PROJET DE LOI

RENSEIGNEMENT
(PROCÉDURE ACCÉLÉRÉE)

(n° 461, 460, 445)

N°	23

DIRECTION

DE LA SEANCE

28 MAI 2015

A M E N D E M E N T

C	
G	

présenté par

M. MALHURET

ARTICLE 1ER

Après l'alinéa 123

Insérer trois alinéas ainsi rédigés :

« Art. L. 833-3-… – I. – La Commission nationale de contrôle des techniques de renseignement réalise l'agrément des dispositifs mettant en œuvre les techniques de renseignement prévues aux chapitres I^{er} à III du titre V, afin de vérifier leur conformité aux restrictions techniques imposées par les dispositions du présent livre.

« II. – Seuls les modèles de dispositifs agréés par la Commission nationale de contrôle des techniques de renseignement peuvent être utilisés pour les finalités prévues aux chapitres I^{er} à III du titre V.

« III. – Les I et II entrent en vigueur un an après la promulgation de la loi n° du relative au renseignement.

OBJET

Cet amendement vise à doter la Commission nationale de contrôle des techniques de renseignement du pouvoir d'effectuer un audit technique des modèles des dispositifs techniques décrits aux chapitres Ier à III du titre V, préalablement à leur utilisation effective.

Il s'agit en particulier de garantir que les dispositifs respectent autant que possible le principe de « privacy by design », que l'on peut traduire approximativement par : « respect intrinsèque de la vie privée » par le dispositif. Ce principe sera une obligation réglementaire future au sein de l'Union européenne. Il est énoncé par exemple dans l'article 23 de la proposition de règlement 2012/0011 (COD) 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, et rappelé par le considérant 46 de la directive 2012/0010 (COD).

Il fournit également à la Commission nationale de contrôle des techniques de renseignement l'opportunité de se faire communiquer les informations techniques et d'usage nécessaires à l'agrément des dispositifs concernés, ainsi que de leurs évolutions. Ceci lui permet ainsi de disposer de la vision la plus exhaustive qui soit des capacités des nouvelles générations de matériels et logiciels.

Afin de ne pas pénaliser le travail des services de renseignement, une période de grâce d'un an est instaurée à partir de l'entrée en vigueur de la loi, permettant à la Commission nationale de contrôle des techniques de renseignement de procéder à l'agrément desdits dispositifs.

PROJET DE LOI

RENSEIGNEMENT
(PROCÉDURE ACCÉLÉRÉE)

(n° 461, 460, 445)

N°	24

DIRECTION DE LA SEANCE

27 MAI 2015

A M E N D E M E N T

C	
G	

présenté par

M. MALHURET

ARTICLE 2

Alinéa 50, après la première phrase

Insérer une phrase ainsi rédigée :

Le dispositif garantit que seules les correspondances dont l'interception a été autorisée sont effectivement rendues accessibles aux agents chargés de leur recueil.

OBJET

Les dispositifs techniques mentionnés à l'article L. 851-7, tels que les « IMSI catchers », peuvent intercepter l'intégralité des correspondances émanant des équipements terminaux à leur portée. Or, lesdits équipements appartiennent majoritairement à des personnes étrangères à l'enquête, qui peuvent de surcroît être des personnes bénéficiant d'une protection spécifique : parlementaires, avocats, journalistes, etc. Il est donc primordial que le contenu des conversations des personnes étrangères à l'enquête ne puisse être accessible à l'opérateur du dispositif d'interception, du fait même de la conception de celui-ci.

Il s'agit de garantir le principe de « privacy by design », que l'on peut traduire approximativement par : « respect intrinsèque de la vie privée » par le dispositif. Ce principe sera une obligation réglementaire future au sein de l'Union européenne. Il est énoncé par exemple dans l'article 23 de la proposition de règlement 2012/0011 (COD) 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, et rappelé par le considérant 46 de la directive 2012/0010 (COD).

La vérification du respect de cette disposition par le fabricant du dispositif devrait être l'objet de l'agrément, réalisé par la Commission nationale de contrôle des techniques de renseignement, des différents modèles de dispositifs mis en œuvre (voir amendement précédent relatif à l'article L. 833-3 bis (nouveau)).

PROJET DE LOI

RENSEIGNEMENT
(PROCÉDURE ACCÉLÉRÉE)

(n° 461, 460, 445)

N°	25

DIRECTION

DE LA SEANCE

27 MAI 2015

A M E N D E M E N T

C	
G	

présenté par

M. MALHURET

ARTICLE 2

Alinéas 15 à 22

Supprimer ces alinéas.

OBJET

La mise en œuvre de « traitements automatisés destinés […] à détecter des connexions susceptibles de révéler une menace terroriste » par l'analyse massive du trafic est une mesure disproportionnée et inefficace. L'ensemble des avis émis par la communauté scientifique fait état de l'inefficacité de ces méthodes. Cela tient au nombre considérable de « faux positifs » qui seraient obtenus, en regard du faible nombre de personnes ciblées, et à la difficulté de définir un comportement suspect qui ne soit pas la simple expression d'une déviance par rapport à une norme imposée. Il est également fort probable que les personnes les plus dangereuses sachent échapper à cette analyse, par l'usage d'outils de chiffrement et de redirection de leur trafic en dehors du territoire national (outils VPN, Tor, etc.). Plus généralement, les traitements de profilage de masse ne sont pas compatibles avec les exigences morales d'un État démocratique.

SÉNAT

DIRECTION

DE LA SEANCE

PROJET DE LOI

RENSEIGNEMENT
(PROCÉDURE ACCÉLÉRÉE)

(n° 461, 460, 445)

N°	26

28 MAI 2015

A M E N D E M E N T

C	
G	

présenté par

M. MALHURET

ARTICLE 3

Compléter cet article par un alinéa ainsi rédigé :

« … – Sauf sur décision expresse du Premier ministre, aucun transfert de masses de données collectées au titre de cet article ne peut conduire à ce que des volumes de données incluant une proportion significative de ressortissants français ne soient transmis à des services étrangers ou reçus de ceux-ci. »

OBJET

Par le passé, des échanges de données ont pu être réalisés entre services de renseignement français et étrangers, conduisant à ce que des masses de données explicitement relatives à des ressortissants français soient communiquées à des services étrangers. Le présent amendement vise à empêcher les transferts massifs des données de nos concitoyens à des acteurs étrangers.

Le terme « proportion significative » vise à ne pas entraver le fonctionnement des services, dans le cas où le mode de collecte ne peut empêcher que des ressortissants français fassent partie des personnes concernées par la collecte. Les transferts de données ciblés, par exemple relatifs à certains de nos ressortissants impliqués dans des actions terroristes, ne sont également pas empêchés.

PROJET DE LOI

RENSEIGNEMENT
(PROCÉDURE ACCÉLÉRÉE)

(n° 461, 460, 445)

N°	27

DIRECTION
DE LA SEANCE

27 MAI 2015

A M E N D E M E N T

C	
G	

présenté par

M. MALHURET

ARTICLE 3

Alinéa 27, deuxième phrase

Supprimer cette phrase.

OBJET

Le respect de l'équilibre entre sécurité et liberté impose que les données collectées sur les personnes le soient dans un but précis. En l'état actuel, des masses considérables de données personnelles pourraient être recueillies sur l'ensemble des usagers de réseaux de communication, quelle que soit la nationalité effective de ces personnes, sans finalité affichée.

Cet amendement vise à garantir que les données collectées le soient toutes à des fins proportionnées et dans un objectif de traitement rapide.

PROJET DE LOI

RENSEIGNEMENT
(PROCÉDURE ACCÉLÉRÉE)

(n° 461, 460, 445)

N°	66

DIRECTION

DE LA SEANCE

28 MAI 2015

A M E N D E M E N T

C	
G	

présenté par

M. MALHURET

ARTICLE 3

Après l'alinéa 11

Insérer un alinéa ainsi rédigé :

« … – Les dispositifs techniques utilisés à cette fin garantissent que les seules informations captées sont celles effectivement échangées lors d'une conversation sortant du lieu privé. Toute information recueillie accidentellement par ces dispositifs hors de ce cadre est détruite immédiatement.

OBJET

Un même outil de captation des informations émises et reçues par le clavier et les périphériques audio-visuels d'un système de traitement automatisé de données (ou « système informatique ») peut être utilisé pour deux finalités distinctes. L'une est la captation des communications passées entre une personne surveillée et son correspondant situé en dehors du même lieu, avant qu'elles ne soient chiffrées et donc inaccessibles aux agents de renseignement par d'autres moyens. L'autre est la captation de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé. Or, cette deuxième finalité est expressément organisée par l'article L. 853-1.

L'objet de cet amendement est de faire en sorte que les outils mis en œuvre au titre de l'article L. 853-2 ne puissent être utilisés pour obtenir des informations qui auraient nécessité la mise en œuvre des dispositions de l'article L. 853-1, plus protectrices, en restreignant leurs capacités de captation aux moments où une communication est effectivement en cours.

Il s'agit de garantir le principe de « privacy by design », que l'on peut traduire approximativement par : « respect intrinsèque de la vie privée » par le dispositif. Ce principe sera une obligation réglementaire future au sein de l'Union européenne. Il est énoncé par exemple dans l'article 23 de la proposition de règlement 2012/0011 (COD) 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, et rappelé par le considérant 46 de la directive 2012/0010 (COD).

La vérification du respect de cette disposition par le fabricant du dispositif devrait être l'objet de l'agrément, réalisé par la Commission nationale de contrôle des techniques de renseignement, des différents modèles de dispositifs mis en œuvre (voir amendement précédent relatif à l'article L. 833-3 bis (nouveau)).