeuvre du déchiffrement. C'est l'une des raisons pour lesquelles le ministre de l'intérieur s'est déplacé aux Etats-Unis, les 19 et 20 février 2015, afin d'évoquer la question du chiffrement avec ses homologues américains et les représentants des principales entreprises d'informatique, dont Apple.