ASSEMBLÉE NATIONALE

29 février 2016

LUTTE CONTRE LE CRIME ORGANISÉ, LE TERRORISME ET LEUR FINANCEMENT - (N° 3515)

Commission	
Gouvernement	

Retiré

AMENDEMENT

N º 532

présenté par
M. Galut, Mme Adam, Mme Lousteau, M. Cresta, Mme Gueugneau, M. Bardy, Mme Troallic, M. Colas, M. Arnaud Leroy, Mme Crozon, Mme Bouziane-Laroussi, M. Alexis Bachelay, Mme Dufour-Tonini, M. Laurent, M. Potier, Mme Tallard, Mme Iborra, Mme Berger, M. Daniel, M. Delcourt, M. Destans, M. Juanico, M. Liebgott, M. Pouzol, Mme Rabault, Mme Rabin et M. Terrasse

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 3, insérer l'article suivant:

Après l'article 99-3 du code de procédure pénale, il est inséré un article 99-3-1 ainsi rédigé :

« *Art. 99-3-1.* – Pour les enquêtes concernant les infractions mentionnées au 11° de l'article 706-73 du code de procédure pénale, le juge d'instruction, ou l'officier de police judiciaire par lui commis, peut requérir de tout concepteur de matériel électronique d'accéder, par tous moyens, aux données susceptibles d'intéresser l'enquête en cours contenues sur des supports électroniques relevant de sa conception.

« Le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende d'un million d'euros. »

EXPOSÉ SOMMAIRE

Le présent amendement a pour objet de permettre l'accès aux données contenues dans tout matériel électronique (téléphones, tablettes, ordinateurs), y compris les données pouvant faire l'objet d'un chiffrement.

Face à la multiplication des systèmes de cryptage, essentiels en matière de protection des données personnelles, il apparaît non moins nécessaire de garantir l'accès à toute donnée permettant de faire progresser rapidement une enquête judiciaire face aux infractions les plus graves.

L’objectif de cet amendement est de préserver un équilibre entre le droit à la protection de la vie privée des citoyens et le droit à la sécurité. D’une part, l’accès à ces données chiffrées serait possible uniquement dans le cadre d’une enquête judiciaire portant sur des infractions à caractère terroriste, et sur demande d’un magistrat ou officier de police judiciaire dûment autorisé.

D’autre part, les concepteurs de matériel électronique ne pourraient opposer la non connaissance des clés de chiffrement - alors qu’ils disposent des moyens techniques pour accéder à ces données - sans s’exposer à une amende extrêmement sévère et à la hauteur de leur chiffre d’affaire. Il s’agit donc de renforcer le caractère dissuasif d’un refus par un montant adapté aux entreprises visées, étant précisé qu’il s’agit d’une somme maximale pouvant être réduite par le juge.

ASSEMBLÉE NATIONALE

25 février 2016

LUTTE CONTRE LE CRIME ORGANISÉ, LE TERRORISME ET LEUR FINANCEMENT - (N° 3515)

Commission	
Gouvernement	

Rejeté

AMENDEMENT

N º 221

présenté par
M. Ciotti, M. Goujon, M. Larrivé, M. Olivier Marleix, M. Lellouche, M. Mariani, M. Myard, M. Foulon, M. Nicolin, M. Cinieri, M. Lazaro, M. Bénisti, M. Brochand, M. Abad, M. Reynès, M. Gandolfi-Scheit, M. Salen, M. Straumann, M. Dhuicq, M. Siré, M. Suguenot, M. Christ, Mme Grosskost, M. Philippe Armand Martin, M. Gérard, M. Vitel, M. Sermier, M. de La Verpillière, M. Daubresse, M. Ginesy, M. Morel-A-L'Huissier, M. Luca, M. de Ganay, Mme Genevard et M. Guibal

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 3, insérer l'article suivant:

Après l’article 421-2-3 du code pénal, il est inséré un article 421-2-3-1 ainsi rédigé :

« *Art. 421-2-3-1*. – Dans le cadre d’une enquête relative à des infractions terroristes, les fabricants d’outils de télécommunications, les opérateurs de télécommunications, les fournisseurs d’accès à internet ou tout prestataire de services sur internet sont tenus de communiquer l’ensemble des informations pertinentes pour la résolution de celle-ci aux services compétents.

« La violation de cette obligation est punie d’une amende maximale de 2 millions d’euros et d’une interdiction de commercialisation des produits et services de la société en cause sur le territoire national pendant une durée maximale d'un an. »

EXPOSÉ SOMMAIRE

Les téléphones mobiles et internet sont devenus centraux tant pour le recrutement des terroristes que pour la préparation des actes de terrorisme.

À ce titre, les fabricants d’outils de télécommunications,les opérateurs de télécommunications, les fournisseurs d’accès à internet et plus globalement les prestataires de services sur internet peuvent

disposer d'informations déterminantes pour la résolution des enquêtes relatives aux infractions terroristes.

Or, les services peuvent se heurter aux dispositifs contenus dans certains téléphones, les données étant illisibles lorsque l'on ne dispose pas du code de déverrouillage. Il en est de même pour certains contenus sur internet.

L'amiral Michael Rogers, à la tête de la NSA, affirme que sans le chiffrement, les attentats de Paris auraient pu être évités.

Au total, huit téléphones portables sur les 133 analysés en 2015 n'ont pu « être traités », selon le service central de l'informatique et des traces technologiques de la police judiciaire. C'est par exemple le cas d'un iPhone 4S, saisi dans le cadre de l'enquête sur les attentats du 13 novembre, et le cas du téléphone portable de Sid Ahmed Ghlam qui avait prévu d'attaquer une Église l'an passé.

Aussi, le présent amendement propose de contraindre ces opérateurs à communiquer l'ensemble des informations pertinentes aux services compétents.

La violation de cette obligation serait punie d'une amende maximale de 2 millions d'euros et d'une interdiction de commercialisation des produits et services de la société en cause sur le territoire national, pendant une durée pouvant aller jusqu'à un an.