Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

Délibération n° 1/2016 du 14 janvier 2016

Saisie pour avis par le Premier ministre[1] d'un projet de décret relatif aux techniques de renseignement, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes :

I. Remarques de portée générale

La CNCTR relève que le projet de décret est pris pour l'application du livre VIII du code de la sécurité intérieure ainsi que pour celle de l'article 226-3 du code pénal.

En particulier, l'article 2 du projet précise le cadre juridique applicable aux accès administratifs aux données de connexion prévus aux articles L. 851-1, L. 851-2 et L. 851-4 du code de la sécurité intérieure.

A titre liminaire, la CNCTR souligne que les accès administratifs aux données de connexion, prévus au chapitre Ier du titre V du livre VIII du code de la sécurité intérieure, sont désormais soumis à la même procédure que les autres techniques de renseignement : leur mise en œuvre suppose une autorisation du Premier ministre accordée, sauf urgence absolue[2], après avis de la commission. Cette unification de procédure, que la Commission nationale de contrôle des interceptions de sécurité (CNCIS) avait préconisée, constitue, pour la CNCTR également, une évolution positive. Elle permettra d'éviter le risque de doctrines divergentes entre deux instances, l'accès administratif aux données de connexion étant jusqu'à présent soumis soit à l'autorisation d'une personnalité qualifiée lorsqu'il a lieu en temps différé, soit à celle du Premier ministre après avis de la CNCIS lorsqu'il a lieu en temps réel. A compter de l'entrée en vigueur du projet de décret, le nécessaire contrôle préalable à la mise en œuvre des techniques pourra donc être pleinement assuré par la CNCTR, autorité administrative indépendante.

La CNCTR observe en outre que le titre V du livre VIII du code de la sécurité intérieure présente les techniques de renseignement selon l'atteinte qu'elles peuvent porter à la vie privée, en partant de la technique réputée la moins intrusive, en l'espèce le recueil administratif des données de connexion. Si la CNCTR considère qu'un tel recueil est effectivement moins attentatoire à la vie privée que d'autres techniques, elle rappelle que les données de connexion sont des données sensibles et que le degré d'intrusion doit être apprécié au regard du mode de recueil mis en œuvre et, partant, de la nature et de la quantité des données collectées.

---

[1] Le secrétariat général de la défense et de la sécurité nationale (SGDSN) a adressé à la commission une saisine initiale reçue le 3 décembre 2015 et une saisine rectificative reçue le 7 janvier 2016.

[2] La procédure en urgence absolue, régie par l'article L. 821-5 du code de la sécurité intérieure, n'est toutefois pas applicable aux accès administratifs aux données de connexion prévus aux articles L. 851-2 et L. 851-3 du même code.

Les flux de communications électroniques sont aujourd'hui tels que le recueil des données de connexion permet de connaître ou de déduire de très nombreuses informations sur les personnes visées. Prises dans leur ensemble, ces données peuvent fournir des indications sur la vie privée, comme les habitudes de la vie quotidienne, les lieux de séjours ou les déplacements. A cet égard, un recueil en temps réel augmente l'atteinte portée à la vie privée, ce pourquoi le législateur a expressément décidé, sous le contrôle du Conseil constitutionnel, de limiter, en fonction du motif invoqué, de la durée de surveillance ou de la nature des données recueillies, la possibilité d'un tel recueil, qui n'est prévu qu'aux articles L. 851-2 et L. 851-4 du code de la sécurité intérieure.

II. Observations détaillées

1. Sur la définition des données de connexion

a) La CNCTR rappelle tout d'abord que l'article L. 851-1 du code de la sécurité intérieure définit les données de connexion susceptibles d'être recueillies non seulement en application de cet article mais aussi en application des articles L. 851-2 et L. 851-3, qui s'y réfèrent. Ces données sont les « *informations ou documents traités ou conservés* » par les « *réseaux* » ou les « *services de communications électroniques* » des opérateurs de communications électroniques, des hébergeurs et des fournisseurs de services sur internet, « *y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* »[3].

L'article L. 851-1 du code de la sécurité intérieure prévoit en outre qu'un décret en Conseil d'Etat fixe les modalités d'application de ses dispositions, après avis de la Commission nationale de l'informatique et des libertés (CNIL) et de la CNCTR.

La CNCTR estime que le décret d'application prévu à l'article L. 851-1 du code de la sécurité intérieure doit préciser la nature des données de connexion mentionnées par la loi. Elle considère, sous réserve des observations ci-dessous, que le projet de décret remplit cet objectif en créant un nouvel article R. 851-5 dans le code de la sécurité intérieure.

b) La CNCTR rappelle en outre que les données de connexion, par opposition au contenu de correspondances échangées ou d'informations consultées, désignent le « contenant », c'est-à-dire les données permettant l'acheminement d'une communication électronique[4].

---

[3] Ces formulations sont reprises de l'article L. 246-1 du code de la sécurité intérieure, créé par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019, lui-même inspiré de l'article L. 34-1-1 du code des postes et des communications électroniques, issu de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

[4] La notion de communication électronique s'entend au sens du 1° de l'article L. 32 du code des postes et des communications électroniques, à savoir « *les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique* ». Selon cette définition, une communication électronique peut consister en un échange entre deux personnes, entre une personne et une machine ou entre des machines.

Cette distinction de principe a été clairement énoncée au cours des travaux qui ont conduit à l'adoption de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Dès l'étude d'impact du projet de loi, le Gouvernement indiquait en effet : « *En application du nouveau régime juridique et comme cela était déjà le cas sous l'empire du régime précédent, l'accès aux données de connexion ne permet pas de connaître le contenu des échanges effectués par les personnes surveillées (...) Il ne s'agit donc que de la collecte de toutes les « traces » d'une connexion ou d'un appel, des factures détaillées dont dispose chaque abonné. Jamais l'accès au contenu d'une connexion ou d'un appel n'est permis* ».

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a par ailleurs jugé que la notion de données de connexion, telle qu'elle figure à l'article L. 851-1 du code de la sécurité intérieure, « *ne peut être entendue comme comprenant le contenu de correspondances ou les informations consultées* » (considérant 55).

La CNCTR note que l'interdiction d'accéder, par le biais d'un recueil de données de connexion, au contenu des correspondances échangées ou des informations consultées est en tout état de cause garanti par la loi, en l'occurrence par l'article L. 851-7 du code de la sécurité intérieure, qui subordonne le recueil des données de connexion au respect de l'article 226-15 du code pénal[5]. La CNCTR approuve néanmoins le rappel exprès de cette exclusion de principe dans le projet de décret, qui introduit dans le code de la sécurité intérieure un nouvel article R. 851-5 définissant les données de connexion « *à l'exclusion du contenu des correspondances échangées ou des informations consultées* » ainsi qu'un nouvel article R. 851-9, aux termes duquel : « *Les informations ou documents recueillis en application du présent chapitre ne peuvent, sans l'autorisation prévue à l'article L. 852-1*[6]*, être exploités aux fins d'accéder au contenu de correspondances échangées ou d'informations consultées* ».

c) La CNCTR souhaite apporter des précisions sur les conséquences de cette exclusion.

Techniquement, une émission électronique se matérialise par une suite d'enveloppes protocolaires, dites « couches », incluses les unes dans les autres, dont les plus intérieures, souvent appelées « couches hautes » sont transmises telles quelles au destinataire tandis que les extérieures, souvent appelées « couches basses », sont utilisées pour l'acheminement de l'émission.

Dans le modèle de référence défini par l'Union internationale des télécommunications (UIT), dans sa recommandation X.200 portant sur l'interconnexion de systèmes ouverts[7], les couches sont numérotées de 1 à 7, la première étant la plus extérieure et la septième la plus intérieure.

Afin de distinguer, au sein des émissions, les données de connexion du contenu des communications, la CNCTR considère que les données se trouvant dans les couches 1 à 3 (physique, liaison de données et réseau) du modèle de l'UIT font partie des données de connexion puisqu'elles sont destinées aux équipements des réseaux ou produites par eux. En outre, la CNCTR constate que des données de connexion sont présentes dans les couches 4 à 7 (transport, session, présentation, application).

---

[5] L'article 226-15 du code pénal réprime d'un an d'emprisonnement et de 45 000 euros d'amende l'atteinte au secret des correspondances, y compris celles empruntant la voie électronique.

[6] L'autorisation prévue à l'article L. 852-1 est celle autorisant le recueil du contenu des communications, dénommé « interception de sécurité ».

[7] Voir notamment l'article 6 de la recommandation.

Examinée à la lumière de ces éléments, la liste des données de connexion figurant au I du nouvel article R. 851-5 du code de la sécurité intérieure doit être, selon la CNCTR, interprétée de la façon suivante :

- Les données mentionnées au 1°, à savoir celles que les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet doivent conserver[8], constituent des données de connexion ;

- Les données mentionnées au 2° sont celles « *permettant de localiser les équipements terminaux* » non nécessairement conservées, comme les coordonnées *GPS* d'un *smartphone* transmises automatiquement à des serveurs distants par les logiciels qu'il embarque, sans même qu'une correspondance humaine (voix, synchronisation de courrier électronique ou autres) soit acheminée. Les données relatives à la localisation des équipements terminaux utilisés étant expressément incluses dans les données de connexion mentionnées par la loi à l'article L. 851-1 du code de la sécurité intérieure, la CNCTR les considère comme des données de connexion.

- Les données mentionnées au 3°, à savoir celles « *relatives à l'accès des équipements terminaux aux réseaux ou aux services en ligne* », peuvent être des données techniques envoyées par un équipement terminal pour manifester son existence à un réseau ou à un service en ligne afin d'établir une connexion. Par exemple, lorsqu'un utilisateur désactive le mode avion de son *smartphone* après un atterrissage, son équipement émet des signaux afin d'accéder aux réseaux présents dans son environnement.

  Cette catégorie de données comprend également les adresses internet ou *URL*[9]. La CNCTR note que, dans sa délibération n° 2015-455 du 17 décembre 2015 portant sur le projet de décret, la CNIL a décrit les *URL* comme « *nécessaire[s] à l'acheminement d'une communication* » tout en étant « *porteuse[s] par nature des informations consultées* ». La CNCTR considère également les *URL* comme des données mixtes, qui peuvent comporter à la fois des données de connexion et des mots faisant référence au contenu de correspondances échangées ou d'informations consultées. Elle souligne que le recueil de ces données dans le cadre des accès administratifs aux données de connexion ne saurait permettre de recueillir un tel contenu. Le recueil ne peut avoir pour objet que de reconstituer, grâce aux seules parties d'*URL* pertinentes, le chemin informatique utilisé pour échanger des correspondances ou consulter des informations.

  En conséquence, la CNCTR estime que lorsque des données de cette catégorie se trouvent dans les couches 4 à 7 du modèle de l'UIT, leur recueil ne peut être autorisé que si une analyse approfondie, conduite sous son contrôle par type de données, permet, en l'état des possibilités techniques, d'en éliminer le contenu des communications. Ainsi, en ce qui concerne les *URL*, seuls les éléments qui déterminent le chemin utilisé pour échanger des correspondances ou consulter des informations peuvent être recueillis, les autres éléments devant être éliminés. C'est à

[8] Cette obligation de conservation résulte, pour les opérateurs de communications électroniques, de l'article L. 34-1 du code des postes et des communications électroniques et, pour les hébergeurs et les fournisseurs de services sur internet, de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[9] *Uniform resource locator*.

cette condition que la CNCTR admet le recueil d'*URL* dans le cadre d'accès administratifs aux données de connexion.

- Les données mentionnées au 4°, à savoir celles « *relatives à l'acheminement des communications électroniques par les réseaux* », permettent de reconstituer le trajet de communications découpées en paquets susceptibles d'emprunter des routes différentes en fonction de l'encombrement du trafic, de la qualité du service offert, des accords entre opérateurs ou d'autres paramètres. Elles sont, pour la CNCTR, à destination exclusive des équipements des réseaux intermédiaires traversés et constituent donc des données de connexion.

- Les données mentionnées au 5°, à savoir celles « *relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service en ligne* », incluent les *login* et mots de passe des personnes. La CNCTR estime que ces données sont exemptes de contenu de communications et constituent des données de connexion.

- Les données mentionnées au 6°, à savoir « *les caractéristiques techniques des équipements terminaux et les données de configuration de leurs logiciels* », désignent notamment des informations émises par un *smartphone* sans que son utilisateur le demande, telle celles relatives à leurs paramètres d'affichage (taille d'écran, format audio, capacités de mémoire, type de système d'exploitation, liste des applications et numéros de version, *etc.*). La CNCTR estime que ces données sont exemptes de contenu de communications et constituent des données de connexion.

La CNCTR souligne que les développements ci-dessus sur la nature des données de connexion constituent une analyse globale, empirique, non exhaustive et non définitive. Cette analyse a vocation à être approfondie, en particulier lors de la rédaction de l'arrêté tarifaire prévu au nouvel article R. 873-2 du code de la sécurité intérieure, qui doit énumérer les prestations pouvant être demandées aux opérateurs de communications électroniques, aux hébergeurs et aux fournisseurs de services sur internet pour recueillir les données de connexion. La CNCTR révisera en outre périodiquement l'analyse en fonction des évolutions techniques. Elle demande en conséquence que les nouveaux types de données qui pourraient être regardées comme faisant partie des données de connexion fassent l'objet d'un avis de sa part avant toute autorisation de recueil, afin qu'elle puisse s'assurer qu'aucun contenu de communications ne sera collecté.

2. <u>Sur le mode de recueil des données de connexion</u>

a) S'agissant de l'accès administratif aux données de connexion prévu à l'article L. 851-1 du code de la sécurité intérieure, la CNCTR considère que la loi, eu égard tant à sa rédaction qu'aux travaux parlementaires qui ont précédé son adoption, n'a ni pour objet ni pour effet de permettre le recueil en temps réel des données, qui doit être expressément prévu, comme il l'est aux articles L. 851-2 et L. 851-4 du code. Le recueil autorisé sur le fondement de l'article L. 851-1 du code ne peut donc intervenir qu'en temps différé.

A cet égard, dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel, après avoir analysé les dispositions des articles L. 851-1 et L. 851-2 du code de la sécurité intérieure, a jugé « *qu'en outre, lorsque le recueil des données a lieu en temps réel, il ne*

pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code » (considérant 56), c'est-à-dire dans les conditions prévues à l'article L. 851-2.

En conséquence, les données de connexion susceptibles d'être recueillies en application de l'article L. 851-1 du code de la sécurité intérieure ne peuvent être que des données préalablement conservées par les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet. Il s'agit, par définition, des données mentionnées au 1° du I du nouvel article R. 851-5 du code.

La CNCTR souhaite que le cadre juridique exposé ci-dessus ressorte clairement des dispositions du projet de décret. Elle note que, dans sa saisine rectificative, le Premier ministre indique garantir que « *les données de connexion traitées par les réseaux mais non conservées ne peuvent pas être recueillies dans le cadre de l'article L. 851-1* » du code de la sécurité intérieure. Cette garantie est censée être apportée par le II du nouvel article R. 851-5 du code, aux termes duquel : « *Les informations énumérées aux 2° à 6° du I ne peuvent être recueillies qu'en application des articles L. 851-2 à L. 851-6, dans les conditions et limites prévues par ces articles* ».

La CNCTR préconise une rédaction plus directe, plus complète et, partant, plus sûre. Elle propose que le II du nouvel article R. 851-5 du code de la sécurité intérieure soit ainsi rédigé :

« II. - Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé. ».

Si le Gouvernement souhaitait conserver au surplus l'alinéa du II figurant dans la saisine rectificative, la CNCTR recommanderait de modifier les références qu'il contient. Seuls les articles L. 851-2 et L. 851-3 du code de la sécurité intérieure se réfèrent en effet à l'ensemble des données de connexion mentionnées à l'article L. 851-1 du même code, dont la nature doit être précisée par décret en Conseil d'Etat. En revanche, les articles L. 851-4 à L. 851-6 du code définissent chacun de façon autonome les données susceptibles d'être recueillies sur leur fondement : il s'agit des « *données techniques relatives à la localisation des équipements terminaux utilisés* » à l'article L. 851-4, des données permettant « *la localisation en temps réel d'une personne, d'un véhicule ou d'un objet* » à l'article L. 851-5 et des « *données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que [d]es données relatives à la localisation des équipements terminaux utilisés* » à l'article L. 851-6. La CNCTR propose dès lors que la référence aux articles L. 851-4 à L. 851-6 soit supprimée et que l'alinéa soit ainsi rédigé :

« Les informations énumérées aux 2° à 6° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3, dans les conditions et limites prévues par ces articles. ».

b) En ce qui concerne l'accès administratif aux données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure, la CNCTR observe que ce recueil s'effectue, aux termes de la loi, « *sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1* » du code.

Au nouvel article R. 851-7 du code de la sécurité intérieure, le projet de décret dispose que lorsque le recueil en temps réel est demandé par des services de renseignement dits « du second cercle », il est effectué par le groupement interministériel de contrôle (GIC). La CNCTR estime cette procédure conforme à la loi.

Par ailleurs, pour le bon déroulement des contrôles *a posteriori* dont la loi l'a chargée, la CNCTR demande qu'un accès permanent, complet, direct et immédiat à l'ensemble des données de connexion recueillies en application de l'article L. 851-2 du code de la sécurité intérieure, quel que soit le service demandeur, lui soit garanti dans les locaux du GIC.

3. Sur les services de renseignement dits « du second cercle » pouvant être autorisés à recueillir les données de connexion en temps réel en application de l'article L. 851-2 du code de la sécurité intérieure

Dans sa saisine rectificative, le Premier ministre ouvre à certains services de renseignement dits « du second cercle » la possibilité de recueillir les données de connexion en temps réel en application de l'article L. 851-2 du code de la sécurité intérieure. En créant un nouvel article R. 851-1-1 dans le code, le Gouvernement souhaite ainsi modifier la liste des services du second cercle pouvant être autorisés à mettre en œuvre les techniques de renseignement prévues au livre VIII du code, sur laquelle s'était prononcée la CNCTR par sa délibération n° 2/2015 du 12 novembre 2015[10].

S'agissant d'une technique de renseignement que le Gouvernement n'avait initialement pas destinée aux services du second cercle et qui suppose une expertise technique spécifique, la CNCTR préconise une approche restrictive.

En premier lieu, la CNCTR rappelle que l'unité de coordination de la lutte contre le terrorisme (UCLAT) est chargée, par l'arrêté du 8 octobre 1984 qui la crée, d'une mission de coordination, d'animation et d'orientation des directions et services actifs de police en matière de lutte contre le terrorisme. Comme dans sa délibération du n° 2/2015 du 12 novembre 2015, la CNCTR estime que l'UCLAT n'a pas de rôle opérationnel justifiant que lui soit donné accès à des techniques de renseignement. Elle émet donc un avis défavorable à la proposition de lui donner un accès aux données de connexion en temps réel sur le fondement de l'article L. 851-2 du code de la sécurité intérieure.

En second lieu, la CNCTR estime que le caractère intrusif du recueil de données de connexion prévu à l'article L. 851-2 du code de la sécurité intérieure aussi bien que les ressources qu'il exige de mobiliser conduit à en faire un dispositif centralisé, réservé à quelques services de portée principalement nationale.

[10] Le projet de décret sur lequel a porté la délibération de la CNCTR est devenu le décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure.

Pour cette raison, la CNCTR émet un avis favorable concernant les seuls services suivants :

1° Services placés sous l'autorité du directeur général de la police nationale :

a) A la direction centrale de la police judiciaire : la sous-direction anti-terroriste et la sous-direction de la lutte contre la cybercriminalité ;

b) A la direction centrale de la sécurité publique : l'unité nationale de recherche et d'appui des services du renseignement territorial ;

2° Unités placées sous l'autorité du directeur général de la gendarmerie nationale :

A la direction des opérations et de l'emploi : la sous-direction de l'anticipation opérationnelle et la sous-direction de la police judiciaire ;

3° Services placés sous l'autorité du préfet de police de Paris :

a) A la direction du renseignement : la sous-direction de la sécurité intérieure et la sous-direction du renseignement territorial ;

b) A la direction régionale de la police judiciaire de Paris : la section antiterroriste de la brigade criminelle de la sous-direction des brigades centrales.

4. Sur les missions du groupement interministériel de contrôle

La CNCTR estime que la rédaction du nouvel article R. 822-1 du code de la sécurité intérieure, qui définit les missions du GIC, doit être complétée.

La CNCTR rappelle, comme elle l'a déjà indiqué dans sa délibération n° 2/2015 du 12 novembre 2015, que le GIC lui paraît devoir jouer, d'une manière générale, un rôle essentiel dans la traçabilité de la mise en œuvre des techniques de renseignement et dans la centralisation des informations recueillies, auxquelles elle doit disposer d'un accès libre et permanent pour exercer le contrôle *a posteriori* dont elle est chargée par la loi. Elle souhaite donc que le nouvel article R. 822-1 du code de la sécurité intérieure confie explicitement au GIC des missions dans ces deux domaines. Elle suggère d'ajouter dans le projet d'article les deux alinéas suivants :

« 5° Contribuer à la centralisation des renseignements collectés lors de la mise en œuvre des techniques de renseignement autres que celles mentionnées aux 3° et 4° ;

« 6° Concourir à la traçabilité de l'exécution des techniques de renseignement. ».

La CNCTR appelle en outre à nouveau l'attention du Gouvernement sur l'urgence s'attachant à organiser cette traçabilité et à définir les modalités de cette centralisation, ainsi que l'exigent les articles L. 822-1 et L. 854-4 du code de la sécurité intérieure.

5. Sur l'autorisation de plein droit accordée à certains services de l'Etat pour fabriquer des appareils et dispositifs techniques permettant de porter atteinte à la vie privée

La CNCTR relève que le Gouvernement souhaite modifier l'article R. 226-5 du code pénal pour accorder de plein droit à certains services de l'Etat désignés par arrêté du Premier ministre l'autorisation de fabriquer des appareils et dispositifs techniques permettant de porter atteinte à la vie privée et, en l'espèce, de mettre en œuvre des techniques de renseignement prévues au livre VIII du code de la sécurité intérieure.

La CNCTR, comme la CNCIS avant elle, souligne qu'un contrôle efficace des atteintes portées à la vie privée suppose non seulement de vérifier la légalité des demandes de mise en œuvre des techniques de renseignement par les services de l'Etat, mais également de réguler les opérations de commercialisation et d'acquisition par des sociétés privées ou par les services de l'Etat des appareils et dispositifs techniques qui permettent d'intercepter des communications électroniques ou de capter des données personnelles.

En conséquence, si elle admet que soit accordée l'autorisation de plein droit évoquée ci-dessus, la CNCTR recommande que le registre prévu à l'article R. 226-10 du code pénal et défini par arrêté du 16 août 2006 soit modifié afin de retracer non seulement les opérations de commercialisation portant sur les appareils et dispositifs techniques contrôlés mais également celles de fabrication. Le registre ainsi tenu devra attester, même succinctement, les fonctionnalités des appareils et dispositifs techniques fabriqués ainsi que leur adéquation aux missions confiées aux services bénéficiaires de l'autorisation de plein droit.

Délibéré en formation plénière le 14 janvier 2016

Francis DELON

Président de la Commission nationale
de contrôle des techniques de renseignement