

## AVIS DU COMITÉ PERMANENT R SUR LA PROPOSITION DE LOI RELATIVE AUX MÉTHODES DE RECUEIL DES DONNÉES DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

### INTRODUCTION

Le 21 janvier 2009, Monsieur Patrick Vankrunkelsven, président de la commission Justice du Sénat, a demandé au Comité permanent R de rendre un avis le 28 janvier sur la proposition de loi relative aux méthodes de recueil des données des services de renseignement et de sécurité.

Le Comité permanent R a étudié la proposition de loi aussi minutieusement que possible, compte tenu du court laps de temps qui lui était imparti pour rendre son avis. Le comité a en outre particulièrement focalisé son attention sur la protection des droits fondamentaux des personnes et sur l'efficacité et la coordination des deux services belges de renseignement et de sécurité. Le Comité permanent R n'a pas pour ambition de rendre une étude complète et définitive sur la proposition de loi.

Le Comité permanent R tient avant tout à souligner que – d'abord par le gouvernement Verhofstadt II pour le projet de loi initial et ensuite par les sénateurs qui ont déposé la présente proposition de loi – nombre de ses avis et réflexions ont déjà été suivis. Le Comité permanent R se réjouit tout particulièrement du fait que le contrôle *ex posteriori*, qui

revenait initialement à un collège à créer – est du ressort du Comité permanent R dans la proposition actuelle. Cette option ne peut que profiter au contrôle démocratique des services de renseignement.

Dans le présent avis, le Comité permanent R tient à formuler certaines réflexions et remarques sur les articles. Certaines réflexions et remarques touchent au principe; d'autres sont plutôt techniques. Elles ne concernent toutefois pas le fond de l'affaire: la nécessité urgente d'attribuer des compétences complémentaires aux services de renseignement, par le biais d'une base légale claire, où l'attention nécessaire est accordée à la protection des droits et des libertés des citoyens.<sup>122</sup> Le Comité permanent R répète que la situation actuelle, c'est-à-dire que les services de renseignement belges ne disposent que de quelques compétences opérationnelles, qui ne sont que vaguement décrites, n'est plus tenable. Les menaces actuelles (p. ex. l'extrémisme et le terrorisme) contre la pérennité de l'état démocratique et de l'Etat providence et la position des services de renseignement par rapport à leurs homologues étrangers, contraignent les autorités à franchir ce pas.

## COMMENTAIRE DES ARTICLES

### Article 2

L'article 2, 1<sup>o</sup>, de la proposition de loi ajoute un deuxième paragraphe à l'article 2 de la Loi du 30 novembre 1998.

Dans la lecture actuelle de l'alinéa 1er, il est absolument impossible, même d'une manière passive, d'avoir connaissance d'informations particulièrement intéressantes (comme p. ex. un attentat imminent) provenant d'un titulaire d'une profession qui rompt le secret de ses sources en raison de l'état d'alerte. Si un service de renseignement demeure passif et reçoit l'information de cette manière, de telles informations doivent pouvoir être utilisées.

Dans l'alinéa 4, il est requis qu'un membre de la commission soit 'présent' lors de la mise en oeuvre d'une méthode exceptionnelle. En raison du caractère continu et prolongé de certaines méthodes, c'est matériellement impossible.

Toujours dans l'alinéa 4, un suppléant pour le président de la commission et un suppléant pour le président de l'Ordre doivent être prévus. En outre, il convient de prévoir une réglementation pour le cas où un représentant de l'Ordre n'est pas présent. Le fonctionnement d'un service de renseignement ne peut en être hypothéqué.

En cas d'application de l'article 18/2 à l'égard d'un avocat ou d'un médecin, la proposition détermine, dans son article 2, 2<sup>o</sup>, alinéa 2, que cette mesure ne peut être exécutée qu'après que le président de l'Ordre auquel appartient le médecin ou l'avocat ait été informé et que les renseignements nécessaires lui aient été transmis. Pour autant que ces renseignements soient classifiés, ce qui n'est pas improbable, cette disposition restera

<sup>122</sup> Voir e.a. les Rapports d'activités suivants du Comité permanent R : 1996, pp. 26-53; 1999, p.71 et suiv.; 2000, p.53; 2001, pp. 212-222. Voir également l'audition avec le président du Comité permanent R à propos des activités préparatoires relatives à la compétence d'interception du SGRS (*Doc.parl.* 2002-2003, 2059/3, 7). Voir aussi l'avis du Comité permanent R dans le projet de loi initial qui a été introduit par le gouvernement Verhofstadt II (*Doc.parl.*, Sénat, 2005-2006, 2138/1 et Comité permanent R, *Rapport d'activités 2006*, Anvers, Intersentia, 2007, 70-81) et le memorandum du Comité à l'informateur du Roi (Comité permanent R, *Rapport d'activités 2007*, Anvers, Intersentia, 2007, 50-52).

lettre morte. Du reste, il n'est mentionné nulle part que le président de l'Ordre est passible d'une sanction pénale s'il ne prend pas toutes les mesures pour garantir la confidentialité des renseignements reçus. Il faut clairement différencier ce délit d'omission du délit actif stipulé à l'art. 458 du Code pénal. Soumettre le président de l'Ordre et son suppléant au régime des habilitations de sécurité pourrait constituer une solution.

L'article 2,3° de la proposition de loi ajoute un troisième paragraphe à l'article 2 de la Loi du 30 novembre 1998. Cette disposition stipule que les citoyens qui ont fait l'objet d'une méthode spécifique ou exceptionnelle en sont informés après une période de cinq ans. Le texte actuel prévoit toutefois que cela peut se faire « sans préjudice de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité ». En d'autres termes : quand une donnée est classifiée, on ne peut rien communiquer. Dans la précédente lecture de cette disposition, une évaluation était encore possible. Cette obligation de notification ne sera-t-elle pas pratiquement minée étant donné que l'utilisation de méthodes spécifiques et (certainement) exceptionnelles fera souvent l'objet d'une classification ?

Dans le même paragraphe, le terme « wettelijk » doit être remplacé par « legitiem ».

Toujours dans le même paragraphe, il est stipulé que le dirigeant du service informe la commission de chaque demande d'informations et de la réponse fournie par le service de renseignement. Dans le projet initial, le collège (à présent le Comité permanent R) en était informé. Le Comité permanent R estime qu'il est important que l'organe de contrôle parlementaire ait une vision complète du respect de l'obligation de notification.

#### Article 3

Une définition du « processus de radicalisation » est donnée dans le point 15°. Vu la définition large que le législateur a donnée à la notion de 'crimes terroristes', le Comité permanent R est d'avis d'utiliser ce terme et ne pas faire référence aux 'actes terroristes', qui semblent encore plus vaste.

#### Article 5

La tutelle conjointe du ministre de l'Intérieur est retirée, alors que ce ministre a bel et bien autorité (sous la forme d'un droit de réquisition) sur la Sécurité de l'Etat concernant la protection des personnes. Une tutelle conjointe semble dès lors indiquée.

Le Comité permanent R tient, dans ce cadre, à souligner qu'il attache une grande importance à une responsabilité politique partagée sur les services de renseignement : *« Confier à un seul ministre la responsabilité politique des services de sécurité comporte des risques inhérents à toute concentration de pouvoir dans les mains d'un seul homme. »*<sup>123</sup>

#### Article 6

L'alinéa 2 de la proposition de loi prête à confusion si elle est lue en regard de l'art. 18/1 et de l'art. 20 de la loi dans sa version modifiée. Il n'est pas clair si et quelles méthodes (ordinaires/spécifiques/exceptionnelles) peuvent être utilisées pour prêter assistance aux autorités judiciaires ou même administratives.

Le même problème se pose si cette disposition est lue en regard de l'article 19 de la Loi du 11 décembre 1998 relative à la classification. Pour des matières d'une telle importance, il ne peut subsister la moindre confusion sur la volonté du législateur.

<sup>123</sup> Comité permanent R, *Rapport complémentaire d'activités 1999*, 90.

De plus, certaines méthodes demeurent exclues dans le cadre de la mission de protection de personnalités importantes.

Hormis le fait que les dispositions donnent lieu à des interprétations diverses, le Comité permanent R s'interroge sur la nécessité de faire appel à des services de renseignement, qui ont leur finalité propre et leur propre raison d'être dans une démocratie, pour des missions judiciaires. En faisant appel à des services de renseignement pour des missions judiciaires, on leur enlève une partie de leur capacité de renseignement (déjà entamée) de leur tâche première : le travail de renseignement. Les services de renseignement ont pour mission principale d'utiliser leur capacité dans le cadre de menaces liées au terrorisme, au potentiel scientifique et économique, à la prolifération et aux organisations sectaires... Si cette capacité est réservée pour des missions judiciaires ou administratives, cela aura inévitablement des conséquences sur la qualité des analyses relatives à la menace et des '*intelligence failures*' risqueraient de se produire.

À la lecture de la réglementation proposée, les autorités judiciaires semblent pouvoir, par exemple, demander aux services de renseignement de procéder à des observations ou de fouiller un lieu privé. Mais cela pourrait aussi signifier que certaines méthodes de renseignement pourraient être utilisées par les services de renseignement dans le cadre d'une information judiciaire et cela, alors que ces mêmes méthodes ne peuvent normalement être utilisées dans des instructions judiciaires que sous certaines conditions strictes. C'est par exemple le cas pour l'enregistrement des données de télécommunication : il ne peut être ordonné que par le procureur du Roi dans le cadre d'une enquête pénale, en cas de flagrant délit, mais peut être tout simplement demandé par un officier du renseignement dans le cadre d'un travail de renseignement. La tentation est alors forte de choisir la voie de la moindre résistance 'légale'. La possibilité d'une telle interprétation dans l'avant-projet est inquiétante.

Le Comité permanent R estime qu'au contraire, il convient d'emprunter la voie inverse : la possibilité de collaborer doit être supprimée ou ne doit être rendue possible qu'à titre très exceptionnel, dans des cas décrits dans la loi (par ex. en cas de menace imminente de certains délits). En outre, l'assistance technique doit être réduite à son essence-même : apporter un soutien aux autorités judiciaires en leur prodiguant des conseils techniques et en leur prêtant une assistance technique dans le cadre d'actes posés par le pouvoir judiciaire.

Le Comité permanent R constate en outre que, malgré ses recommandations antérieures, il n'y a toujours pas, à ce jour, de définition claire des notions de '*collaboration*' et de '*assistance technique*'. Le législateur a néanmoins confié cette tâche en 1998 aux ministres concernés, qui devaient établir un protocole à ce sujet. Le Comité permanent R recommande d'utiliser cet avant-projet pour définir ces notions dans la loi et, en même temps, en donner une portée limitée.

Enfin, le Comité permanent R tient à attirer l'attention sur le fait que la réglementation proposée semble aussi impliquer que les services de renseignement peuvent prêter leur concours aux autorités administratives et qu'ils peuvent faire appel à cet effet à des méthodes ordinaires ou même spécifiques.

#### Article 7

L'art. 13bis proposé n'offre pas d'exonération pour des délits lorsque des méthodes ordinaires sont utilisées, comme p. ex. la filature, au cours de laquelle des infractions de

roulage doivent être commises pour ne pas perdre de vue une *target*. C'était néanmoins le but recherché au départ, avec en arrière-pensée la fuite d'Erdal.

L'alinéa 3 du paragraphe 2 qui est proposé va très loin. Il permet apparemment à des citoyens-infiltrants, ou même à des agents des services extérieurs à qui les services de renseignement belges ont fait appel, de commettre des délits. De surcroît, les termes utilisés ('ont fourni') laissent supposer qu'une exonération peut être accordée *a posteriori*.

#### Article 8

L'article 8 confirme la primauté absolue de l'instruction judiciaire sur le travail de renseignement. Le Comité permanent R a déjà plusieurs fois souligné qu'il ne peut adhérer à ce choix. Les deux finalités (travail de renseignement et travail judiciaire) ont chacun leur intérêt et l'un ne peut passer devant l'autre sans aucune raison. En d'autres termes, il est faux de dire que chaque enquête judiciaire est par définition aussi importante que n'importe quelle enquête de renseignement. Le Comité permanent R est d'avis que si les services de renseignement doivent être attentifs aux intérêts du judiciaire, l'inverse est vrai aussi: la police et le pouvoir judiciaire doivent considérer que le recueil du renseignement est important. Si les intérêts des parties convergent, il doit y avoir une concertation et, au besoin, – s'il y a par ex. une contestation sur les intérêts en cause – la commission ou le ministre responsable politiquement se doit de trancher.

Le Comité permanent R tient aussi à souligner que le démarrage d'une enquête par un service de renseignement ne nécessite aucun acte formel et ne peut pas toujours être daté et situé précisément. Les termes utilisés dans la première phase de l'alinéa 2 sont inadaptés à cet égard.

#### Article 9

Le Comité permanent R continue d'insister sur le fait qu'il faut profiter de cette proposition de loi pour aboutir à une réglementation complète en ce qui concerne les méthodes ordinaires. Ces méthodes seront en fin de compte utilisées quotidiennement par les services concernés. Elles ne font néanmoins pas l'objet de normes suffisamment claires dans la législation telle qu'elle existe, au regard des critères de la Convention européenne des Droits de l'Homme.

Le Comité permanent R pense plus précisément à l'observation, à la surveillance et à la filature (qui peut apparemment être illimitée dans le temps tant qu'on ne procède pas à une observation de lieux privés), à l'infiltration (pour autant qu'elle puisse être considérée comme une méthode ordinaire) et au fonctionnement des informateurs. De récents dossiers renforcent le Comité dans sa conviction. Une réglementation (secrète) du Comité ministériel du renseignement et de la sécurité (art.13 de la proposition de loi) en la matière ne suffit pas. Tout comme cette méthode – délicate, il est vrai – a été réglée dans la Loi sur les méthodes particulières de recherche, la même chose devrait être possible avec la Loi sur les méthodes de recueil des données.

#### Article 10

Si l'alinéa 2 de l'art. 14 'dans le respect de la loi' (qui n'était effectivement pas clair) est remplacé par 'dans le respect de la présente loi', il doit en être de même dans l'alinéa 1<sup>er</sup>.

Le Comité permanent R avait insisté dans son premier avis sur l'éclaircissement de cette disposition. Elle ne comprend pas non plus la portée de la modification proposée. La signification en était vraisemblablement que ces personnes ne sont pas liées par le secret professionnel ni par les exigences de la Loi sur le traitement des données à caractère personnel. Le Comité permanent R peut adhérer à une telle interprétation.

Le Comité permanent R est d'avis que les motifs de refus pour la communication de données (alinéa 3) doivent être limités aux cas de danger pour l'intégrité physique de tiers.

En outre, il doit être prévu qu'une troisième instance (la commission semble ici particulièrement indiquée) puisse se prononcer en dernier ressort sur un éventuel refus.

Dans l'alinéa 4 (où on parle subitement de 'législation en vigueur'), la notion de '*secteur public*' est maintenu. Pour le Comité permanent R, ce n'est pas clair de prime abord. Les autorités judiciaires en font-elles partie? Cette notion a-t-elle une signification large comme dans la Loi actuelle du 30 novembre 1998?

#### Article 14

Dans la disposition qui doit devenir l'[article 18/3](#) de la Loi du 30 novembre 1998, l'alinéa 2 du paragraphe 1<sup>er</sup> stipule que préalablement à l'utilisation de la méthode à l'égard p. ex. d'un avocat, il doit exister des indices concrets attestant que l'intéressé se livre à de telles pratiques. Ce ne sera pas possible dans tous les cas. Ce n'est qu'après avoir contrôlé, par exemple, une adresse IP que l'on peut savoir si l'on a affaire à un avocat.

Dans la disposition qui doit devenir l'[article 18/4, §2](#), alinéa 1<sup>er</sup><sup>124</sup>, un rapportage mensuel de l'utilisation des méthodes spécifiques est prévu. Le Comité permanent R se demande toutefois comment un contrôle effectif et une réparation adéquate peuvent être garantis si la commission n'est informée que mensuellement de la liste des méthodes spécifiques mises en œuvre. Rien n'empêche que la commission soit immédiatement informée.

Dans la disposition qui doit devenir l'[article 18/4, §2, alinéa 4](#)<sup>125</sup>, une interdiction 'd'exploitation' de données recueillies illégalement est prévue. Posé en principe, il aura certainement un effet autorégulateur. Le Comité permanent R s'interroge sur l'efficacité, la portée et l'opportunité d'une telle mesure. Tout d'abord, cette mesure ne sera pas toujours *effective*. La commission doit donc être informée après un certain temps de l'utilisation de moyens spécifiques ou le service de renseignement pourrait avoir la possibilité d'utiliser des moyens spécifiques ou exceptionnels sans en informer la commission. Les informations recueillies de cette manière seront déjà pour la plupart traitées par les services d'analyse de ces services de renseignement. En outre, il est possible que ces données soient envoyées à – et utilisées par d'autres autorités. Le Comité permanent R pense ici par exemple à l'OCAM, qui procèdera à des analyses stratégiques et ponctuelles sur la base des données, à l'Autorité nationale de sécurité qui décide de l'octroi des habilitations de sécurité, aux autorités judiciaires qui peuvent utiliser ces informations comme informations de départ ou information leur permettant de diriger une recherche ou encore comme preuve, ou même des services étrangers... Alors, se pose la question de

---

<sup>124</sup> La même remarque vaut naturellement pour les dispositions semblables de l'art. 14 de la proposition.

<sup>125</sup> La même remarque vaut naturellement pour les dispositions semblables de l'art. 14 de la proposition.

la portée de l'interdiction 'd'exploitation'. Cette interdiction vaut-elle seulement pour l'avenir ou concerne-t-elle des données qui ont déjà été transmises ou traitées? Cette interdiction vaut-elle seulement pour les deux services belges de renseignement comme le texte de l'avant-projet le laisse supposer? Ou en d'autres termes: les données peuvent-elles encore être utilisées dans une procédure administrative ou judiciaire et quelle sanction est prévue en cas d'utilisation éventuelle? Plus importante est la question de savoir si une telle interdiction d'usage absolue est souhaitable. Si un service de renseignement effectue une perquisition juste après l'expiration de l'habilitation octroyée<sup>126</sup> et à cette occasion est informé qu'une attaque terroriste se prépare, la sanction telle que prévue dans le projet est disproportionnée. Toutefois, quand, dans le cadre d'une enquête de sécurité, une personne est mise sur écoute<sup>127</sup> pendant des mois, et qu'à cette occasion une banalité est mise au jour, le Comité permanent R est d'avis que cette information ne peut être utilisée contre l'intéressé. Par conséquent, le Comité permanent R pense qu'en cas d'usage de la sanction prévue, une évaluation raisonnable de l'intérêt individuel et de l'intérêt général doit être rendue possible. A cet effet, la jurisprudence de la Cour de Cassation concernant 'la preuve obtenue illégalement' peut éventuellement constituer une source d'inspiration.

Le Comité permanent R tient immédiatement à ajouter que chaque fois qu'il est constaté qu'un membre d'un service de renseignement a recueilli des données de façon illégale, une enquête disciplinaire ou même pénale doit être lancée. En effet, nombreuses sont les méthodes exceptionnelles qui sont punissables si elles sont utilisées en dehors du cadre de la proposition de loi (par ex. fraude à l'identité, interdiction d'écoute et d'enregistrement, violation de domicile, criminalité informatique...). Le Comité permanent R pense que le minimum et le maximum des peines fixées dans ces dispositions doivent être doublés compte tenu de la qualité des éventuels contrevenants. Plus que l'interdiction d'exploitation des données, cette sanction semble plus adaptée et aura certainement un effet dissuasif.

Dans la disposition qui doit devenir l'article 18/6, §1, alinéa 1<sup>er</sup><sup>128</sup>, il est prévu que l'opérateur reçoive une question motivée. Le Comité permanent R est très certainement d'avis que chaque requête doit être motivée, mais d'autre part, il n'y a aucune raison de porter ces motivations à la connaissance de l'opérateur. Au contraire, tant la protection de la vie privée que les intérêts publics s'y opposent. La motivation doit être connue de la commission et du Comité permanent R.

Dans la disposition qui doit devenir l'article 18/10, §1, alinéa 1<sup>er</sup>, il est stipulé que le dirigeant du service demande une autorisation pour l'utilisation de la méthode exceptionnelle. Le Comité permanent R se demande si on ne doit pas envisager, tout comme dans le cas des compétences d'interception dont le SGRS dispose actuellement (art 44bis de la L.R&S), d'exiger l'autorisation préalable du ministre compétent pour les méthodes exceptionnelles. Cette façon de procéder, par laquelle les plus hautes autorités politiques prennent elles-mêmes la décision et, qui plus est, portent la responsabilité d'autoriser des mesures très intrusives (surtout les mises sur écoute), est d'application aux Pays-Bas et en Grande-Bretagne.

<sup>126</sup> La proposition de loi prévoit e.a. le fait que la période au cours de laquelle les méthodes exceptionnelles peuvent être utilisées, doit être fixée préalablement.

<sup>127</sup> La proposition de loi l'interdit.

<sup>128</sup> La même remarque vaut naturellement pour les dispositions semblables de l'art. 14 de la proposition.

Dans la disposition qui doit devenir l'article 18/10, §3, alinéa 1<sup>er</sup>, il est stipulé que la commission doit rendre un avis conforme endéans les trois jours ouvrables. Compte tenu des week-ends et des jours fériés, le Comité permanent R est d'avis que ce délai peut être trop long. Le risque existe alors qu'il puisse être fait usage plus rapidement de la possibilité d'exception reprise dans le paragraphe 4.

Dans la disposition qui doit devenir l'article 18/10, §4, un éventuel suppléant doit être chaque fois prévu. En outre, l'alinéa 1<sup>er</sup> de ce paragraphe doit être complété dans le sens que la commission prend la décision finale une fois qu'elle est au courant de l'affaire.

Dans la disposition qui doit devenir l'article 18/10, §7, le '§4' doit être remplacé par '§5' et le '§5' par '§6'.

Dans la disposition qui doit devenir l'article 18/12, alinéa 4, il semble indiqué de ramener de trois à deux mois le délai de remise des rapports à la commission (ce qui correspond à la durée de l'habilitation). Dans la même disposition, il convient de définir qui décide des modalités de dissolution et de liquidation si le Comité permanent R prend la décision d'en finir avec ces méthodes.

Dans la disposition qui doit devenir l'article 18/16, le Comité permanent R tient à insister sur deux limitations. D'une part, la possibilité de pénétrer dans des bâtiments pour avoir accès à des systèmes informatiques n'est pas prévue. D'autre part, tous les systèmes informatiques publics sont exclus, alors qu'il n'est pas impensable que des personnes manipulent justement ces systèmes pour poursuivre leurs activités.

Le Comité permanent R veut attirer l'attention sur le fait que la disposition qui doit devenir l'article 18/17, §4, alinéa 2, n'est pas praticable dans le sens où la réglementation implique que le dirigeant du service ou le Directeur des Opérations doit écouter lui-même toutes les communications pour indiquer quels passages peuvent être transcrits.

La disposition qui doit devenir l'article 18/18, §7, établit que 'l'exploitation' de données provenant d'écoutes est limitée à un an. Le Comité permanent R s'interroge sur la portée, l'opportunité et la praticabilité d'une telle limitation. Qu'advient-il des données et analyses qui sont basées sur ces informations? Les informations peuvent-elles encore être utilisées dans le cadre d'enquêtes de sécurité? Peuvent-elles encore être exploitées dans le cadre judiciaire? L'avant-projet n'apporte pas de réponse à ces questions. Le Comité permanent R ne voit d'ailleurs pas une telle réglementation pour les données recueillies par le biais d'autres méthodes (parfois très intrusives). Cette disposition va à l'encontre du fonctionnement spécifique des services de renseignement qui peuvent juste constituer leurs renseignements en groupant et en analysant les informations qui ont été recueillies depuis longtemps à l'aide de diverses méthodes.

#### Article 15

Selon l'article 15 de la proposition de loi, l'article 29 du Code d'instruction criminelle qui stipule une obligation de dénonciation pour les fonctionnaires qui, dans l'exercice de leurs fonctions, ont connaissance de faits punissables, est maintenu. L'obligation de dénonciation est même élargie à certains faits dont on suppose qu'ils vont être commis. Une telle obligation de dénonciation absolue peut mettre en péril des opérations en cours menées par un service de renseignement, sans qu'il soit possible d'évaluer l'intérêt d'une poursuite et l'intérêt qu'un service de renseignement continue à suivre un phénomène ou un groupe. Le Comité permanent R avait déjà posé la question de l'utilité d'une obligation de dénonciation absolue. Dans son rapport d'activités 2004, le Comité a plaidé en faveur

d'une réglementation plus souple qui permettrait de choisir la meilleure voie (judiciaire ou renseignement).

Une obligation de dénonciation limitée est d'ailleurs aussi d'application aux Pays-Bas et en Allemagne. Le Comité permanent R est d'avis que cette décision de dénoncer certains faits ou non ou de reporter temporairement la dénonciation peut revenir à la commission. Cet organe évaluera à cet effet les différents intérêts en cause.

#### Article 16

Cette disposition modifie l'article 20 de la Loi du 30 novembre 1998.

Le Comité permanent R fait ici intégralement référence aux remarques formulées pour l'article 6. Il tient une fois encore à répéter qu'il souhaite donner une interprétation très limitée à la coopération avec d'autres services. Cependant, si le choix se porte sur une coopération effective des services, l'utilisation des compétences doit rester limitée aux méthodes ordinaires.

Le Comité permanent R est d'autre part d'avis qu'un autre aspect de l'article 20 de la Loi du 30 novembre 1998 doit être spécifié. Cela concerne la transmission de données à caractère personnel à des services étrangers. Actuellement, l'art. 20 stipule seulement qu'il doit y avoir une 'collaboration' avec les services de renseignement et de sécurité étrangers et que le Comité ministériel du renseignement et de la sécurité doit en définir les conditions. Le Comité permanent R n'a pas connaissance d'une telle réglementation à ce jour. Le comité est du reste d'avis que cette règle manque de précision, e.a. compte tenu des exigences stipulées dans le CEDH et dans la Loi sur le traitement des données à caractère personnel. Selon le Comité permanent R, les réglementations en vigueur aux Pays-Bas, en Allemagne et au Danemark peuvent constituer une source d'inspiration en la matière.

Ainsi, la Loi néerlandaise relative aux services de renseignement et de sécurité (2002) fixe explicitement la compétence de ces services pour communiquer leurs données, dans le cadre de la bonne exécution de leurs missions, à des services de renseignement et de sécurité d'autres pays ou à d'autres organes internationaux de sécurité, de renseignement et de liaison. En outre, cette loi énonce la règle du tiers service et en fixe les conditions. La transmission de données personnelles à des services extérieurs fait également l'objet de dispositions particulières. Elles mettent l'accent sur les données plutôt anciennes ou dont l'exactitude ne peut être établie. Il est également intéressant de signaler l'obligation de consigner toute remise de données à caractère personnel.

L'Allemagne a élaboré une réglementation similaire dans son *Bundesverfassungsschutzgesetz* (2002). Celle-ci stipule que le *Bundesamt für Verfassungsschutz* (BfV) peut communiquer des données personnelles à des autorités étrangères ainsi qu'à des instances internationales et supranationales, si cette communication est nécessaire à l'exécution de ses tâches ou à la protection d'intérêts de sécurité majeurs du destinataire. La transmission de données prend fin si elle va à l'encontre des intérêts étrangers de la République fédérale allemande ou d'intérêts supérieurs de l'instance concernée. Toutes les communications de données doivent être consignées. Le destinataire doit être averti que les données ne peuvent être utilisées qu'aux fins auxquelles elles ont été transmises. Il est en outre explicitement prévu que le BfV peut s'enquérir de l'usage prévu des données.

Le Danemark a lui aussi élaboré un règlement en la matière dans les *Internal guidelines for the handling of information*. La section 4-1 s'énonce de la manière suivante (traduction libre):

*« Des données peuvent être communiquées à des autorités policières ou des services de renseignement et de sécurité étrangers coopérants afin de parer à ou d'éviter des faits punissables ou de vérifier des informations. Cette communication ne peut toutefois intervenir qu'après évaluation de la proportionnalité entre l'objectif de la divulgation et ses conséquences pour l'individu. »* Le Comité permanent R tient encore à ajouter que l'organe de contrôle danois vérifie effectivement le respect des règles en vigueur en la matière. À cette fin, le service contrôlé est tenu de consigner toute transmission de données à l'étranger. L'organe de contrôle effectue des échantillons chaque année.

En somme, la loi en tant que telle doit être suffisamment claire sur la forme que peut prendre une éventuelle collaboration, vu qu'on peut imaginer qu'un service étranger peut par exemple demander à un de nos services de renseignement de mettre une personne sur écoute sur notre territoire.

#### Article 17

Dans la disposition qui doit devenir l'article 18/18, §7, le Comité permanent R recommande de porter la peine maximale à un an par souci d'uniformité avec la disposition qui doit devenir l'art. 48/8. En outre, la délivrance d'un mandat d'arrêt est de cette manière rendue possible.

#### Article 18

Cette disposition établit la commission. Le Comité permanent R insiste sur le rôle crucial de cette instance dans tous les aspects de la loi. Il est d'avis que la manière dont la commission est composée mènera à des situations intenable au niveau du travail, ce qui nuira sans aucun doute à l'efficacité (du contrôle) des méthodes spécifiques et particulières. Le Comité permanent R souhaite formuler des propositions et réflexions ponctuelles, en tenant compte du fait que la commission devra être opérationnelle 24 heures sur 24 et 7 jours sur 7 :

- la commission doit pouvoir disposer de quatre membres effectifs ;
- chaque membre doit avoir un suppléant, qui soit aussi effectivement disponible ;
- le pluralisme de l'expertise est indispensable dans la composition de la commission ;
- compte tenu de la charge de travail et des exigences de disponibilité, il n'est pas indiqué de faire appel à des 'magistrats honoraires' ;
- la combinaison des qualités requises et des incompatibilités (provisaires) rendent particulièrement difficile, voire impossible, la composition d'une commission ;
- en raison de l'indépendance de la commission et pour ne pas amputer une nouvelle fois les services de renseignement d'une partie de leur personnel (cf. l'OCAM dont le cadre a dû être rempli), la commission doit disposer d'un cadre propre et d'un greffier qui devra pouvoir soutenir la commission tant sur le plan matériel que sur le fond ;
- une clause d'obligation de secret doit être définie (cf. Comité permanent R) pour les membres et les membres du personnel de la commission.

#### Article 19

Le Comité permanent R réitère sa satisfaction de voir que l'idée du collège n'a pas été retenue dans la proposition, et que celle-ci octroie au Comité permanent R la compétence du contrôle *a posteriori*. Le Comité permanent R n'a que quatre remarques techniques à formuler à la réglementation proposée :

- dans la disposition qui doit devenir l'art. 43/5, alinéa 2 de la Loi du 30 novembre 1998, le délai dans lequel le Comité permanent R doit rendre sa décision peut être ramené à huit jours calendrier;
- dans la disposition qui doit devenir l'art. 43/6, §4 alinéa 3 de la Loi du 30 novembre 1998, les motifs de refus de témoigner doivent être ramenés à un seul motif: le danger pour l'intégrité physique de tiers;
- dans la disposition qui doit devenir l'art. 43/6, §4 alinéa 3 de la Loi du 30 novembre 1998, le président doit pouvoir désigner son suppléant en cas d'absence;
- la version française de la disposition qui doit devenir l'art. 43/6, §4 alinéa 4 de la Loi du 30 novembre 1998 ne correspond pas à la version néerlandaise. Cette dernière semble être la version correcte, selon le Comité permanent R.

#### Article 25

Le Comité permanent R recommande d'ajouter que les résultats obtenus ne peuvent être commentés qu'en termes généraux.

#### Une nouvelle disposition

Le Comité permanent R recommande que soient supprimés les termes « à l'exception de ceux qui concernent une information ou instruction judiciaire en cours » dans les articles 48, §2, alinéa 2, et 51 de la Loi de contrôle. Dans la proposition de loi, l'option déjà retenue est la suivante: les membres des services de renseignement ne peuvent invoquer le secret de l'instruction lorsqu'ils sont entendus par le Comité permanent R (voir l'article 43/6, §4, alinéa 2). A juste titre. Certainement dans le cas où les services de renseignement collaborent plus étroitement et plus fréquemment avec le pouvoir judiciaire, une grande partie de leur fonctionnement échappe au contrôle démocratique. La pratique a montré que le Comité permanent R peut à peine exercer son contrôle en cas d'information ou instruction judiciaire en cours. Ce manque de contrôle ne pourra jamais être totalement compensé par un contrôle judiciaire car, dans de nombreux cas, des données des services de renseignement ne se retrouvent pas dans le dossier d'instruction. En outre, la finalité du contrôle judiciaire se situe ailleurs.

Pour éviter tout malentendu concernant l'option choisie dans la présente proposition de loi, les articles 48, §2, alinéa 2, et 51 de la Loi du 18 juillet 1991 organique des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace doivent également être adaptés en ce sens.

Il n'y a donc aucun malentendu sur le fait que le Comité permanent R exerce aussi un contrôle sur le fonctionnement des services de renseignement quand ils prêtent leur concours à des instructions judiciaires, sans pour cela mettre en péril ces instructions ou émettre de jugement sur celles-ci. Cela signifie concrètement que le secret de l'instruction n'est pas opposable au Comité permanent R, mais que le Comité permanent R devient dépositaire de ce secret et doit dès lors en tenir compte dans la conduite de ses enquêtes et dans ses rapports.

#### Article 28

Le Comité permanent R s'interroge sur la nécessité des modifications de la Loi relative à la publicité de l'administration qui ont été proposées. L'art. 26 de la Loi du 11 décembre 1998

relative à la classification et aux habilitations, attestations et avis de sécurité prévoit en effet déjà un motif d'exception pour les données classifiées. Le problème réside toutefois dans le fait que le Conseil d'Etat a établi que l'autorité (donc la Sûreté de l'Etat ou le SGRS) doit démontrer que les données qu'un citoyen veut consulter sont classifiées. La question est naturellement de savoir comment ces services peuvent le faire autrement qu'en laissant consulter des documents, ce qui implique une violation de la classification.