

ROYAUME DE BELGIQUE

KONINKRIJK BELGIË

AVIS 32.623/4

DE LA SECTION DE LÉGISLATION
DU CONSEIL D'ÉTAT

ADVIES 32.623/4

VAN DE AFDELING WETGEVING
VAN DE RAAD VAN STATE

Le CONSEIL D'ÉTAT, section de législation, quatrième chambre, saisi par le Ministre de la Défense, le 29 novembre 2001, d'une demande d'avis, dans un délai ne dépassant pas un mois, sur un avant-projet de loi "modifiant l'article 44 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité", a donné le 28 janvier 2002 l'avis suivant :

De RAAD VAN STATE, afdeling wetgeving, vierde kamer, op 29 november 2001 door de Minister van Landsverdediging verzocht hem, binnen een termijn van ten hoogste een maand, van advies te dienen over een voorontwerp van wet "tot wijziging van artikel 44 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten", heeft op 28 januari 2002 het volgende advies gegeven :

OBSERVATIONS GENERALES

I. De la portée exacte de la disposition en projet

Selon l'article 259bis, § 5, du Code pénal, le Service général du renseignement et de la sécurité des forces armées est habilité à capter, à écouter, à prendre connaissance ou à enregistrer des radiocommunications militaires émises à l'étranger, et ce à des fins militaires.

L'avant-projet de loi modifie l'article 259bis, § 5, du Code pénal afin d'autoriser de manière plus large le Service général du renseignement et de la sécurité des forces armées à procéder à des captations, des écoutes, des prises de connaissance ou des enregistrements de "toute forme de communication émise à l'étranger", à des fins militaires ainsi que "pour des motifs de sécurité et de protection de nos troupes et de celles de nos alliées lors de mission à l'étranger et de nos compatriotes établis à l'étranger".

Ainsi qu'en a convenu le fonctionnaire délégué, la disposition en projet ne traduit pas correctement les intentions de l'auteur du projet. Telle qu'elle est rédigée, on ignore en effet si les 1° et 2° du paragraphe 5 en projet constituent des conditions cumulatives ou distinctes à la mise en oeuvre de ces opérations par le Service général du renseignement et de la sécurité des forces armées.

Comme l'a expliqué le fonctionnaire délégué, ces conditions sont distinctes. Quant à la seconde condition, elle concerne, selon lui, également toute forme de communication émise à l'étranger.

Sous la réserve de l'observation générale suivante, la rédaction du texte en projet doit dès lors être fondamentalement revue afin d'éviter toute ambiguïté sur sa portée exacte.

.../...

II. De la compatibilité de la disposition en projet avec le droit international

La disposition en projet concerne "toute forme de communication émise à l'étranger". Comme l'a souligné le fonctionnaire délégué, l'habilitation ainsi donnée au Service général du renseignement et de la sécurité des forces armées est strictement limitée aux communications partant de l'étranger. Il ne peut s'agir d'écouter, par exemple, des conversations téléphoniques lorsque l'appel est réalisé depuis le territoire de la Belgique. Par contre, les écoutes peuvent avoir lieu lorsqu'un appel est fait depuis l'étranger et qu'il est destiné soit à un correspondant établi dans un autre Etat étranger, soit à un correspondant établi sur le territoire belge.

En d'autres termes, le Service général du renseignement et de la sécurité des forces armées peut ainsi surveiller toutes les communications téléphoniques et les autres types de communications, comme les courriers électroniques échangés sur le réseau internet, qui ont lieu un peu partout dans le monde, que ce soit à des fins militaires ou pour des motifs de sécurité et de protection des troupes belges et alliées ainsi que des "compatriotes" établis à l'étranger.

La question qui se pose est de savoir si au regard du droit international, de telles mesures de surveillance peuvent se déployer au-delà du territoire de la Belgique.

1. Il ressort des explications fournies par le fonctionnaire délégué que les écoutes, les interceptions et les enregistrements des différentes formes de communications se feront au départ du territoire belge mais pas exclusivement. Ainsi, il est probable qu'un tel dispositif accompagne les troupes militaires belges dans la plupart de leurs déplacements en territoire étranger, que ce soit dans le cadre d'un conflit armé ou lors de missions humanitaires. Dans cette dernière hypothèse, il appartiendra à la Belgique de démontrer que ce dispositif est légitime eu égard aux missions qui ont été confiées à ses troupes militaires en vertu du mandat international sur la base duquel elles pénètrent sur le territoire d'un Etat étranger.

Si les opérations d'écoute ou d'interception de communications se font au départ de la Belgique en dehors du contexte d'un conflit armé, il convient de faire une distinction entre les données qui peuvent être directement localisées en Belgique bien qu'elles aient été émises à l'étranger et les données qui sont effectivement à l'étranger et qui jouissent d'un système de protection et auxquelles on ne peut avoir accès que grâce au recours à un dispositif technique.

Ainsi, en matière informatique, certains auteurs comme S. Evrard, estiment qu'il convient de faire une distinction

"... entre les données qui sont consultables publiquement à partir d'un ordinateur situé en Belgique, peu importe leur localisation, et les données non consultables publiquement qui se trouvent sur des ordinateurs situés à l'étranger."

Dans le premier cas, écrit cet auteur,

"... il nous semble évident que les autorités peuvent prendre copie desdites données. L'on pourra, par exemple prendre copie de photos à caractère pédophile, de pamphlets racistes, ou d'offres en vente de fichiers musicaux illicites dès lors que ceux-ci sont consultables via un ordinateur en Belgique, même si ces données sont stockées sur des ordinateurs situés à l'étranger.

En revanche, il nous semble que l'on ne pourra pas prendre de copie de fichiers non consultables publiquement situés à l'étranger. Dans ce cas en effet, seule l'autorité dudit pays aura compétence, le cas échéant sur commission rogatoire, pour effectuer ladite copie ⁽¹⁾."

Par exemple, le Service général du renseignement et de la sécurité des forces armées ayant eu accès à des données protégées par le système informatique d'un département ministériel d'un Etat étranger, pourrait être déclaré coupable d'une intrusion illicite dans ce système informatique ou être accusé de porter atteinte à la sûreté de cet Etat. Ainsi, la Belgique elle-même s'est dotée d'un dispositif juridique lui permettant de poursuivre de telles infractions visées notamment aux articles 122bis et 550bis du Code pénal.

⁽¹⁾ S. Evrard, "La loi du 28 novembre 2000 relative à la criminalité informatique", J.T., 2001, p. 244.

L'autorisation ainsi donnée par la loi en projet au Service général du renseignement et de la sécurité des forces armées risque d'entrer en conflit avec l'ordonnancement juridique d'autres Etats garantissant la protection de certaines données touchant aux intérêts essentiels de ceux-ci ⁽²⁾.

2. Dans un avis 28.029/2 donné le 31 mai 1999, sur un avant-projet de loi "relatif à la criminalité informatique", la section de législation du Conseil d'Etat a été amenée à s'interroger sur les effets extraterritoriaux de certains actes de contrainte.

Elle s'est exprimée comme suit :

"Parmi les règles fondamentales du droit international figure celle selon laquelle l'Etat exerce l'autorité étatique sur son propre territoire, et le fait seul, à l'exclusion de tout autre Etat. Il en découle qu'en temps de paix, il est absolument interdit à un Etat de procéder à une fonction de contrainte sur le territoire d'un autre Etat. Ceci concerne notamment tous les actes de la fonction exécutive, liés ou non à la justice. Un Etat ne peut ainsi, en dehors de son territoire, ni procéder à une arrestation, ni dresser un procès-verbal constatant un délit, ni mener une enquête, etc. La jurisprudence internationale est, sur ce point, constante ⁽³⁾.

Il n'est, toutefois, pas simple de déterminer la portée exacte que revêt cette règle quant aux actions judiciaires ou policières touchant à des données informatiques, notamment les mandats de perquisition et de saisie qui concernent de telles données. La difficulté ne résulte pas seulement de l'incertitude persistante qui peut parfois planer sur la question de savoir où sont exactement localisées des données informatiques; elle tient encore au fait que, grâce précisément à l'informatique, une autorité est capable, sans pour autant quitter physiquement le territoire de l'Etat dont elle relève, d'investiguer sur des données situées à l'étranger.

⁽²⁾ C'est ainsi que le Parlement européen a relevé au sujet d'une résolution relative à l'interception légale des télécommunications que pareille résolution "n'est pas contraignante et n'habilite en aucun cas les services de la sûreté à procéder à des interceptions en dehors de la zone relevant de la juridiction nationale" (extrait du rapport du 23 avril 1999 de M. G. Schmid sur le projet de résolution du Conseil relative à l'interception légale de télécommunications compte tenu des nouvelles technologies, P.E. 229.986/déf., p. 7, référence citée par D. Yernault, "«Echelon» et l'Europe - La protection de la vie privée face à l'espionnage des communications", J.T.D.E., 2000, p. 190).

⁽³⁾ Paul Reuter, Droit international public, p. 165.

Il semble bien que la plupart des Etats s'accordent encore aujourd'hui pour estimer que le seul fait de la présence de l'autorité judiciaire ou policière sur le territoire de son propre Etat ne suffit pas à lui permettre d'étendre son action sur n'importe laquelle des données qui, cependant, peuvent apparaître sur l'écran d'un ordinateur se trouvant, lui aussi, sur ce même territoire. Encore faut-il, pour rendre l'investigation licite, que les données (que l'autorité peut ainsi "voir", et dont elle peut éventuellement "s'emparer") ne se trouvent pas localisées sur le territoire d'un Etat étranger. Cette opinion générale des Etats a été récemment exposée dans la Recommandation n° R(95) 13 précitée, du Comité des ministres du Conseil de l'Europe aux Etats membres.

On peut y lire qu'à l'égard des "données stockées dans un autre pays ... la plupart des Etats membres tendent à considérer qu'une perquisition transfrontalière sur réseau menée par les autorités chargées de l'enquête sans l'autorisation des autorités compétentes du pays concerné pourrait constituer une violation de la souveraineté et du droit international, ainsi qu'un contournement partiel de la voie traditionnelle d'entraide judiciaire". La même Recommandation ajoute encore que "cela pourrait être considéré aussi comme une violation de la législation du pays (où les données se trouvent) et même y constituer une infraction pénale" (n° 189, p. 76).

La compatibilité du projet avec la règle de droit international ainsi identifiée est dès lors, pour le moins, problématique."

Si les missions du Service général du renseignement et de la sécurité des forces armées sont d'abord des missions ayant trait à la protection du territoire, des intérêts militaires de la Belgique et des ressortissants belges établis à l'étranger ⁽⁴⁾, il ressort également de la loi du 30 novembre 1998 organique des services de renseignements et de sécurité que les renseignements ainsi récoltés pourront être communiqués aux autorités judiciaires, la loi précitée invitant à une "coopération mutuelle aussi efficace que possible" ⁽⁵⁾.

Dans ce contexte, la loi autorise les services de renseignement et de sécurité, dans les limites d'un protocole approuvé par les ministres concernés, à prêter "leur concours et notamment leur assistance technique aux autorités judiciaires et administratives".

⁽⁴⁾ Voir notamment l'article 11 de la loi du 30 novembre 1998 organique des services de renseignements et de sécurité.

⁽⁵⁾ Voir les articles 19 et 20 de la loi du 30 novembre 1998, précitée.

Il se peut dès lors que des éléments de preuve d'infraction ou de tentative d'infraction soient directement fournis aux autorités judiciaires grâce au dispositif utilisé par le Service général du renseignement et de la sécurité des forces armées alors que ces autorités judiciaires auraient dû recourir à des commissions rogatoires pour obtenir ces mêmes éléments.

L'autorisation ainsi donnée par la loi en projet au Service général du renseignement et de la sécurité des forces armées de capter, d'écouter, de prendre connaissance et d'enregistrer toute forme de communication émise à l'étranger, ne peut avoir pour effet de contourner les obligations internationales de la Belgique sur le plan de l'entraide judiciaire, au risque de méconnaître la souveraineté d'autres Etats et d'affecter la régularité des éléments de preuves recueillis.

La loi en projet devrait en conséquence être plus précise sur les obligations du Service général du renseignement et de la sécurité des forces armées dès lors qu'il collabore avec les autorités judiciaires et leur apporte des renseignements sur la commission d'infractions ou la tentative d'une telle commission.

III. De la compatibilité de la disposition en projet avec la Convention de sauvegarde des droits de l'homme et des libertés fondamentales

Les écoutes ainsi que les enregistrements auxquels pourront se livrer les services de renseignement des forces armées constituent une ingérence dans la vie privée et familiale des citoyens puisqu'il s'agira de "toute forme de communication émise à l'étranger" en ce compris des conversations téléphoniques de particuliers.

1. Ainsi que l'a souligné le fonctionnaire délégué, le but du projet de loi est essentiellement de surveiller des personnes étrangères établies en dehors du territoire belge, les citoyens vivant sur le territoire belge n'étant, en principe, pas concernés. Selon lui, les garanties relatives à la protection de la vie privée exigées en vertu de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ne s'imposent à la Belgique que pour ce qui concerne les personnes établies sur notre territoire.

.../...

Selon l'article 1^{er} de la Convention, "Les hautes parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au Titre I de la Convention".

La Cour européenne des droits de l'homme dans son arrêt *Loizidou contre la Turquie* du 23 mars 1995 a notamment rappelé que,

"si l'article 1^{er} fixe des limites au domaine de la Convention, la notion de «juridiction» au sens de cette disposition ne se circonscrit pas au territoire national des hautes parties contractantes. [...]"

et que

"la responsabilité des parties contractantes peut entrer en jeu à raison d'actes émanant de leurs organes et se produisant sur ou en dehors de leur territoire (arrêt *Drozdz et Janousek c. France et Espagne* du 26 juin 1992, série A n° 240, p. 29, par. 91)."

On peut fermement conclure aujourd'hui sur ce point

"que la notion de juridiction énoncée à l'article 1^{er} de la Convention ne se limite pas à l'applicabilité territoriale, mais comporte l'idée d'une juridiction exercée sur l'individu par l'entremise des organes ou instances étatiques" ⁽⁶⁾.

Par ailleurs, comme en a convenu le fonctionnaire délégué, les mesures de surveillance, envisagées par la loi en projet, par les services de renseignements des forces armées pourront également concerner des citoyens établis sur le territoire belge dès lors que des appels en provenance de l'étranger leur sont destinés ou encore à des citoyens belges établis à l'étranger ou circulant à l'étranger.

En conclusion, le fait que les mesures de surveillance opérées par les services de renseignements des forces armées concerneraient principalement des communications émises à l'étranger n'a pas pour conséquence d'écarter la mise en oeuvre de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et plus particulièrement l'article 8 de cette Convention.

⁽⁶⁾ J. A. CARILLO-SALCEDO, Article 1, in L.E. PETTITI - E. DECAUX - P.-H. IMBERT, *La Convention européenne des droits de l'homme, commentaire article par article*, Economica, Paris, 1995, p. 137.

2. Une pareille ingérence doit nécessairement être conforme à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales qui impose une triple condition : cette ingérence étatique doit poursuivre l'un des buts légitimes énumérés au paragraphe 2 de cette disposition (à savoir notamment la sécurité nationale, la sûreté publique ainsi que la prévention d'infractions pénales), elle doit être prévue par la loi et enfin être nécessaire dans une société démocratique.

a) La condition de la légalité suppose que l'ingérence ait une base légale en droit interne mais aussi que la loi en cause soit accessible aux intéressés et que ceux-ci puissent en prévoir les conséquences ⁽⁷⁾.

La Cour européenne des droits de l'homme a jugé que,

"dans le contexte particulier de contrôles secrets du personnel affecté à des secteurs touchant à la sécurité nationale, l'exigence de prévisibilité ne saurait cependant être la même qu'en maints autres domaines." ⁽⁸⁾.

Elle a ajouté en l'espèce que cette exigence

"ne saurait signifier qu'un individu doit se trouver en mesure d'escompter avec précision les vérifications auxquelles la police spéciale suédoise procédera à son sujet en s'efforçant de protéger la sécurité nationale." ⁽⁹⁾

Elle a néanmoins souligné que

"dans un système applicable à tous les citoyens, tel celui de l'ordonnance sur le contrôle du personnel, la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée [...] En outre, lorsque sa mise en oeuvre s'opère au moyen de mesures secrètes, échappant au contrôle des personnes concernées comme du public, la loi elle-même, par opposition à la pratique administrative dont elle s'accompagne, doit définir l'étendue du pouvoir d'appréciation attribué à l'autorité compétente avec assez de netteté - compte tenu du but légitime poursuivi - pour fournir à l'individu une protection adéquate contre l'arbitraire." ⁽¹⁰⁾.

⁽⁷⁾ Not. arrêts Malone du 2 août 1984, par. 67 et 68, et mars 1987, par. 50.

⁽⁸⁾ Arrêt Leander du 26 mars 1987, par. 51.

⁽⁹⁾ Ibid.

⁽¹⁰⁾ Ibid.

C'est en un sens comparable que la Cour européenne des droits de l'homme s'est exprimée dans son arrêt du 16 février 2000 en cause Amann contre la Suisse lorsqu'elle souligna que les règles de procédure pénale suisse n'étaient pas suffisamment prévisibles dès lors qu'elles visent

"... avant tout la surveillance de personnes suspectées ou inculpées d'un crime ou d'un délit, voire les tiers présumés recevoir ou transmettre des informations à ces dernières, mais ne réglemente pas de façon détaillée le cas des interlocuteurs écoutés «par hasard», en qualité de «participants nécessaires» à une conversation téléphonique enregistrée par les autorités en application de ces dispositions. En particulier, la loi ne précise pas les précautions à prendre à leur égard.

La Cour conclut que l'ingérence ne saurait passer pour «prévues par la loi» puisque le droit suisse n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré." ⁽¹¹⁾.

Ni la disposition en projet, ni la loi du 30 novembre 1998, précitée, ne contiennent les précisions permettant de rencontrer les exigences de la jurisprudence européenne. La loi en projet se borne à donner une autorisation générale de captation, d'écoute, de prise de connaissance ou d'enregistrement. Une pareille formulation ne satisfait ni à l'exigence d'accessibilité, ni à l'exigence de prévisibilité prévue par l'article 8 de la Convention européenne des droits de l'homme. Pour répondre à ces exigences, le texte en projet devrait nécessairement viser les missions du Service général du renseignement et de la sécurité des forces armées ainsi que les conditions dans lesquelles celui-ci est amené à les exercer légalement conformément à la loi du 30 novembre 1998, précitée.

b) En ce qui concerne la nécessité d'un contrôle effectif des activités des services de renseignements, il y a lieu d'être également attentif à la jurisprudence de la Cour européenne des droits de l'homme, dont il résulte que,

"... pour que les systèmes de surveillance secrète soient compatibles avec l'article 8 de la Convention, ils doivent contenir des garanties établies par la loi et qui sont applicables au contrôle des activités des services concernés. Les procédures de contrôle doivent respecter aussi fidèlement que possible les valeurs d'une société démocratique, en particulier la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention. Elle implique, entre autres, qu'une ingérence de l'exécutif dans les droits de l'individu soit soumise à un contrôle

⁽¹¹⁾ Arrêt Amann du 16 février 2000, par. 61 et 62.

efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire, car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière." ⁽¹²⁾

La Cour n'exige pas que le contrôle soit nécessairement exercé par le pouvoir judiciaire. En effet, dans ses arrêts *Klass et Leander*, elle admet que celui-ci puisse l'être par une autorité présentant toutes les garanties d'impartialité et d'indépendance .

En l'espèce la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements a institué le Comité permanent de contrôle des services de renseignements (ci-après dénommé "le Comité permanent R") dont la mission est, en vertu de l'article 33 de cette loi, d'enquêter sur les activités et les méthodes des services de renseignements, sur leurs règlements et directives internes ainsi que sur tous les documents réglant le comportement des membres des services de renseignements afin de vérifier, conformément à l'article 1^{er} de cette loi, que les services de renseignements ne méconnaissent pas les droits que la Constitution confère aux citoyens.

Le Comité permanent R est assisté, dans cette mission, par le Service d'enquêtes des services de renseignements qui examinera notamment toutes les plaintes et les dénonciations des particuliers qui ont été directement concernés par l'intervention d'un service de renseignements ⁽¹³⁾.

Eu égard à ces dispositions, il n'apparaît cependant pas que le Comité permanent R et le service d'enquêtes précité disposent d'un pouvoir de décision, de sorte que les écoutes des services de renseignements ne sont pas soumises au contrôle effectif requis tant par la jurisprudence européenne que par les dispositions combinées des articles 8, § 2, et 13 de la Convention européenne des droits de l'homme.

En conclusion, la loi en projet doit être fondamentalement repensée car elle n'apporte aucune réponse précise quant aux garanties mises en évidence par la jurisprudence de la Cour européenne des droits de l'homme, qui doivent nécessairement entourer pareille ingérence étatique dans la vie privée des citoyens.

⁽¹²⁾ Arrêt *Rotaru* du 4 mai 2000, § 59.

⁽¹³⁾ Article 40 de la loi du 18 juillet 1991, précitée.

ALGEMENE OPMERKINGEN

I. Precieze strekking van de ontworpen bepaling

Volgens artikel 259bis, § 5, van het Strafwetboek is de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht ertoe gemachtigd om militaire radiocommunicatie die in het buitenland is uitgezonden te onderscheppen, af te luisteren, er kennis van te nemen of haar op te nemen, om redenen van militaire aard.

Het voorontwerp van wet wijzigd artikel 259bis, § 5, van het Strafwetboek met de bedoeling de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht een ruimere bevoegdheid te geven voor het onderscheppen, afluisteren, kennisnemen of opnemen van "elke vorm van communicatie uitgezonden in het buitenland", om redenen van militaire aard, alsook "om redenen van veiligheid en bescherming van onze troepen en van (die) van onze geallieerden tijdens operaties in het buitenland en van onze onderdanen die in het buitenland gevestigd zijn".

De gemachtigde ambtenaar is het ermee eens dat de bedoelingen van de steller van het ontwerp niet correct worden weergegeven in de ontworpen bepaling. Zoals die bepaling gesteld is, is het immers niet bekend of de onderdelen 1° en 2° van de ontworpen paragraaf 5 cumulatieve dan wel afzonderlijke voorwaarden vormen voor de uitvoering van die operaties door de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht.

Zoals de gemachtigde ambtenaar heeft uitgelegd, gaat het om afzonderlijke voorwaarden. De tweede voorwaarde heeft volgens hem ook betrekking op elke vorm van communicatie uitgezonden in het buitenland.

Onder voorbehoud van de volgende algemene opmerking, moet de redactie van de ontworpen regelgeving dus grondig worden herzien opdat onduidelijkheid omtrent de precieze strekking ervan wordt voorkomen.

II. Verenigbaarheid van de ontworpen bepaling met het internationale recht

De ontworpen bepaling heeft betrekking op "elke vorm van communicatie uitgezonden in het buitenland". Zoals de gemachtigde ambtenaar heeft onderstreept, is de machtiging die aldus aan de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht wordt gegeven, strikt beperkt tot communicatie uit het buitenland. Er kan bijvoorbeeld geen sprake van zijn telefoongesprekken af te luisteren wanneer vanuit België wordt gebeld. Ze mogen daarentegen wel worden afgeluisterd wanneer vanuit het buitenland wordt gebeld naar iemand die in een ander buitenlands land of in België is gevestigd.

Met andere woorden : de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht kan aldus toezicht houden op alle telefoongesprekken en andere vormen van communicatie, zoals via het internet uitgewisselde elektronische berichten, die zowat overal ter wereld tot stand komen, ongeacht of het nu voor militaire doeleinden is dan wel voor de veiligheid en bescherming van de Belgische troepen en die van de bondgenoten, alsook van Belgische onderdanen die in het buitenland gevestigd zijn.

De vraag rijst of zulke toezichtsmaatregelen zich volgens het internationale recht buiten het grondgebied van België mogen uitstrekken.

1. Uit de uitleg van de gemachtigde ambtenaar blijkt dat het afluisteren, onderscheppen en opnemen van de verschillende vormen van communicatie vanuit België zal geschieden, maar niet uitsluitend. Zo is het waarschijnlijk dat zulke apparatuur de Belgische militaire troepen vergezelt op de meeste van hun tochten op buitenlands grondgebied, zowel in het kader van gewapende conflicten als tijdens humanitaire opdrachten. In laatstgenoemd geval staat het aan België aan te tonen dat die apparatuur legitiem is, gelet op de opdrachten die aan haar militaire troepen zijn toevertrouwd krachtens het internationale mandaat op basis waarvan ze zich op het grondgebied van een buitenlandse staat begeven.

Wordt vanuit België communicatie afgeluisterd of onderschept los van een gewapend conflict, dan moet een onderscheid worden gemaakt tussen gegevens die rechtstreeks in België kunnen worden gelokaliseerd, hoewel ze in het buitenland zijn uitgezonden, en gegevens die zich daadwerkelijk in het buitenland bevinden, onder een beveiligingssysteem vallen en slechts toegankelijk zijn door middel van technische apparatuur.

Zo oordelen sommige auteurs, zoals S. Evrard, dat op het stuk van de computer het volgende onderscheid moet worden gemaakt :

"... entre les données qui sont consultables publiquement à partir d'un ordinateur situé en Belgique, peu importe leur localisation, et les données non consultables publiquement qui se trouvent sur des ordinateurs situés à l'étranger."

In het eerste geval geldt volgens die auteur :

"... il nous semble évident que les autorités peuvent prendre copie desdites données. L'on pourra, par exemple prendre copie de photos à caractère pédophile, de pamphlets racistes, ou d'offres en vente de fichiers musicaux illicites dès lors que ceux-ci sont consultables via un ordinateur en Belgique, même si ces données sont stockées sur des ordinateurs situés à l'étranger.

En revanche, il nous semble que l'on ne pourra pas prendre de copie de fichiers non consultables publiquement situés à l'étranger. Dans ce cas en effet, seule l'autorité dudit pays aura compétence, le cas échéant sur commission rogatoire, pour effectuer ladite copie ⁽¹⁾."

Als bijvoorbeeld de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht toegang heeft gehad tot gegevens die beschermd worden door het computersysteem van een ministerie van een buitenlandse staat, zou hij schuldig kunnen worden verklaard aan onwettige inbraak in dat computersysteem of beschuldigd kunnen worden van aantasting van de veiligheid van die staat. Zo heeft België zelf ook regelgeving om zulke strafbare feiten als genoemd in onder meer de artikelen 122bis en 550bis van het Strafwetboek te kunnen vervolgen.

⁽¹⁾ S. Evrard, "La loi du 28 novembre 2000 relative à la criminalité informatique", J.T., 2001, blz. 244.

De machtiging die aldus bij de ontworpen wet aan de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht wordt gegeven, kan dus in conflict komen met de rechtsordening van andere staten ter bescherming van bepaalde gegevens die te maken hebben met wezenlijke belangen van die staten ⁽²⁾.

2. In advies 28.029/2 van 31 mei 1999 over een voorontwerp van wet "inzake informaticacriminaliteit" heeft de afdeling wetgeving van de Raad van State kanttekeningen geplaatst bij de exterritoriale gevolgen van sommige dwangmaatregelen.

Ze heeft het volgende opgemerkt :

"Een van de fundamentele regels van het internationaal recht bepaalt dat een staat staatsgezag uitoefent op zijn eigen grondgebied, en dat alleen doet, zonder inmenging van enige andere staat. Hieruit volgt dat een staat in vredetijd absoluut geen dwangmiddelen mag gebruiken op het grondgebied van een andere staat. Dit geldt inzonderheid voor alle handelingen van de uitvoerende macht, die al dan niet betrekking hebben op justitie. Een staat mag dus buiten zijn grondgebied geen arrestatie verrichten, noch een proces-verbaal opmaken waarbij een strafbaar feit vastgesteld wordt, noch een onderzoek doen, enz. Dit is vaste internationale rechtspraak ⁽³⁾.

Het is evenwel niet eenvoudig de precieze strekking van die regel te bepalen ten aanzien van het optreden van justitie of politie in verband met computergegevens, inzonderheid wat betreft bevelen tot opsporing en inbeslagname van zulke gegevens. Dat probleem is niet alleen het gevolg van de blijvende onzekerheid die soms bestaat over de vraag waar computergegevens precies te vinden zijn; het houdt ook verband met het feit dat een autoriteit, precies dank zij de informatica, gegevens in het buitenland kan navorsen zonder daarom het grondgebied van de staat waaronder ze ressorteert, in stoffelijke zin te verlaten.

De meeste staten zijn het er thans blijkbaar nog altijd over eens dat alleen het louter aanwezig zijn van gerechtelijke of politieautoriteiten op hun eigen grondgebied hun niet toestaat hun optreden uit te breiden tot alle gegevens; deze gegevens kunnen nochtans verschijnen op het scherm van een computer, die zich eveneens op datzelfde grondgebied bevindt. Om het onderzoek wettig te laten

⁽²⁾ Zo heeft het Europees Parlement in verband met een resolutie inzake de legale interceptie van telecommunicatieverkeer opgemerkt dat zulk een resolutie "(...) geen bindend karakter (heeft) en de veiligheidsautoriteiten van de EU-staten (...) bij interceptiemaatregelen buiten het eigen grondgebied hieraan geen rechten (kunnen) onttelen" (uittreksel uit het verslag van 23 april 1999 van de heer G. Schmid over de ontwerp-resolutie van de Raad over de legale interceptie van telecommunicatieverkeer in verband met nieuwe technologieën, PE 229.986/def, blz. 6. Zie ook D. Yernault, "«Echelon» et l'Europe - La protection de la vie privée face à l'espionnage des communications", J.T.D.E., 2000, blz. 190).

⁽³⁾ Paul Reuter, Droit international public, blz. 165.

verlopen, is het bovendien noodzakelijk dat de gegevens (die de overheid aldus kan "zien", en eventueel kan bemachtigen) zich dus niet op het grondgebied van een vreemde staat bevinden. Die algemene opvatting van de staten is onlangs uiteengezet in de voornoemde Aanbeveling nr. R(95) 13 van het Ministercomité van de Raad van Europa aan de Lid-Staten.

Daarin staat te lezen dat wat betreft de "gegevens die in een ander land opgeslagen zijn ..., de meeste Lid-Staten ervan lijken uit te gaan dat een opsporing op het netwerk over de grenzen heen door de overheden die belast zijn met het onderzoek, zonder toestemming van de bevoegde autoriteiten van het betrokken land, een schending van de soevereiniteit en van het internationaal recht zou kunnen vormen, alsmede een gedeeltelijk omzeilen van het traditionele middel van de wederzijdse rechtshulp". In dezelfde Aanbeveling wordt ook verklaard dat dat ook beschouwd zou kunnen worden als een overtreding van de wetgeving van het land (waar de gegevens zich bevinden) en er zelfs een strafbaar feit zou kunnen zijn" (nr. 189, blz. 76).

Het is dus op zijn minst twijfelachtig of het ontwerp niet strijdig zal zijn met de aldus bepaalde regel van internationaal recht."

Hoewel de opdrachten van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht in de eerste plaats opdrachten zijn die betrekking hebben op de bescherming van het grondgebied, de militaire belangen van België en de Belgische onderdanen in het buitenland ⁽⁴⁾, blijkt ook uit de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst dat de aldus ingewonnen inlichtingen kunnen worden meegedeeld aan de gerechtelijke overheden, aangezien de voornoemde wet "een zo doeltreffend mogelijke wederzijdse samenwerking" voorschrijft ⁽⁵⁾.

In dat verband biedt de wet de inlichtingen- en veiligheidsdiensten de mogelijkheid om binnen de perken van een protocol, goedgekeurd door de betrokken ministers, "hun medewerking en in het bijzonder hun technische bijstand (te) verlenen aan de gerechtelijke en bestuurlijke overheden".

Het is dus mogelijk dat bewijsmateriaal voor een strafbaar feit of een poging tot het plegen van een strafbaar feit rechtstreeks wordt doorgezonden aan de gerechtelijke instanties, dankzij de apparatuur die door de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht wordt aangewend, terwijl die gerechtelijke instanties met een ambtelijke opdracht hadden moeten werken om dat materiaal te verkrijgen.

⁽⁴⁾ Zie inzonderheid artikel 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.

⁽⁵⁾ Zie de artikelen 19 en 20 van de genoemde wet van 30 november 1998.

De machtiging die aldus door de ontworpen wet aan de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht wordt verleend om elke vorm van communicatie uitgezonden in het buitenland te onderscheppen, af te luisteren, er kennis van te nemen en op te nemen, mag niet tot gevolg hebben dat de internationale verplichtingen van België op het stuk van de wederzijdse rechtshulp worden omzeild, want dan kan de soevereiniteit van andere staten worden geschonden en de regelmatigheid van het ingewonnen bewijsmateriaal worden aangetast.

In de ontworpen wet zou dus duidelijker moeten worden vermeld welke verplichtingen de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht moet nakomen, aangezien die dienst samenwerkt met de gerechtelijke autoriteiten en ze inlichtingen over gepleegde strafbare feiten of pogingen tot het plegen van zulke feiten verstrekt.

III. Verenigbaarheid van de ontworpen bepaling met het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden

De afluisterpraktijken en opnamen die de inlichtingendiensten van de krijgsmacht zich zullen kunnen veroorloven, vormen een inmenging in het privé- en gezinsleven van de burgers, aangezien het zal gaan om "elke vorm van communicatie uitgezonden in het buitenland", dus ook om telefoongesprekken van privé-personen.

1. Zoals de gemachtigde ambtenaar heeft benadrukt, heeft het wetsontwerp hoofdzakelijk tot doel toezicht te houden op buitenlanders die niet op het Belgische grondgebied gevestigd zijn, terwijl burgers die op het Belgische grondgebied wonen in principe niet betrokken zijn. Volgens hem hoeft België de waarborgen voor de bescherming van de persoonlijke levenssfeer opgelegd krachtens artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden alleen in acht te nemen voor personen die op ons grondgebied zijn gevestigd.

Luidens artikel 1 van het Verdrag "(verzekeren) de Hoge Verdragsluitende Partijen (...) eenieder, die ressorteert onder haar rechtsmacht, de rechten en vrijheden welke zijn vastgesteld in de Eerste Titel van dit Verdrag".

Het Europese Hof voor de rechten van de mens heeft in zijn arrest - Loizidou van 23 maart 1995 tegen Turkije onder meer het volgende opgemerkt :

"si l'article 1^{er} fixe des limites au domaine de la Convention, la notion de «juridiction» au sens de cette disposition ne se circonscrit pas au territoire national des hautes parties contractantes. [...]".

en

"la responsabilité des parties contractantes peut entrer en jeu à raison d'actes émanant de leurs organes et se produisant sur ou en dehors de leur territoire (arrest - Drozd en Janousek van 26 juni 1992 tegen Frankrijk en Spanje, serie A nr. 240, blz. 29, rechtsoverweging 91).

Op dat punt kan thans de vaste conclusie zijn :

"... la notion de juridiction énoncée à l'article 1^{er} de la Convention ne se limite pas à l'applicabilité territoriale, mais comporte l'idée d'une juridiction exercée sur l'individu par l'entremise des organes ou instances étatiques" ⁽⁶⁾.

Bovendien heeft de gemachtigde ambtenaar bevestigd dat de in de ontworpen wet geplande toezichtsmaatregelen die door de inlichtingendiensten van de krijgsmacht zullen worden genomen, ook betrekking kunnen hebben op burgers die op het Belgische grondgebied gevestigd zijn, wanneer oproepen uit het buitenland voor hen bestemd zijn of voor Belgische burgers die in het buitenland wonen of daar rondreizen.

Het besluit is dan ook dat de omstandigheid dat de toezichtsmaatregelen die door de inlichtingendiensten van de krijgsmacht zullen worden genomen, voornamelijk betrekking zouden hebben op communicatie uitgezonden in het buitenland, niet tot gevolg heeft dat het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, in het bijzonder artikel 8 van dat Verdrag niet behoeft te worden toegepast.

⁽⁶⁾ J.A. CARILLO-SALCEDO, Artikel 1, in L.E. PETTITI - E. DECAUX - P.-H. IMBERT, La Convention européenne des droits de l'homme, artikelsgewijze bespreking, Economica, Parijs, 1995, blz. 137.

2. Zulk een inmenging moet absoluut in overeenstemming zijn met artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, waarin drie voorwaarden worden gesteld : een inmenging van enig openbaar gezag moet één van de wettige doeleinden beogen opgesomd in lid 2 van die bepaling (onder meer's lands veiligheid, de openbare veiligheid en het voorkomen van strafbare feiten), ze moet bij de wet bepaald zijn en tot slot moet ze in een democratische samenleving nodig zijn.

a) Het wettigheidsvereiste houdt in dat de inmenging een wettelijke basis in het interne recht moet hebben, maar ook dat de belanghebbenden de wet in kwestie moeten kunnen inzien en de gevolgen ervan moeten kunnen inschatten ⁽⁷⁾.

Het Europese Hof voor de rechten van de mens heeft geoordeeld :

"dans le contexte particulier de contrôles secrets du personnel affecté à des secteurs touchant à la sécurité nationale, l'exigence de prévisibilité ne saurait cependant être la même qu'en maints autres domaines." ⁽⁸⁾.

Voorts heeft het in het onderhavige geval gesteld :

"(cette exigence) ne saurait signifier qu'un individu doit se trouver en mesure d'escompter avec précision les vérifications auxquelles la police spéciale suédoise procédera à son sujet en s'efforçant de protéger la sécurité nationale." ⁽⁹⁾.

Het heeft echter op het volgende gewezen :

"dans un système applicable à tous les citoyens, tel celui de l'ordonnance sur le contrôle du personnel, la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée [...] En outre, lorsque sa mise en oeuvre s'opère au moyen de mesures secrètes, échappant au contrôle des personnes concernées comme du public, la loi elle-même, par opposition à la pratique administrative dont elle s'accompagne, doit définir l'étendue du pouvoir d'appréciation attribué à l'autorité compétente avec assez de netteté - compte tenu du but légitime poursuivi - pour fournir à l'individu une protection adéquate contre l'arbitraire." ⁽¹⁰⁾.

⁽⁷⁾ Noot arresten Malone van 2 augustus 1984, rechtsoverwegingen 67 en 68, en maart 1987, r.o. 50.

⁽⁸⁾ Arrest Leander van 26 maart 1987, r.o. 51.

⁽⁹⁾ Ibid.

⁽¹⁰⁾ Ibid.

Het Europese Hof voor de rechten van de mens heeft een vergelijkbaar standpunt ingenomen in zijn arrest van 16 februari 2000 in de zaak - Amann tegen Zwitserland. Daarin heeft het Hof onderstreept dat de Zwitserse regels van strafprocesrecht onvoldoende rechtszekerheid bieden, aangezien ze gericht zijn op :

"... avant tout la surveillance de personnes suspectées ou inculpées d'un crime ou d'un délit, voire les tiers présumés recevoir ou transmettre des informations à ces dernières, mais ne réglemente pas de façon détaillée le cas des interlocuteurs écoutés «par hasard», en qualité de «participants nécessaires» à une conversation téléphonique enregistrée par les autorités en application de ces dispositions. En particulier, la loi ne précise pas les précautions à prendre à leur égard.

La Cour conclut que l'ingérence ne saurait passer pour «prévue par la loi» puisque le droit suisse n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré." ⁽¹¹⁾.

Noch de ontworpen bepaling, noch de genoemde wet van 30 november 1998 bevatten de preciseringen die noodzakelijk zijn om aan de vereisten van de Europese jurisprudentie te kunnen voldoen. De ontworpen wet bepaalt zich ertoe een algemene machtiging tot het onderscheppen, af luisteren, kennisnemen of opnemen te verlenen. Zulke bewoordingen voldoen niet aan de vereiste van toegankelijkheid, noch aan de vereiste van rechtszekerheid gesteld in artikel 8 van het Europese Verdrag tot bescherming van de rechten van de mens. Wil men de ontworpen regeling in overeenstemming brengen met die vereisten, dan moet in de ontworpen regeling in ieder geval worden vermeld welke opdrachten de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht heeft en onder welke voorwaarden hij die opdrachten overeenkomstig de genoemde wet van 30 november 1998 wettig heeft te vervullen.

b) Wat de noodzaak betreft om daadwerkelijk controle uit te oefenen op de werkzaamheden van de inlichtingendiensten, dient ook acht te worden geslagen op de jurisprudentie van het Europese Hof voor de rechten van de mensen, waaruit blijkt :

"... pour que les systèmes de surveillance secrète soient compatibles avec l'article 8 de la Convention, ils doivent contenir des garanties établies par la loi et qui sont applicables au contrôle des activités des services concernés. Les procédures de contrôle doivent respecter aussi fidèlement que possible les valeurs d'une société démocratique, en particulier la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention. Elle implique, entre autres, qu'une

⁽¹¹⁾ Arrest Amann van 16 februari 2000, rechtsoverwegingen 61 en 62.

ingérence de l'exécutif dans les droits d'individu soit soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire, car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière." ⁽¹²⁾.

Het Hof eist niet dat de controle per se door de rechterlijke macht wordt uitgeoefend. In zijn arresten - Klass en Leander stelt het Hof immers dat die controle ook kan worden uitgeoefend door een autoriteit die alle waarborgen biedt inzake onpartijdigheid en onafhankelijkheid.

In casu is bij de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten het Vast Comité van Toezicht op de inlichtingendiensten ingesteld (hierna te noemen Vast Comité I). Krachtens artikel 33 van die wet heeft dat comité tot taak onderzoeken in te stellen naar de activiteiten en werkwijzen van de inlichtingendiensten, naar hun interne reglementen en richtlijnen alsmede naar alle documenten die de handelwijze van de leden van de inlichtingendiensten regelen, teneinde overeenkomstig artikel 1 van die wet na te gaan of de inlichtingendiensten niet de rechten schenden die de Grondwet aan de burgers verleent.

Het Vast Comité I wordt in die taak bijgestaan door de dienst Enquêtes voor de inlichtingendiensten, die onder meer alle klachten en aangiften onderzoekt van particulieren die rechtstreeks betrokken zijn geweest bij het optreden van een inlichtingendienst ⁽¹³⁾.

Uit die bepalingen blijkt evenwel niet dat het Vast Comité I en de genoemde dienst Enquêtes beslissingsbevoegdheid hebben, zodat er geen daadwerkelijke controle bestaat op af luisteroperaties door de inlichtingendiensten, gelijk zowel door de Europese jurisprudentie als door de in onderlinge samenhang gelezen bepalingen van artikel 8, lid 2, en artikel 13 van het Europese Verdrag voor de rechten van de mens wordt voorgeschreven.

⁽¹²⁾ Arrest Rotaru van 4 mei 2000, r.o. 59.

⁽¹³⁾ Artikel 40 van de genoemde wet van 18 juli 1991.

Het besluit is dan ook dat de ontworpen wet grondig moet worden herzien omdat ze geen duidelijk antwoord geeft in verband met de waarborgen die in de jurisprudentie van het Europese Hof voor de rechten van de mens worden benadrukt, in welke waarborgen bij zulk een staatsinmenging in het privé-leven van de burgers stellig moet worden voorzien.

La chambre était composée de

De kamer was samengesteld uit

Madame
Mevrouw

M.-L. WILLOT-THOMAS,

président de chambre,
kamervoorzitter,

Messieurs
de Heren

P. LIÉNARDY,
P. VANDERNOOT,

conseillers d'Etat,
staatsraden,

J. van COMPERNOLLE,
B. GLANSDORFF,

assesseurs de la section de législation,
assessoren van de afdeling wetgeving,

Madame
Mevrouw

A.-C. VAN GEERSDAELE,

greffier assumé,
toegevoegd griffier.

Le rapport a été présenté par Mme P. VANDERNACHT, auditeur. La note du Bureau de coordination a été rédigée et exposée par Mme G. MARTOU, référendaire adjoint.

Het verslag werd uitgebracht door Mevr. P. VANDERNACHT, auditeur. De nota van het Coördinatiebureau werd opgesteld en toegelicht door Mevr. G. MARTOU, adjunct-referendaris.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de M. P. LIÉNARDY.

De overeenstemming tussen de Franse en de Nederlandse tekst werd nagezien onder toezicht van de H. P. LIÉNARDY.

LE GREFFIER - DE GRIFFIER,

LE PRÉSIDENT - DE VOORZITTER,

A.-C. VAN GEERSDAELE

M.-L. WILLOT-THOMAS