PROJET du 05.07.2006

Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)

Modification du ….

Rapport explicatif

Table des matières

1. Partie générale

1.1 Situation juridique actuelle

1.1.1 Mandat politique

Les instruments permettant de garantir la sûreté intérieure sont la protection de l'Etat et la police. Ils font partie de la politique de sécurité dans la mesure où ils contribuent à lutter contre les menaces pesant sur de grandes parties du pays et de la population. La lutte contre la violence de portée non stratégique fait partie de la politique de sécurité des cantons. Si les troubles sont déjà intervenus, il revient principalement aux cantons de les dissiper.

Les organes de la protection de l'Etat et la police sont chargés des mandats suivants en matière de politique de sécurité:

- Les organes de la protection de l'Etat prennent des mesures préventives afin de détecter à temps les menaces émanant du terrorisme, de l'extrémisme violent, du service de renseignements prohibé, du commerce illicite d'armes et de substances radioactives et du transfert illégal de technologie. Ils apportent en outre leur soutien aux autorités policières et aux autorités de poursuite pénale en leur fournissant des renseignements relatifs au crime organisé.
- La police, essentiellement soumise à la souveraineté cantonale, veille à la sécurité et à l'ordre publics et lutte contre la criminalité. La Confédération intervient notamment pour maîtriser des événements que les cantons ne peuvent contenir avec leurs propres moyens. Si la situation l'exige, c'est elle qui dirige les engagements.

1.1.2 Services de renseignements intérieur et extérieur de la Confédération

Il n'existe plus de frontière stricte entre la sûreté intérieure et la sûreté extérieure. La sûreté est indivisible. Les risques et les menaces revêtent un caractère transfrontalier de plus en plus marqué et l'instabilité et les conflits, même dans des zones éloignées, peuvent avoir des répercussions directes et immédiates sur la sûreté intérieure de la Suisse.

La Suisse, comme presque tous les Etats démocratiques du monde, exploite un service de renseignements intérieur et un service de renseignements extérieur. Le Service de renseignement stratégique (SRS), rattaché au Département fédéral de la défense, de la protection de la population et des sports (DDPS), est le service de renseignements extérieur de la Suisse. Le Service d'analyse et de prévention (SAP), rattaché à l'Office fédéral de la police, est quant à lui le service de renseignements intérieur de la Suisse. Il est chargé de fournir à temps aux organes politiques dirigeants de la Confédération, mais aussi aux cantons, des informations sur les menaces pesant sur la sûreté intérieure, afin que des mesures préventives puissent être prises à temps. Les tâches du service de renseignements intérieur sont réglées dans la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS 120) et dans les ordonnances correspondantes.

S'agissant des menaces internationales, qui ne peuvent être traitées selon un critère de délimitation territoriale (Suisse – étranger), les services de renseignements

collaborent très étroitement, aujourd'hui au sein de plates-formes dans les domaines du terrorisme, du crime organisé et de la prolifération.

1.1.3 Activités du service de renseignements intérieur

a) Protection de l'existence

Le SAP collecte, analyse et diffuse en permanence des renseignements. Ainsi, il peut informer les organes de conduite de l'Etat des menaces pesant sur l'existence du pays, sur l'ordre de sa société et sur ses institutions démocratiques.

L'art. 1 de la LMSI évoque cette dimension de la protection de l'Etat, qui englobe la société et la nation dans leur ensemble, dans la mesure où il dit de la protection de l'Etat qu'elle contribue à assurer le respect des fondements démocratiques et constitutionnels de la Suisse, ainsi qu'à protéger les libertés de sa population.

b) Tâches du service de renseignements intérieur

Pour menacer sérieusement l'existence d'une société dans son ensemble, ainsi que la sécurité d'un grand nombre de personnes, il faut des personnes animées d'une même volonté destructrice. Vues sous un angle historique, les menaces relevant de la protection de l'Etat se fondent en général sur des motivations politiques et idéologiques. Par contre, la poursuite de la criminalité motivée principalement par des motifs pécuniaires relève historiquement des autorités de poursuite pénale.

Selon le droit en vigueur, le SAP agit contre les menaces émanant du terrorisme, de l'extrémisme violent, du service de renseignements prohibé, du commerce illicite d'armes et de substances radioactives et du transfert illégal de technologie. Il soutient en outre les autorités policières et les autorités de poursuite pénale compétentes en leur fournissant des renseignements sur le crime organisé, notamment des renseignements provenant des autorités de sûreté étrangères.

c) But préventif

Les recherches auxquelles procède le SAP ont pour but de fournir à temps aux autorités compétentes, notamment aux organes de conduite de la Confédération et aux cantons, des informations relatives à la situation en matière de sécurité, afin que les menaces puissent être reconnues à temps (p. ex. appréciation périodique de la situation de la menace par les autorités politiques) et que des mesures puissent être prises (p. ex. interdictions d'entrée prononcées à l'encontre d'étrangers pouvant nuire à la sûreté intérieure de la Suisse ou protection de personnes et d'infrastructures). L'action du SAP vise par conséquent principalement à mettre au jour les menaces pouvant peser sur la sécurité de la Suisse (but préventif de la vérification des soupçons) et le cas échéant à les écarter.

d) Mesures de recherche d'informations

Toute analyse de la menace et toute action en résultant se fondent sur une variété d'informations. Seule une partie des informations nécessaires peut être acquise par l'intermédiaire de sources accessibles au grand public. Car la recherche d'informations qui ne sont pas publiques est une tâche centrale d'un service de renseignements. Le produit résultant de l'activité des services de renseignements ne

peut pas contenir davantage d'informations ni d'informations de meilleure qualité que celles que la loi permet de collecter et d'évaluer.

Lorsque le service de renseignements met au jour des menaces relevant de la protection de l'Etat, les autorités compétentes de la Confédération et des cantons prennent, en vertu de l'art. 2, al. 2, LMSI, les mesures policières et les mesures de droit administratif qui s'imposent pour repousser les menaces ou dissiper les troubles en cours.

Le deuxième alinéa de l'art. 14 LMSI énumère les moyens de recherche d'informations autorisés dans le cadre préventif. Aux termes de cet alinéa, des données personnelles peuvent être recueillies par le biais:

a) de l'exploitation de sources accessibles au public;
b) de demandes de renseignements;
c) de la consultation de documents officiels;
d) de la réception et de l'exploitation de communications;
e) d'enquêtes sur l'identité ou le lieu de séjour de personnes;
f) de l'observation de faits, y compris au moyen d'enregistrements d'images et de sons, dans des lieux publics et librement accessibles;
g) du relevé des déplacements et des contacts de personnes.

A l'art. 14, al. 3, LMSI, le législateur retire au service de renseignements intérieur la possibilité d'avoir recours à des mesures de contrainte prévues par la procédure pénale et exclut l'observation de faits dans des locaux privés. Ainsi, tout traitement préventif est impossible dans le secteur de la communication (poste, téléphone, fax, courriel).

e) Service de renseignement stratégique

Le Service de renseignement stratégique (SRS) est le service de renseignements extérieur de la Suisse. En vertu de l'art. 99, al. 1, de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM)[1], il recherche des informations sur l'étranger importantes pour la sécurité du pays, destinées aux dirigeants politiques et militaires, et en particulier au chef du DDPS, au chef de l'Armée, à la Délégation du Conseil fédéral pour la sécurité et à l'Organe de direction pour la sécurité, les évalue et les diffuse. Conformément à l'art. 99, al. 5, LAAM, il est directement subordonné au chef du DDPS. Le SRS a un mandat de base signé par les trois conseillers fédéraux représentés au sein de la Délégation du Conseil fédéral pour la sécurité. Les activités de collecte et d'analyse d'informations du SRS sont principalement de nature politique, économique, militaire, scientifique et technique. Elles concernent essentiellement les menaces liées au terrorisme, au crime organisé et à la dissémination d'armes de destruction massive et de leurs porteurs (prolifération). Les tâches du SRS sont réglées dans l'ordonnance du 26 septembre 2003 sur l'organisation des services de renseignements au sein du Département fédéral de la défense, de la protection de la population et des sports (Orens)[2].

[1] RS **510.10**
[2] RS **510.291**

1.1.4 Délimitation entre la protection préventive de l'Etat (prévention) et le mandat de la police (prévention des menaces d'ordre général)

Les activités du SAP se limitent aux tâches décrites à l'al. 2 LMSI. Dans ce cadre, les renseignements et les analyses disponibles peuvent se fonder sur des informations relatives à des troubles de la sécurité à venir ou déjà survenus.

S'agissant des troubles à venir, les services de renseignements se concentrent sur la mise au jour des menaces qui peuvent peser sur la sécurité et l'ordre publics, ainsi que sur la mise en garde précoce contre ces menaces. Ils contribuent par exemple à empêcher les attentats terroristes en mettant au jour les réseaux qui les fomentent et en prévenant leurs activités. Les mises en garde des services de renseignements devant intervenir le plus tôt possible, ils doivent procéder à leurs recherches d'informations avant que les menaces ne deviennent concrètes et imminentes, voire avant même que les soupçons d'infraction n'existent.

Par contre, il revient aux corps de police cantonaux de reconnaître à temps et d'empêcher les violences locales (p. ex. violences de rue) est le travail des corps de police cantonaux. Dans le cadre de leur mandat de prévention des menaces d'ordre général, ils ne peuvent intervenir que lorsque les menaces deviennent concrètes et imminentes. Les troubles déjà intervenus sont maîtrisés par les corps de police cantonaux dans le cadre de leur mandat policier général.

1.1.5 Délimitation entre la protection préventive de l'Etat (prévention) et la répression relevant du droit pénal

Le but des actes des autorités (prévention ou répression) constitue le critère de délimitation.

Tant les activités préventives que répressives reposent sur des soupçons.

La protection préventive de l'Etat consiste à vérifier les soupçons relatifs à une menace pesant sur la sécurité de la Suisse ou de ses habitants, relevant du terrorisme, de l'extrémisme violent, du service de renseignements prohibé, du commerce illicite d'armes ou de substances radioactives ou du transfert illégal de technologie (but préventif).

La répression consiste quant à elle à vérifier des soupçons relatifs à une infraction au droit fédéral ou au droit cantonal (but répressif).

Le but de la protection préventive de l'Etat est de mettre au jour autant que possible les structures menaçant l'Etat et la société, ou de prévenir et de déjouer les menées antidémocratiques. Ainsi, les autorités compétentes recherchent et traitent les données et les informations relatives aux menaces pouvant peser sur la sécurité, et prennent ou proposent les mesures appropriées pour les contrer.

Les recherches d'informations préventives requièrent en général un mode d'action stratégique ayant un effet à long terme.

Il en va différemment de la répression relevant du droit pénal. Dans ce cas, l'Etat intervient pour confier aux organes judiciaires le soin de clarifier une présomption d'infraction, en vue de juger une faute individuelle. La répression (justice et police

judiciaire) comprend le règlement du conflit entre la communauté de droit et l'individu qui viole des normes fondamentales de la communauté. En d'autres termes, elle se charge de constater un comportement humain en lien avec une infraction concrète ou un acte préparatoire répréhensible. Elle est donc liée à un cas concret.

Le droit pénal vise à fournir une protection renforcée à certains biens protégés par le droit. Cette protection renforcée résulte, d'une part, de l'effet dissuasif de la peine prévue, de son attribution et de son exécution et, d'autre part, une fois l'infraction commise, de l'atteinte aux biens juridiques de l'auteur (p. ex. peine privative de liberté). L'objectif est alors de rendre l'auteur de l'infraction meilleur ou, en tous les cas, de le placer en lieu sûr.

Selon le principe de la légalité, une personne se rend punissable si elle commet un acte qui, aux termes de la loi, donne lieu à une peine. En principe, la simple préméditation n'est pas punissable. Sous l'influence de la vague terroriste des années 70 néanmoins, des actes préparatoires à certaines infractions capitales (art. 260bis CP: meurtre, assassinat, lésions corporelles graves, brigandage, séquestration et enlèvement, prise d'otage, incendie intentionnel, génocide) ont été déclarés répréhensibles pour eux-mêmes et la punissabilité s'est ainsi déplacée au stade de la planification et de la préparation de l'infraction. De même, dans le domaine de la lutte contre le crime organisé, la "simple" participation à une organisation criminelle a été déclarée punissable (art. 260ter CP). Ce déplacement de ce qui est considéré comme punissable rend la limite entre la prévention et la répression pénale de plus en plus floue.

La poursuite des infractions se fonde sur une répartition des compétences entre les cantons et la Confédération. Le Ministère public de la Confédération (MPC) et la Police judiciaire fédérale (PJF) se chargent des enquêtes de police judiciaire et de la poursuite des crimes. Au cours des dernières années, ces deux organes se sont considérablement renforcés et développés (Projet d'efficacité).

1.1.6 Délimitation entre la protection préventive de l'Etat (prévention) et les recherches préliminaires relevant de la police judiciaire

Les recherches menées à titre préventif en vertu de l'art. 2 LMSI visent à récolter des renseignements exploitables au stade de la prévention, en particulier pour évaluer la situation de la menace et prendre des mesures préventives.

Il en va différemment des recherches préliminaires relevant de la police judiciaire. Celles-ci servent à faire la clarté sur la nécessité ou non d'une procédure pénale. Dans la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC; RS 360), le législateur a attribué le mandat de mettre au jour la grande criminalité au sens des art. 260ter et 340bis CP, de la combattre et d'exploiter pour ce faire un système d'information. Ces tâches sont aujourd'hui du ressort de la PJF. Les mesures de recherche d'informations autorisées dans ce contexte correspondent en grande partie à celles de la LMSI. Néanmoins, les recherches effectuées par la PJF se fondent sur des éléments constitutifs d'infraction concrets et visent l'application du droit pénal. Elles sont par conséquent effectuées dans un but répressif. Il ne peut y avoir de conflit de compétences avec les autorités préventives. Il n'y en a pas davantage lorsque la PJF recherche des informations et des indices pour étayer ses soupçons.

Il se peut néanmoins qu'il y ait des points de recoupement entre les recherches effectuées par les organes répressifs sur un comportement punissable concret et les recherches préventives relatives aux menaces pesant sur la sécurité de la Suisse, lorsque la personne suspecte ou l'infraction présumée sont l'objet de recherches préventives plus vastes. En d'autres termes, la même personne ou le même acte peuvent faire l'objet de recherches sous deux angles totalement différents: d'une part, des recherches visant à étayer des soupçons relatifs à une infraction concrète et, d'autre part, des recherches visant à apprécier la menace pesant sur la sûreté intérieure de la Suisse. Dans la pratique, on constate souvent, en Suisse comme à l'étranger, une superposition à court terme de recherches menées dans le cadre de procédures judiciaires et de recherches de longue durée relevant des services de renseignements. Cette juxtaposition de la répression et de la prévention entraîne une valeur ajoutée et n'a pas de conséquences négatives lorsque l'échange d'informations fonctionne.

Le droit d'être renseigné répond à des règles identiques dans le domaine préventif et dans le cadre de recherches de police judiciaire. Ainsi, selon l'art. 14, al. 4, LOC et l'art. 18, al. 6, LMSI, les personnes recensées ayant déposé une demande de renseignements et qui ont tout d'abord adressé une demande indirecte au préposé fédéral à la protection des données, conformément aux réglementations de l'art. 14, al. 2, LOC et de l'art. 18, al. 1, LMSI, seront renseignées directement dès lors que les intérêts liés au maintien de la sûreté intérieure n'exigent plus le secret, au plus tard lors de l'expiration de l'obligation de conserver les données. Cette protection juridique ultérieure est également assurée au moyen d'un avis a posteriori sur les recherches d'informations réalisées en secret.

1.1.7 Collaboration entre le SAP et la PJF

Le but préventif de la protection de l'Etat n'exclut pas que des informations provenant des services de renseignements puissent être transmises aux autorités de poursuite pénale suisses et étrangères lorsqu'elles peuvent servir à poursuivre des infractions. Il existe d'ailleurs une obligation de transmettre les informations importantes pour la poursuite pénale aux autorités répressives suisses (cf. art. 17, al. 1, LMSI).

Lorsque le SAP, dans ses activités de renseignement, trouve des indices propres à fonder des soupçons, il les transmet aux organes de poursuite pénale compétents de la Confédération ou des cantons. Selon le degré de concret des indices transmis, les autorités de poursuite pénale pourront ouvrir directement une poursuite pénale ou faire des recherches pour étayer encore des soupçons concrets ou les écarter.

A l'inverse, l'art. 13 de la LMSI oblige les services de police et les organes de poursuite pénale à fournir des renseignements au SAP et, en cas de menaces concrètes pesant sur la sûreté intérieure ou la sûreté extérieure, à fournir les informations disponibles au SAP sans qu'il les demande. Ces autorités font d'autres communications au SAP sur la base de la mission générale d'information de l'art. 11 LMSI ou dans le cadre de mandats spécifiques.

1.1.8 Comparaison sous forme de tableau

Tant les organes chargés de la répression que ceux chargés de la prévention assument des tâches dans le domaine de la sécurité. Mais les questions sont analysées sous des angles différents. Le but des recherches (répression ou prévention) est le critère déterminant de délimitation:

Soupçon	
de menace pour la sécurité de la Suisse par le terrorisme, l'extrémisme violent, le service de renseignements prohibé, la prolifération	**d'infraction ou d'acte préparatoire selon le droit pénal fédéral ou cantonal**
Compétences	
Prévention Service d'analyse et de prévention / services de renseignements cantonaux	**Répression** Police judiciaire fédérale, Ministère public de la Confédération, autorités de poursuite pénale cantonales
Activités	
Recherches ciblées relevant des services de renseignements / recherche d'informations Activité d'analyse dans le domaine de la sûreté intérieure	Enquêtes de police judiciaire (impliquant éventuellement l'engagement de mesures de contrainte relevant de la procédure pénale)
Objet	
Tous les actes constituant une menace pour la sécurité, indépendamment du fait qu'ils soient qualifiés ou non d'infractions	Les actes donnant lieu à une peine et les soupçons propres à donner lieu à l'ouverture d'une procédure pénale
But	
But préventif: Recherches ayant pour but d'acquérir la certitude de l'existence d'une menace possible pour les fondements démocratiques et les fondements de l'Etat de droit de la Suisse ou pour les libertés de ses citoyens Stratégie (activité durable d'observation)	But répressif: Recherches ayant pour but d'acquérir la certitude qu'une infraction a été commise ou qu'il y a eu des actes préparatoires délictueux Cas concret
Résultat	
Rapport à l'attention des autorités politiques, éventuellement mesures politiques ou administratives	Exécution de la procédure par les autorités pénales (non-lieu, condamnation, acquittement), éventuellement exécution de la peine

Echange d'informations	
Echange d'informations informel avec les services de renseignements et de sécurité étrangers Surveillance par les organes chargés de la protection des données et les autorités politiques	Echange d'informations formel avec les autorités de justice et de police étrangères
Surveillance	
Organes chargés de la protection des données et autorités politiques	Organes chargés de la protection des données et autorités de justice pénale
Bases légales	
LMSI	LOC droit pénal fédéral / cantonal droit de la procédure pénale fédéral / cantonal

1.2 Situation de la Suisse en matière de sécurité et risques auxquels elle est exposée

La LMSI réglemente la protection préventive de l'Etat en Suisse. Elle est fortement influencée par ladite "affaire des fiches" et accorde une grande importance aux questions liées au traitement des données. Le législateur a largement renoncé aux mesures de recherche d'informations touchant à la sphère privée. L'accent est mis sur la limitation de la protection de l'Etat, plutôt que sur sa fonction de protection elle-même. Cette optique transparaît clairement dans le message de l'époque:

"La loi ne prévoit la recherche d'informations concernant une poursuite pénale potentielle qu'en cas de nécessité absolue." (Message du 7 mars 1994 concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire "S.o. S. – pour une Suisse sans police fouineuse, FF 1994 II 1126). L'idée de la loi est de garantir la sûreté intérieure en utilisant les instruments existants que sont les mesures répressives et les décisions en gardant les mesures préventives pour les domaines dans lesquels il convient d'écarter des menaces sérieuses pesant sur des biens juridiques essentiels. La loi répond par conséquent au principe qu'il est possible de remédier à certaines atteintes à la sûreté intérieure par des mesures ultérieures.

Néanmoins, la situation de la menace s'est considérablement dégradée depuis l'adoption de la LMSI. Il convient donc d'adapter la loi à la nouvelle situation de la menace.

1.2.1 Terrorisme

Il n'existe pas de définition universellement valable du terrorisme, qui soit reconnue aux plans national ou international. En 2003, le Parlement s'est déclaré opposé à l'introduction d'une norme pénale générale contre le terrorisme. L'art. 260^{quinquies} CP sur le financement du terrorisme, entré en vigueur en 2003, contient néanmoins une définition légale indirecte de ce qu'est le terrorisme. Il rend punissable "celui qui, dans le dessein de financer un acte de violence criminelle visant à intimider une population ou à contraindre un Etat ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque, réunit ou met à disposition des fonds".

Cette description correspond largement à celle de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI, RS 120.2; art. 8, al. 1, let. a), selon laquelle les activités terroristes sont des "menées déployées en vue d'influencer ou de modifier les structures de l'Etat et de la société, susceptibles d'être réalisées ou favorisées en commettant des infractions graves ou en menaçant de s'y livrer, et en faisant régner la peur et la terreur". Cette description découle des directives du DFJP du 9 septembre 1992 sur la mise en œuvre de la protection de l'Etat. Elle correspond à son tour sur des points importants aux critères proposés par l'OCDE dans une définition des actes terroristes fournie à des fins actuarielles: usage de la violence ou menace d'usage de la violence avec l'objectif politique, religieux, ethnique, idéologique ou d'ordre similaire, d'influencer ou de déstabiliser un gouvernement, ou de susciter la crainte dans tout ou partie de la population.

Cette définition ne doit rien changer à la situation juridique, ni à la pratique ancrée depuis 1992 dans la protection préventive de l'Etat. La définition de l'OMSI doit demeurer valable. Il n'y a pas lieu d'ancrer une définition dans la loi formelle car il n'y a pas d'unanimité à l'échelon international.

La sécurité de la Suisse s'est dégradée durablement, en particulier dans le contexte de la menace terroriste de ces dernières années. Selon l'appréciation actuelle, la Suisse ne constitue certes pas une cible première du terrorisme islamiste, mais la menace générale d'actes terroristes sur l'Europe est grande, et la Suisse, comme d'autres pays d'Europe occidentale, n'en est pas exclue. Le Conseil fédéral est parvenu à cette appréciation dans son Analyse de la situation et des menaces pour la Suisse à la suite des attentats terroristes du 11 septembre 2001, datée du 26 juin 2002, et rédigée à l'attention du Parlement. La situation continuant d'être tendue en Irak et au Proche-Orient, la menace reste élevée, en particulier pour les citoyens et les intérêts américains, ainsi que pour les alliés des Etats-Unis, tels que la Grande-Bretagne, l'Italie, l'Espagne et la Pologne, mais aussi pour des Etats tels qu'Israël et, en raison de l'importante minorité musulmane qu'elles abritent, la France et l'Allemagne.

Le terrorisme islamiste a pris l'Europe pour cible: Istanbul (les 15 et 20 novembre 2003), Madrid (le 11 mars 2004) et Londres (les 7 et 21 juillet 2005). Les attentats-suicides survenus à Londres le 7 juillet 2005 ont été les premiers attentats-suicides d'origine islamiste à frapper l'Europe occidentale. L'Europe occidentale n'est donc plus seulement une base arrière. Les menaces terroristes ne concernent plus seulement les intérêts anglo-américains et israéliens, mais, de manière générale, les intérêts occidentaux, dont les Nations Unies et le CICR, qui ont leur siège en Suisse, font partie du point de vue des islamistes. Pour propager la terreur, les terroristes

recherchent la publicité et les attentats à l'explosif dans des lieux où la concentration humaine est importante en constituent un moyen. Mieux les cibles traditionnelles sont sécurisées et plus la probabilité que les terroristes s'attaquent à des cibles moins bien protégées (dites "cibles molles") est grande. Enfin, il convient de tenir compte plus que jamais du fait que les recherches menées dans les Etats voisins contre les réseaux terroristes sont plus assidues (car les ressources en personnel sont plus importantes et que les instruments à disposition vont plus loin).

Aujourd'hui, les terroristes utilisent tous les moyens disponibles. Pour attirer l'attention de la communauté internationale, des événements de plus en plus terribles sont organisés et des actes de violence de plus en plus sanglants sont commis. Alors que les attentats conventionnels – les attentats de New York (plus de 3000 morts, des milliers de blessés) et de Madrid (191 morts, env. 1500 blessés) - ont atteint un sommet de cruauté, la crainte d'attaques nucléaires (atomiques ou radiologiques), biologiques ou chimiques ne fait que croître.

Les attentats terroristes du 11 septembre 2001 ont également confirmé que les sociétés industrielles modernes continueront d'être confrontées à un large spectre de menaces, dont le terrorisme classique fait partie. Les schémas d'action traditionnels de la politique de sécurité ont ainsi été remis en question. Cette remise en question concerne essentiellement l'influence des acteurs non étatiques, l'importance croissante de la guerre asymétrique et la recherche préventive d'informations des services de renseignements.

La menace de terrorisme nucléaire est décrite par les experts – notamment par le directeur général de l'Agence internationale pour l'énergie atomique – comme réelle et actuelle, en particulier la menace de terrorisme radiologique au moyen d'une bombe dite sale (bombe contenant des explosifs conventionnels, auxquels on a adjoint du matériel radioactif). Si, dans ce cas, le nombre de morts et de blessés pourrait demeurer limité, l'effet serait néanmoins destructeur sur les plans politique, psychologique et économique. Le terrorisme biologique peut avoir le même potentiel destructeur qu'une attaque nucléaire, par exemple par la diffusion de souches de maladies facilement transmissibles telles que la variole ou la peste bubonique. Une fois mise en circulation, une telle arme ne serait plus contrôlable et pourrait prendre la forme d'une pandémie dévastatrice. Les armes chimiques par contre semblent moins adaptées pour les terroristes. Si, localement, elles pourraient avoir le même potentiel destructeur que les armes atomiques ou biologiques, leur effet resterait limité à un territoire précis.

Depuis les attentats terroristes de Madrid et de Londres, l'Europe occidentale est passée du statut base arrière à celui de terrain d'action du terrorisme islamiste. La situation actuelle se caractérise par l'existence de très petites cellules (qu'il est par conséquent difficile d'infiltrer), sans structure hiérarchique, agissant de manière autonome et souvent indépendamment d'autres cellules et sans contacts avec l'extérieur. L'utilisation de moyens modernes de communication, tant pour la communication interne que pour la diffusion de l'idéologie, et donc pour la radicalisation, se fait en connaissance de cause. Il est particulièrement frappant de constater chez certains la volonté de donner sa vie comme martyr de l'islam dans un attentat-suicide, comme celui de Londres le 7 juillet 2005. A cela s'ajoute que les auteurs d'attentats sont de plus en plus fréquemment recrutés parmi les descendants d'immigrés étrangers, qui sont nés et ont grandi dans le pays-cible, qui en

connaissent très bien les habitudes et également les faiblesses, qui ont l'air bien intégrés et qui ne se sont pas fait remarquer par leur idéologie. Ils se comportent comme des Occidentaux, mais utilisent des langues non européennes, ce qui ne facilite pas l'appréhension de leurs intentions. Par ailleurs, ils savent comment échapper aux mesures des services de renseignements. Or, si ces derniers ne peuvent pénétrer dans la sphère privée, il leur est impossible de reconnaître à temps les structures décrites plus haut, de les surveiller et de les contrôler de quelque manière que ce soit. Des informations provenant de procédures pénales menées en Suisse et dans les pays voisins montrent clairement que notre pays est mis à profit par des personnes soutenant Al-Qaïda.

1.2.2 Service de renseignements prohibé

La notion de service de renseignements prohibé est utilisée en Suisse pour désigner l'espionnage. Les services de renseignements étrangers s'intéressent depuis toujours à la Suisse et à ses intérêts à l'étranger. Ils sont en quête d'informations politiques, économiques et militaires.

De l'avis du Conseil fédéral, il faut différencier le service de renseignements politiques et militaires d'une part, et l'espionnage économique de l'autre. S'agissant de l'espionnage économique, il revient principalement aux entreprises de prendre les mesures appropriées.

Il n'en est pas de même pour le service de renseignements politiques et militaires, contre lequel l'Etat prend depuis toujours des mesures.

Il s'avère que, depuis l'entrée en vigueur de la LMSI, moins d'espions ont pu être démasqués, moins de structures d'espionnage ont été mises au jour et il est plus difficile d'intervenir efficacement contre le service de renseignements prohibé. La clôture de certaines procédures a fait naître la fausse impression que la Suisse n'était plus ou presque plus touchée par l'espionnage. Car, selon les informations dont dispose le SAP, certains pays dissimulent une armada d'officiers de leurs services de renseignements parmi les membres de leur personnel diplomatique en Suisse. A cela s'ajoutent les recherches d'informations effectuées par des bureaux d'investigation et des détectives privés internationaux.

S'agissant du service de renseignements politiques et militaires, il serait illusoire de croire que les services de renseignements étrangers ont mis fin à leurs activités à l'issue de la guerre froide. Le fait que certains pays détachent en Suisse un grand nombre d'officiers de leurs services de renseignements (identifiés ou présumés) montre bien que les activités de renseignement se poursuivent. Si elle ne peut avoir accès aux locaux privés (par des moyens techniques de surveillance, etc.), l'autorité suisse chargée du contre-espionnage pourra difficilement s'opposer à ces activités, car les personnes-cibles ont bénéficié d'une formation professionnelle et disposent de l'équipement nécessaire pour les rendre aussi discrètes que possible. Dans le domaine du contre-espionnage, les compétences en matière de recherche d'informations font de plus en plus cruellement défaut.

1.2.3 Extrémisme violent

La notion d'extrémisme violent désigne les menées déployées par les organisations dont les membres rejettent la démocratie, les droits de la personne humaine ou l'Etat de droit et qui, pour atteindre leurs buts, commettent des actes de violence, les préconisent ou les soutiennent (art. 8, al. 1, let. c, OMSI). Les activités extrémistes renferment un important potentiel de violence et peuvent, même si ce n'est pas automatique, constituer une menace pour la sûreté intérieure d'un pays. Il convient par conséquent de pouvoir reconnaître à temps et prévenir les activités potentiellement violentes des organisations extrémistes.

En Suisse, les milieux de l'extrême droite et de l'extrême gauche sont constitués de nombreux petits groupes, souvent reliés entre eux. Il y a près d'un millier d'extrémistes de droite en Suisse et quelque 2000 extrémistes de gauche. Des groupes extrémistes étrangers utilisent eux aussi la marge de manœuvre relativement grande que leur offrent les droits fondamentaux en Suisse.

Le Conseil fédéral estime néanmoins que la situation juridique actuelle suffit à contenir la menace dans ce domaine.

1.2.4 Commerce illicite d'armes et de substances radioactives et transfert illégal de technologie (prolifération)

La prolifération est la dissémination d'armes nucléaires, chimiques et biologiques et de leurs porteurs (p. ex. fusées), et des biens à double usage nécessaires à leur fabrication. Le transfert de la technologie correspondante en fait également partie.

En situation normale, il n'est pas possible d'acquérir des armes ABC comme produits finis dans le commerce international d'armes. Les milieux qui s'intéressent à ce genre d'armes sont par conséquent tenus de mettre sur pied leurs propres sites de recherche et développement et de production. Il leur faut également des machines, des appareils de mesure et des matériaux qui peuvent également être utilisés dans de nombreux domaines civils (biens à double usage). Ainsi, de manière générale, la livraison de pièces de rechange pour un tunnelier n'est pas problématique. Il n'en va pas de même si la machine doit servir à la construction d'une unité souterraine de fabrication d'armes chimiques ou de fusées.

Il est beaucoup plus facile et moins onéreux de développer et de produire des armes biologiques et chimiques que des armes nucléaires.

Les moyens les plus divers peuvent entrer en jeu pour l'acquisition du savoir-faire nécessaire (débauchage de spécialistes, fondation de sociétés-écrans, rachat de sociétés fabriquant la technologie nécessaire, importation de technologie en cachant l'utilisation et l'utilisateur finaux, etc.).

La Suisse est signataire de l'ensemble des traités internationaux interdisant le commerce d'armes de destruction massive, ainsi que de tous les accords sur le contrôle de l'armement.

La mise au jour du réseau de transfert de technologie nucléaire du père de la bombe atomique pakistanaise, Abdul Qadeer Khan, a montré non seulement à quel point la structure de tels réseaux est complexe et professionnelle, mais aussi que la Suisse

peut être entraînée dans de telles machinations et que ses infrastructures peuvent être et sont mises à profit. Sa réputation risque de s'en trouver écornée.

Dans le domaine du commerce illicite d'armes et de substances radioactives, des réseaux extrêmement complexes sont à l'œuvre, souvent à l'échelon international (si bien qu'un pays n'abritera souvent qu'une partie du puzzle). Les discussions et les processus importants n'ont pas lieu en public, mais en toute discrétion dans des locaux privés. Il n'est pas rare que d'importantes sommes d'argent entrent en jeu dans de telles transactions, ce qui incite encore plus les personnes concernées à garder le silence et à prendre des mesures de précaution encore plus importantes. Comme l'expérience l'a montré, seuls de vagues éléments de soupçons quant à des menaces pesant sur la sécurité sont disponibles dans une première phase. Cela est par exemple le cas lorsqu'une personne connue des services de renseignements entre en Suisse sans que le motif concret du voyage ne soit connu ou lorsque le motif en question entraîne des doutes et des inquiétudes. La clarification de soupçons liés à des faits définis actuels, selon lesquels des personnes ou des organisations constitueraient une menace importante pour la sûreté intérieure ou extérieure de la Suisse, n'a pas de chance d'aboutir dans le domaine de la prolifération si les services de renseignements ne peuvent pas surveiller la sphère privée ou secrète. La mise au jour du réseau de transfert de technologie d'Abdul Qadeer Khan, spécialisé dans la technologie nucléaire prouve que le savoir-faire suisse (infrastructures ou technique) est utilisé de manière ciblée.

1.2.5 Crime organisé

Le crime organisé revêt une dimension internationale et peut, à moyen terme, constituer une menace majeure pour la société, l'Etat et l'économie. L'établissement du blanchiment d'argent, de la corruption et du rachat d'entreprises et d'immeubles dans les affaires courantes menace la stabilité économique et sociale. Les Etats eux-mêmes, notamment leur politique économique ou leur système policier et judiciaire, sont souvent des objets d'infiltration du crime organisé. Les groupes criminels, pour certains reliés entre eux, sont principalement actifs dans les domaines du trafic de stupéfiants, de la traite d'êtres humains, du trafic d'armes, de la corruption, du chantage et du blanchiment d'argent. Les liens que certains groupes du crime organisé entretiennent avec des groupes terroristes sont par ailleurs source d'inquiétude.

Les économies de marché développées, fortement interconnectées sur le plan international, offrent aux organisations criminelles de nombreuses possibilités d'infiltration et de blanchiment d'argent.

De l'avis du Conseil fédéral, le développement du MPC et de la PJF qui a eu lieu ces dernières années dans le cadre du Projet d'efficacité suffit à maîtriser la situation actuelle de la menace.

1.3 Appréciation de l'écart entre la situation de la menace et les moyens à disposition

Comme l'a constaté le Conseil fédéral dans son analyse de la situation et de la menace de 2002, la sécurité et la situation de la menace de la Suisse se sont peu à peu dégradées au cours des dernières années. Les risques se sont accentués, notamment du fait des attentats violents commis par des islamistes. Les auteurs de ces attentats ne visent pas des personnalités particulières, mais entendent provoquer la mort d'un maximum de personnes, en commettant des attentats contre des infrastructures civiles. Le Conseil fédéral est d'avis qu'il faut prévenir de tels actes, en reconnaître les actes préparatoires et empêcher la commission des attentats. Il y a lieu, pour ce faire, de prendre des mesures en vue d'observer les personnes et groupes dangereux et de pouvoir compter sur une coopération internationale optimale.

Les possibilités préventives offertes par la loi, très restrictives, ne suffisent plus à maîtriser la situation de la menace actuelle. Des lacunes manifestes existent, en particulier dans les domaines de la recherche et du traitement des informations.

Ainsi, la sphère privée et secrète ne peut être soumise à observation, quelle que soit la situation de la menace. Il n'est pas possible d'observer les rencontres et les discussions qui ont lieu dans des locaux privés. Il n'est pas davantage possible de surveiller les communications électroniques entre des groupes terroristes ou des personnes spécifiques. Les répercussions sont de plus en plus négatives car les personnes et les groupes ne sont plus structurés de manière hiérarchique en commandos, mais agissent de manière plus ou moins indépendante et ne sont liés entre eux que par des communications électroniques ou par l'intermédiaire de courriers. Il faudrait pour surveiller ces communications utiliser des techniques fondées sur Internet, auxquelles les autorités préventives n'ont pas accès.

Lorsqu'il n'y a aucune communication entre les groupes et les personnes, les autorités chargées de la protection de l'Etat doivent essayer d'acquérir des informations en prenant des identités d'emprunt. C'est là un moyen de découvrir les intentions dangereuses et les menaces, qui fait actuellement défaut.

Par ailleurs, il existe des lacunes dans les bases légales formelles permettant de recourir à l'exploration de signaux, tant dans la LMSI que dans la LAAM. Au cours des dernières années, le Conseil fédéral a dû à plusieurs reprises avoir recours à ses compétences constitutionnelles pour interdire les activités de certaines personnes constituant une menace pour la sécurité de la Suisse ou pour ses relations avec l'étranger. S'il devient nécessaire de prendre régulièrement de telles mesures, elles doivent faire l'objet d'une réglementation dans une loi. Les compétences constitutionnelles du Conseil fédéral ne doivent être utilisées que dans des cas exceptionnels.

1.4 Options d'action

Suite à la dégradation de la situation de la menace, des actions s'imposent, notamment dans les domaines du terrorisme et de la prolifération. Le service de renseignements politiques et militaires dirigé contre la Suisse est lui aussi intolérable. Il est indispensable de réduire les risques pour la sécurité dans ces domaines.

Il s'agit d'examiner les solutions possibles :

- l'utilisation pleine et cohérente des possibilités existantes dans les domaines du droit pénal et de la protection préventive de l'Etat;
- l'amélioration du flux d'informations et de la coordination entre les autorités chargées de la répression et celles chargées de la prévention;
- le développement du droit pénal formel et matériel;
- le développement de la protection préventive de l'Etat (modification de la LMSI).

1.4.1 Utilisation pleine et cohérente des possibilités existantes dans les domaines du droit pénal et de la protection préventive de l'Etat

Rien ne démontre concrètement que les compétences légales actuelles ne sont pas utilisées pleinement et de manière systématique. Néanmoins, il n'est pas possible de collecter les informations nécessaires pour combler de manière satisfaisante les lacunes en matière de sécurité, même en interprétant et en appliquant le droit d'une manière aussi extensive que possible. Il serait souhaitable que les dispositions pénales soient utilisées pleinement en faveur de la LMSI. Tel pourrait être le cas par exemple si les conditions nécessaires à l'ouverture d'une procédure pénale étaient moins restrictives ou si les ressources engagées étaient beaucoup plus importantes. Mais les lacunes existantes ne pourraient néanmoins pas être comblées avec de telles mesures.

1.4.2 Amélioration du flux d'informations et de la coordination entre les autorités chargées de la répression et de la prévention

Le SAP est informé de toutes les recherches préventives effectuées par la Confédération et les cantons dans le domaine de la sûreté intérieure. Il n'en est pas de même des recherches effectuées par les autorités de poursuite pénale, car l'état des connaissances reste limité aux informations transmises par lesdites autorités.

La question se pose de savoir si les déficits d'information existant aujourd'hui dans le domaine de la prévention peuvent être comblés par une amélioration du flux d'informations entre les autorités chargées de la répression et celles chargées de la prévention. La réponse est négative, ne serait-ce que pour des raisons structurelles. En effet, les informations de nature répressive sont collectées dans un cas concret et se limitent aux enquêtes menées dans une procédure pénale concrète par rapport à des éléments constitutifs d'infraction précis. Or les besoins en matière d'information des autorités chargées de la prévention, qui sont liés à l'appréciation exhaustive de la situation de la menace et à la prise des mesures préventives correspondantes, sont bien plus vastes et revêtent un caractère stratégique, d'où la nécessité de procéder à des observations de manière permanente.

L'échange d'informations entre le MPC, la PJF et le SAP fait l'objet d'améliorations permanentes. La collaboration est prévue dans le détail dans des lois, des ordonnances et des directives. Les procédures internes sont établies et sont régulièrement soumises à examen. D'autres mesures sont en cours. Il est clair aujourd'hui déjà que les lacunes dans le domaine de la recherche d'informations en Suisse ne pourront être comblées totalement grâce à un nouveau train d'améliorations.

1.4.3 Développement du droit pénal formel et matériel

Il s'agit en l'occurrence de vérifier si les déficits d'information du SAP pourraient être comblés par un développement du droit pénal matériel (p. ex. une norme pénale sanctionnant les personnes incitant à la haine) ou formel (p. ex. des programmes de protection des témoins).

Les arguments en faveur de cette solution sont les suivants: il serait possible de se reposer sur les structures et le droit de la procédure existants, tout en développant une protection juridique lors de la prononciation de mesures de contrainte relevant de la procédure pénale ou de l'exécution de telles mesures. La doctrine et la jurisprudence sont denses dans ce domaine. En d'autres termes, le système en place fonctionne et peut servir de base.

Mais les réflexions suivantes s'y opposent:

- Les services de renseignements déploient une activité d'observation permanente et se limitent principalement à la mise au jour de faits et de structures. Avant cette mise au jour, il n'y a en principe aucun intérêt à intervenir immédiatement.
- Les recherches de type répressif en rapport avec une infraction et les instruments à disposition n'ont pas le même but que les recherches de type préventif menées par les services de renseignements, qui visent à rechercher des informations dans un contexte de politique de sécurité en vue d'apprécier la situation, et éventuellement de prendre des mesures préventives.
- Avec la LMSI, le législateur a voulu tracer une ligne claire entre la répression et la prévention, que le Conseil fédéral a répercutée de manière conséquente dans la réorganisation de l'Office fédéral de la police. Il convient de s'en tenir à cette conception.
- Si la recherche préventive d'informations avait lieu avec les instruments de la répression, cela reviendrait à réintroduire les méthodes de travail de l'ancienne Police fédérale et à remettre la séparation en question.
- Pour que des informations puissent être collectées avec des instruments relevant de la répression, il faut qu'une enquête de police judiciaire ait été ouverte. Si celle-ci n'aboutit à aucun résultat, la personne concernée continuera de facto à porter une image négative. Cela est notamment le cas lorsque le grand public a été informé de la procédure. Il peut en résulter des poursuites contre les autorités, notamment lorsque, en raison de l'image négative qui lui est collée, une personne voit son existence économique anéantie ou remise en question.
- Rendre punissable la phase préparatoire d'une infraction en allant plus loin que les art. 260^{bis} et 260^{ter} CP, qui concernent les actes préparatoires délictueux, serait non seulement contraire à la systématique du code pénal, mais ne parviendrait pas à combler les lacunes dans la recherche préventive d'informations, car le but de ces dispositions est tout autre.

- Toute action répressive se fonde sur une norme pénale. Dans une telle norme, le comportement répréhensible est décrit de manière précise. Si une norme pénale permet des actes d'enquête de grande ampleur visant à collecter des informations à titre préventif, le comportement punissable doit être décrit de manière très large. Cependant, la norme perd ainsi de sa prévisibilité, c'est-à-dire que l'individu ne sait plus comment il doit se comporter pour continuer de respecter la loi.
- Selon le droit en vigueur, une action répressive ne peut être entreprise que si les soupçons de commission d'une infraction sont suffisants. Or c'est justement ce qui fait défaut lorsque les services de renseignements lancent des recherches. Dans une première phase, il n'y a que des suppositions et de vagues indices. A cela s'ajoute que les menaces pour la sûreté intérieure ne sont souvent pas reconnaissables a priori et que les actes correspondants ne peuvent pas (encore) être poursuivis selon le droit pénal. Ainsi, si l'on veut créer une infraction permettant que des recherches préventives soient engagées rapidement, il faudrait renoncer à des soupçons initiaux ou alors en exiger un minimum. Néanmoins, des procédures pénales sans soupçons seraient contraires au principe selon lequel les procédures pénales doivent être dûment motivées.

Ainsi, les inconvénients d'un développement du code pénal dépassent de loin les avantages.

1.4.4 Développement de la protection préventive de l'Etat (modification de la LMSI)

Les lacunes constatées grèvent la prévention des menaces et en particulier la protection préventive de l'Etat. Dans la mesure où la LMSI réglemente les tâches et les moyens de la protection préventive de l'Etat, c'est là qu'il faut intervenir. Là aussi, il est possible de s'appuyer sur un système qui a fait ses preuves, avec des structures existantes.

Par ailleurs, d'autres éléments parlent en faveur d'un développement de la LMSI:

- La prévention est un instrument de la politique de sécurité. Ce sont les responsables politiques, ou l'exécutif, qui indiquent leurs besoins dans le cadre de la loi et qui attribuent les mandats correspondants. C'est également à eux qu'il s'agit de donner la possibilité de reconnaître à temps les menaces d'ampleur nationale relevant de la politique de sécurité et de les intégrer dans l'appréciation politique. Enfin, ce sont eux qui, sur la base entre autres des informations fournies par les autorités fédérales et cantonales chargées de la sécurité, prennent les décisions en matière de politique de sécurité et en assument la responsabilité. Il paraît donc judicieux de combler les lacunes constatées dans le dispositif préventif dans le cadre de la LMSI, qui est placée sous le contrôle et sous la surveillance des responsables politiques.
- Tous les moyens à disposition, les instruments tant préventifs que répressifs, doivent être utilisés pour lutter contre le terrorisme et les autres menaces du même type. Pour reconnaître les menaces à temps et les prévenir, c'est-à-dire pour empêcher les actes terroristes et autres, c'est la prévention qui prime et, par conséquent, le travail des services de renseignements.
- Les services de renseignements de tous les pays ne sont pas au même niveau. En rapprochant certaines compétences des services de renseignements suisses

de celles de pays voisins, il sera possible d'éviter que notre pays ne devienne un espace de moindre sécurité.
- Le développement de la LMSI renforcera durablement la coopération internationale.
- Le développement de la LMSI ne modifiera en rien les principes de la procédure pénale selon lesquels il faut des soupçons suffisants pour qu'il puisse y avoir une enquête de droit pénal et selon lesquels les personnes soumises au droit doivent savoir quels sont les comportements répréhensibles.
- Le développement de la prévention permettra d'obtenir des informations durables et approfondies sur les domaines de la grande criminalité. Ces informations parviendront pleinement aux organes répressifs agissant de manière ponctuelle et leur permettront d'engager leurs ressources de manière ciblée.
- Les recherches ciblées effectuées par les services de renseignements et les mesures prises précocement permettent d'éviter des infractions graves, de renoncer dans de nombreux cas à l'ouverture d'une procédure pénale, longue et gourmande en ressources, et par conséquent de décharger efficacement les autorités de poursuite pénale.

1.4.5 Révision totale ou partielle?

Il reste à examiner si les travaux législatifs à venir exigent une révision totale ou partielle. Préférence est donnée à une révision partielle pour les raisons suivantes:

- Pour l'heure, nul ne sait ce qu'il adviendra des réglementations proposées dans le cadre du volet LMSI I (lutte contre la violence lors de manifestations sportives) après écoulement de leur durée de validité (2009).
- Les modifications souhaitées dans le cadre du volet LMSI II se présentent certes sous la forme de nombreux articles de loi, mais se concentrent sur le plan matériel sur un nombre restreint de thèmes, l'accent étant clairement mis sur la recherche d'informations grâce à des moyens spéciaux.
- Les modifications souhaitées ne s'intègrent pas de manière idéale dans la systématique de la loi, mais cette intégration est néanmoins défendable.
- La LMSI devra encore être adaptée au-delà des volets législatifs LMSI I et II, notamment dans le domaine des contrôles de sécurité relatifs aux personnes.
- Il semble par conséquent bien plus judicieux de procéder à une révision totale à un moment ultérieur.

1.5 Projets législatifs en suspens dans le domaine de la sûreté intérieure

La législation dans le domaine de la sûreté intérieure fait constamment l'objet de modifications et de réaménagements. Actuellement, de nombreux accords internationaux, lois et ordonnances sont en élaboration ou en révision. Néanmoins, il n'existe pas de liens importants entre ces projets et le présent volet législatif (cf. annexe 1).

Le présent projet de révision a pour but premier l'amélioration de la recherche d'informations en vue de permettre l'appréciation de la situation dans le contexte de

la politique de sécurité et la prise des mesures qui en découlent. Il influence grandement l'ensemble du système de prévention des menaces et aura des répercussions indirectes sur le droit pénal formel et matériel.

Les bases légales fondant l'activité du SRS sont en cours de réexamen.

1.6 Comparaison et liens avec le droit européen

1.6.1 Généralités

Les législations qui existaient à l'étranger avant le 11 septembre 2001 et celles adoptées après ces attentats terroristes ne peuvent être appliquées telles quelles à la Suisse en raison des différences dans les situations de la menace, les systèmes juridiques (fonctions de l'exécutif, du législatif et du judiciaire) et les expériences de chaque Etat en matière de terrorisme (p. ex. Espagne / ETA).
L'aggravation de la menace terroriste a entraîné de manière générale un renforcement de la coopération entre les services de renseignements de la communauté internationale. Celle-ci a reconnu la nécessité d'agir ensemble dans la lutte contre le terrorisme et d'institutionnaliser la coopération internationale dans ce domaine. Ainsi, le Groupe antiterroriste / GAT (Counter Terrorist Group / CTG) fondé par le "Club de Berne" sert d'interface entre l'UE et les dirigeants des services de sécurité et des services de renseignements des Etats membres.
Début 2003 et à la mi-2005, l'Institut suisse de droit comparé (ISDC) a examiné les bases légales de la sûreté intérieure des principaux pays européens.
Dans tous ces Etats, la législation est influencée par les événements du 11 septembre 2001 aux Etats-Unis.

Les structures étatiques et la marge de manœuvre juridique varient d'un Etat à l'autre. Il n'est donc pas facile d'établir des comparaisons claires avec la Suisse et de tirer des conséquences pour notre pays. Les tableaux ci-dessous présentent les mesures adoptées sur le plan légal et les compétences existant dans certains pays choisis, ainsi que la protection juridique et le système de contrôle existant dans ces pays. Vous trouverez des explications détaillées en annexe. L'absence de réglementation légale expresse ne signifie pas forcément que la mesure en question n'est pas appliquée dans le pays concerné. Cela signifie que l'on considère qu'elle ne nécessite pas de réglementation ou qu'elle est comprise dans d'autres réglementations.

1.6.2 Comparaison juridique

Comparaison juridique avec d'autres pays

Mesure	Répression / poursuite pénale	Prévention
Exploration de signaux (art. 14a P)		Allemagne, France, Italie, Pays-Bas
Dédommagement des informateurs (art. 14b P)	France, Italie	Italie, France
Protection des informateurs (art. 14c P)	Autriche, Allemagne, France, Italie	Autriche, Allemagne, France, Pays-Bas
Identité d'emprunt (art. 14d P)	Autriche, Allemagne, France, Italie, Pays-Bas	Autriche, Allemagne, France, Pays-Bas
Surveillance de la correspondance par poste et télécommunication (art. 18k P)	Autriche, Allemagne, France, Italie, Luxembourg, Pays-Bas	Allemagne, France (pas de surveillance par poste), Italie, Luxembourg, Pays-Bas
Observation secrète d'un lieu qui n'est pas librement accessible au public (art. 18l P)	Autriche, Allemagne, France, Italie, Luxembourg, Pays-Bas	Autriche, Allemagne, France, Italie, Pays-Bas
Perquisition secrète dans un système informatique (art. 18m P)	Allemagne, France, Luxembourg, Pays-Bas	France, Pays-Bas
Interdiction d'activités dangereuses pour la sûreté intérieure ou extérieure (art. 18n P)	Autriche, Allemagne, Italie, Luxembourg, Pays-Bas	France, Allemagne, Autriche

Protection juridique et contrôles institutionnels à l'étranger

Pays	Contrôle ordinaire	Contrôle spécifique
Allemagne	**Général:** Haute surveillance du préposé à la protection des données, contrôle parlementaire; action en injonction auprès du tribunal administratif	**Surveillance de la correspondance par poste et télécommunication:** Requête du président de l'Office fédéral de protection de la Constitution ou par un représentant, mesure engagée par le ministère concerné; instance de contrôle: commission G 10 (commission constituée en vertu de l'art. 10 de la Constitution). Exception: péril en la demeure -> exécution immédiate et information ultérieure à la commission. **Identité d'emprunt:** accord du ministère fédéral de l'Intérieur
Autriche	Possibilité de recours auprès de la commission pour la protection des données, du tribunal administratif ou de la cour constitutionnelle	**Général:** contrôle du délégué à la protection juridique; contrôle parlementaire, les autorités chargées de la sécurité informent sans attendre le ministère fédéral de l'Intérieur; **Investigations secrètes et utilisation secrète d'enregistreurs d'images et de son**: suivi effectué par le délégué à la protection juridique;

France	Demandes de consultation de la "Commission nationale de l'informatique et des libertés" (CNIL)	**Surveillance de la correspondance par poste:** Requête du ministre de la Défense, du ministre de l'Intérieur et du ministre chargé des Douanes ou de leurs suppléants, ordre du premier ministre ou de deux personnes nommées par lui, instance de contrôle: "Commission nationale de contrôle des interceptions de sécurité", indépendante de l'administration
Italie	Chaque semestre, le gouvernement livre au Parlement un rapport sur les activités des services de protection des données (Garante per la protezione dei dati personali). Il contrôle les données collectées.	**Surveillance de la correspondance par poste et télécommunication:** Requête par le premier ministre, accord du juge. Le premier ministre peut déléguer ses compétences aux services; ordre du procureur général. En cas de péril en la demeure, ordre immédiat. Au plus tard dans les 24 heures, une autorisation doit être demandée par voie ordinaire auprès du juge. Le juge doit décider dans les 48 heures.
Luxembourg	Commission de contrôle parlementaire; contrôle de la surveillance des données par le procureur général ou l'un de ses délégués et par deux représentants d'une commission spéciale choisis par le ministre; l'organe supérieur de protection des données (ANS) veille à la sécurité des données classifiées.	**Surveillance de la correspondance par poste et télécommunication:** Requête par le Service de renseignements de l'Etat en accord avec la commission spéciale; ordre du directeur des services de télécommunication, qui fait exécuter et contrôler les écoutes par un organe spécialement prévu à cet effet. La commission de contrôle parlementaire est informée tous les six mois des mesures mises en œuvre en matière de contrôles téléphoniques.
Pays-Bas	Commission de surveillance; médiateur indépendant. Commission de contrôle parlementaire **Identité d'emprunt:** Il est permis d'ouvrir le courrier de tiers si le tribunal de district de La Haye approuve la demande du chef des services	**Surveillance de la correspondance par poste et télécommunication:** Requête par le chef de l'AIVD et du MIVD, ordre du ministre de l'Intérieur. En cas de péril en la demeure, une autorisation ultérieure est possible, si elle est demandée dans les plus brefs délais **Observation:** En général sur autorisation écrite du ministre compétent. Observation de locaux privés: d'entente avec le ministre de l'Intérieur ou le chef des services.

1.6.3 Comparaison avec la Suisse

Les structures de sécurité et la marge de manœuvre juridique des autorités chargées de la sécurité varient d'un Etat à l'autre. La comparaison des situations juridiques montre néanmoins que les mesures de prévention existant actuellement en Suisse et les ressources à disposition sont largement en deçà des possibilités dont disposent un grand nombre d'Etats d'Europe occidentale.

Il peut en résulter des lacunes dangereuses, ressenties à l'échelon international. Des autorités étrangères peuvent en effet opérer une recherche illégale d'informations sur territoire suisse. Il en a déjà été ainsi dans plusieurs cas.

Si la Suisse ne peut contribuer à la coopération internationale, elle se nuira à elle-même, car les autres Etats pourraient devenir réticents à fournir des informations. Il

pourrait en résulter un nouvel affaiblissement du dispositif suisse de prévention du terrorisme.

L'expérience des derniers attentats montre que les réseaux terroristes peuvent être mis au jour beaucoup trop tard s'il y a des ruptures dans le flux d'informations. Dans les cas où des attentats terroristes ont pu être déjoués, des moyens de recherche d'informations ont été utilisés dont la Suisse ne dispose pas à ce jour au niveau préventif. Citons, à titre d'exemples, l'attentat planifié contre le marché de Noël de Strasbourg en 2000, la découverte en 2003 à Londres d'un laboratoire fabriquant de la ricine, un poison végétal, la découverte du réseau islamiste "Hofstadt" aux Pays-Bas en 2003 ou encore l'attentat déjoué du groupe néonazi "Camaraderie Sud" contre l'inauguration du centre culturel juif en Allemagne.

La Suisse doit être en mesure d'approcher le standard minimal des autres Etats européens. Il n'est pas nécessaire pour l'heure d'adopter des mesures plus poussées.

1.7 Les nouvelles dispositions

L'objectif de la présente révision de loi est de mettre en œuvre les mesures découlant de l'"Analyse de la situation et des menaces pour la Suisse après les attentats du 11 septembre 2001" du 26 juin 2002 à l'attention du Parlement, ainsi que des interventions parlementaires déposées après le 11 septembre 2001.
Pour atteindre cet objectif, il faut, d'une part, améliorer l'efficacité des instruments utilisés par les services de renseignements pour rechercher des informations et, d'autre part, se rapprocher des normes européennes. Les autorités et les unités administratives de la Confédération et des cantons seront tenues, dans des cas concrets concernant uniquement la lutte contre le terrorisme, le service de renseignements politiques ou militaires prohibé et le transfert illégal de biens de technologie (prolifération d'armes de destruction massive), de fournir des renseignements précis. Les transporteurs commerciaux seront aussi soumis aux mêmes conditions et tenus de fournir des renseignements, dans la mesure où les données qu'ils auront en tout état de cause déjà récoltées seront nécessaires. Par ailleurs, il sera possible d'utiliser des moyens spéciaux de recherche d'informations sous certaines conditions très strictes et comme ultime mesure. En cas de soupçons fondés, il sera en outre possible de surveiller la correspondance par poste et télécommunication, de même que les lieux non accessibles au public - au besoin au moyen d'appareils techniques - et de perquisitionner des systèmes informatiques, et ce uniquement dans le cadre de la lutte contre le terrorisme, contre le service de renseignements politiques ou militaires prohibé et contre la prolifération.
L'utilisation de moyens spéciaux de recherche d'informations sera soumise à un double contrôle: la procédure sera ouverte par une demande de l'Office fédéral de la police. Le Tribunal administratif fédéral examinera ensuite si la demande est conforme au droit. Si l'examen juridique s'avère positif, la demande d'examen sous l'angle politique est envoyée au chef du DFJP, qui consulte le chef du DDPS en sa qualité de président de la Délégation du Conseil fédéral pour la sécurité. En cas d'accord, le chef du DFJP décide alors de la suite à donner à la demande; en cas de désaccord, c'est le Conseil fédéral qui prend la décision.
A la fin de l'opération, la personne visée devra être informée qu'elle a fait l'objet d'une surveillance, sauf dans des cas précis où des intérêts publics prépondérants l'exigent

et où la protection de tiers serait compromise. Le chef du DFJP fixe les exceptions à l'obligation de communication.
La compétence du Conseil fédéral d'interdire à une personne, une organisation ou un groupe de déployer une activité précise (p. ex. une collecte de fonds), si l'activité vise directement ou indirectement à propager, à soutenir ou à encourager de toute autre manière que ce soit des agissements terroristes ou extrémistes violents et menace concrètement la sûreté intérieure ou extérieure de la Suisse, doit être déléguée au chef du DFJP et faire l'objet d'une réglementation sur le plan législatif. Cela dit, la compétence d'interdire des organisations demeure une prérogative du Conseil fédéral.
La possibilité de recourir à des informateurs et le statut de leurs indemnisations (non soumises à l'AVS, ni à l'impôt) doivent être inscrites dans une loi formelle; ces informateurs doivent par ailleurs pouvoir jouir d'une protection en cas de besoin. Les informateurs et les collaborateurs du SAP doivent pouvoir être dotés d'une identité d'emprunt garantissant leur protection lors de leurs recherches d'informations. La présentation de la situation (qui a fait ses preuves depuis longtemps) par le Centre fédéral de situation doit être réglée dans une loi. Un ajout dans le domaine des contrôles de sécurité relatifs aux personnes (clearing) doit assurer que des Suisses, tout comme des étrangers domiciliés en Suisse, puissent continuer à collaborer à l'avenir à des projets classifiés à l'étranger.

1.8 Mise en œuvre

La mise en œuvre doit se fonder autant que possible sur les structures existantes de la Confédération (Tribunal administratif fédéral, Service d'analyse et de prévention) et des cantons (services de renseignements cantonaux). Environ 40 postes seront nécessaires pour les tâches exécutées par le Tribunal administratif fédéral et le Service des tâches spéciales (STS) du DETEC (pour la surveillance de la correspondance par poste et télécommunication), et pour la mise en œuvre, aux plans juridique, opérationnel et administratif, des nouveaux moyens de recherche, ainsi que pour le traitement des résultats obtenus auprès de l'Office fédéral de la police. Ces postes devront être compensés en interne au sein du DFJP.
Les postes supplémentaires sont donc pour l'essentiel nécessaires dans les domaines suivants:

- Renforcement des structures opérationnelles, notamment dans les services de police qui se chargeront de rechercher et de traiter les informations (policiers, interprètes, techniciens, analystes opérationnels);
- Renforcement des structures informatiques, notamment dans le domaine de la saisie des données, de l'assurance-qualité et de la correspondance avec l'étranger;
- Renforcement des structures étrangères aux services de renseignements, telles que celles du STS DETEC (chargé des aspects techniques et de l'administration) ou du Tribunal administratif fédéral (chargé du secrétariat).

La mise en œuvre des nouvelles compétences n'entraînera donc que de faibles besoins supplémentaires en ressources.

2. Commentaire des articles

2.1 Structure générale

L'introduction de moyens spéciaux de recherche d'informations obéissant à des règles distinctes de celles qui prévalent pour le régime ordinaire actuel se traduit, au niveau des subdivisions de la loi, par l'introduction d'un chapitre nouveau, décomposé en deux sections: la première définissant les conditions générales applicables aux nouveaux moyens et la seconde décrivant les différents moyens spéciaux de recherche d'informations et leurs modalités d'exécution. Cette présentation a des conséquences sur la structure générale de la loi; elle rend nécessaire l'élévation des sections actuelles au rang de chapitres.

2.2 Art. 2, al. 4, let. b^{bis} et b^{ter}

L'al. 4 énumère exhaustivement ce qu'il faut entendre par mesures préventives au sens de la LMSI. Il s'agit donc de compléter cette énumération pour tenir compte de l'introduction des nouveaux moyens spéciaux de recherche d'informations (let. b^{bis}), réglés dans le chapitre 3a, et de celle des interdictions d'activités (let. b^{ter}), réglées dans le chapitre 3b.

2.3 Art. 7, al. 2, 3e phrase

Conformément à l'art. 7, al. 2, LMSI, les cantons accomplissent de manière indépendante les tâches définies par la présente loi. Si plusieurs cantons doivent coopérer ou s'il y a péril en la demeure, l'office fédéral peut prendre la direction des opérations. Cette compétence doit être complétée de manière à permettre à l'office fédéral d'assumer la coordination de l'échange d'informations si cela facilite de manière significative le travail de la Confédération et des cantons. L'office fédéral doit donc garantir une coordination dans l'échange des informations entre les unités administratives (cantonales), qui conservent leurs compétences originelles. La notion de coordination indique que la mesure revêt essentiellement un caractère de coopération. Par ailleurs, le critère de l'importance significative montre clairement que l'échange réciproque d'informations doit présenter de nets avantages. Autrement dit, il faut que la coordination assurée par l'office fédéral soit à même d'apporter une amélioration substantielle de l'information pour tous les organes concernés. Enfin, la règle ne prévoit qu'une faculté et non une obligation de se charger de la coordination.

Intérêt public et proportionnalité
Cette extension du rôle de l'office dans l'exécution des tâches légales se justifie du fait que la prévention, notamment du terrorisme ou de l'extrémisme violent, devient de plus en plus compliquée compte tenu de l'internationalisation des divers mouvements du terrorisme ou de l'extrémisme violent. Le dépistage précoce des menaces implique, en effet, une connaissance pointue de réseaux complexes dépassant le cadre des frontières nationales. Il nécessite aussi de nombreux échanges d'informations avec des partenaires étrangers. Dès lors, cette mesure, en tant qu'elle se limite à la coordination, respecte le principe constitutionnel de la subsidiarité qui est déterminant pour la répartition des tâches entre la Confédération

et les cantons (cf. le nouvel art. 5a Cst., accepté par le peuple et les cantons le 28 novembre 2004 et dont l'entrée en vigueur est prévue pour le 1er janvier 2008).

2.4 Chapitre 3 Recherche générale et traitement des informations

En raison de la nouvelle structure de la loi, la section 3 actuelle devient le chapitre 3.

Quant au titre du chapitre, il doit être complété de manière à introduire la notion de recherche générale d'informations par opposition à celle de recherche spéciale (chapitre 3a). C'est, au niveau de la structure et de la terminologie, une des conséquences du changement d'orientation de la LMSI. La recherche générale d'informations correspond à celle qui a été pratiquée jusqu'à maintenant; elle recourt, conformément à la conception qu'avait le législateur de 1997 du rôle de la police préventive dans un Etat libéral, à des moyens de recherche peu contraignants (cf. la recherche d'informations à partir de sources accessibles au public ou l'observation de faits dans des lieux librement accessibles, art. 14, al. 2) et fondés essentiellement sur des règles d'entraide administrative entre autorités (cf. le devoir d'information des cantons, le devoir de renseigner de certaines autorités).

Quant au régime du traitement des informations, qui est l'objet central de la LMSI actuelle, il n'est pas modifié et, sauf disposition expresse dans le chapitre 3a, il s'applique aussi au traitement des données issues des moyens spéciaux de recherche d'informations.

2.5 Article 10a Situation en matière de sûreté intérieure

Cette disposition règle expressément au niveau de la loi une activité que les organes de sûreté fédéraux exercent déjà actuellement (cf. art. 9, al. 2, let. a, ch. 2, de l'ordonnance du 17 novembre 1999 sur l'organisation du Département fédéral de justice et police; RS 172.213.1).

Al. 1
L'Office fédéral de la police est responsable du traitement permanent de la situation dans le domaine de la sûreté intérieure. Il gère à ce titre le Centre fédéral de situation, qui intègre dans la présentation de la situation les éléments déterminants issus des différents domaines de la sûreté intérieure (cantons, autres services fédéraux). Le Centre fédéral de situation participe en outre de manière significative à la direction du réseau national de renseignements lors d'événements particuliers (p. ex. grandes conférences). Les tâches ne peuvent être accomplies sans un flux d'informations permanent, qui doit être réglementé.

Al. 2
Le Centre fédéral de situation a recours, entre autres, à une présentation électronique de la situation (PES) pour diffuser les informations relatives à la situation. Ce système d'information électronique ne constitue pas un fichier au sens de la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1). Les données personnelles n'y sont pas non plus traitées de manière systématique. Il s'agit plutôt d'un système d'information sur la situation, auquel les services autorisés

ont accès pour consulter des données actualisées concernant la situation en matière de sûreté intérieure. En cas d'événement particulier (p. ex. réseau de renseignements lors d'une manifestation de grande envergure; attentat terroriste), des informations supplémentaires liées à l'événement sont diffusées par le biais de la PES.

Le système de traitement des données relatives à la protection de l'Etat (ISIS) et la PES ne sont techniquement pas reliés. Les données personnelles publiques sont des données qui ont déjà été publiés par les médias. Les autres données personnelles sont intrinsèquement liées à un événement pertinent pour la situation. En vertu de la LMSI, les destinataires sont autorisés à recevoir ce genre d'informations.

Al. 3
Les services qui ont besoin des informations consultables dans la PES pour accomplir leurs tâches conformément à l'art. 17 (communication de données personnelles) ont accès à la présentation permanente de la situation de la PES. L'office fédéral règle l'accès aux contenus consultables dans un délai limité (présentation de la situation liée à un événement particulier) et à ceux ne renfermant pas de données sensibles.

Al. 4
L'al. 4 comble une lacune de la loi actuelle. Il permet, uniquement pour une durée déterminée, de communiquer des données à des services privés, limitées à la présentation de la situation liée à un événement (p. ex. aux entreprises de sécurité privées actives dans le cadre d'une grande manifestation). Pour ce faire, il faut que la communication soit nécessaire à la sûreté intérieure et extérieure.

2.6 Art.13, titre, al. 3 et 4 Devoir général de renseigner incombant aux autorités

L'introduction d'un autre devoir de renseigner (cf. art. 13a) commande une adaptation de l'art. 13, afin de mettre en évidence la différence entre les deux devoirs d'informer qui sont dorénavant prévus par la loi.

Titre
Le titre de l'art. 13 est modifié de manière à mettre en évidence le fait que tous les domaines de la LMSI sont visés par cet article, ce que suggère le qualificatif "général" pour définir le devoir de renseigner.

Al. 3
Puisque l'obligation de communiquer des renseignements concernant une menace liée au terrorisme, au service de renseignements politiques ou militaires prohibé, au commerce illicite d'armes et de substances radioactives ainsi qu'au transfert illégal de technologie devient une obligation permanente, la délégation au Conseil fédéral doit être réduite aux seuls domaines auxquels elle est encore susceptible de s'appliquer, à savoir à l'extrémisme violent et au service prohibé de renseignements qui ne sont ni politiques ni militaires et qui ne peuvent donc guère être que de nature économique.

Al. 4
Cette disposition est transférée dans un article autonome (cf. art. 13b), puisqu'elle doit s'appliquer aux différends surgissant entre autorités tenues de renseigner en vertu de l'art. 13a aussi bien que de l'art. 13. En outre, elle doit être adaptée au fait que ces devoirs de renseigner s'étendent dorénavant à d'autres autorités ou organismes que les autorités administratives ou les organes de poursuite pénale déjà mentionnés à l'art. 13, ce qui nécessite une révision du régime du règlement des différends.

2.7 Art. 13a Devoir spécifique de renseigner incombant aux autorités

Le projet de loi sera adapté à la révision partielle de la LMSI concernant la propagande incitant à la violence et la violence lors de manifestations sportives (modification du 24 mars 2006; LMSI I) au terme de la procédure de consultation. Cette révision a été approuvée par le Parlement mais n'est pas encore entrée en vigueur.

Comme nous l'avons dit précédemment, cette disposition introduit un nouveau devoir de renseigner. Elle constitue, par rapport à l'art. 13, une règle spéciale, qui est à la fois *plus étroite*, puisqu'elle ne vise que *certains des domaines* d'application de la LMSI (comp. l'al. 1 avec l'art. 2, al. 1 et 2, LMSI), et *plus large*, puisqu'elle vise *toutes les autorités* de la Confédération et des cantons ainsi que les organisations et établissements accomplissant des tâches de service public.

Al. 1
Cet alinéa circonscrit le devoir de renseigner à certains types de menaces (cf. let. a à c). Il s'agit de celles qui, de par leur gravité, sont le plus susceptibles de mettre en danger les valeurs fondamentales de notre pays. En d'autres termes, ce sont les menaces propres à mettre en cause l'existence ou le fonctionnement même de l'Etat en s'attaquant à ses institutions parlementaires, judiciaires ou gouvernementales, à miner son système démocratique en entravant l'exercice des droits populaires ou à paralyser le régime libéral en intimidant la population et en la poussant à des réflexes sécuritaires. Constituent, à notre avis, de telles menaces le terrorisme, le service de renseignements politiques ou militaires prohibé et le commerce illicite d'armes et de substances radioactives ainsi que le transfert illégal de technologie.

Cette disposition oblige en principe toutes les autorités et unités administratives de la Confédération et des cantons à fournir des renseignements. A titre d'exemple, le Bureau de communication en matière de blanchiment d'argent (MROS) fait partie des unités administratives de la Confédération. Par unités administratives des cantons, on entend aussi celles des communes. Les organisations qui accomplissent des tâches de service public sont aussi tenues de fournir des renseignements. En vertu de l'art. 2, al. 4, de la loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA; RS 172.010), il s'agit d'organisations de droit public ou privé qui sont extérieures à l'administration fédérale, auxquelles sont confiées des tâches administratives. Pour des raisons pratiques toutefois, il n'est pas possible d'établir dans la loi une liste des organisations concernées. Une telle liste serait trop rigide et inappropriée aux circonstances, compte tenu des changements

rapides qui peuvent intervenir dans ce domaine. C'est pourquoi nous proposons de renoncer à énumérer ces organisations dans la présente loi et d'introduire une délégation en faveur du Conseil fédéral (voir l'al. 2).

L'expression "dans un cas particulier" exprime l'idée que les autorités et organisations tenues de renseigner ne sont pas obligées de fournir des renseignements de manière périodique, quasi automatique ou standardisée. Il s'agit, au contraire, d'un devoir de renseigner dans un cas concret et sur la base d'une demande précise que leur adresse l'office fédéral ou les organes de sûreté cantonaux agissant pour son compte.

Le destinataire des renseignements obtenus auprès des différentes autorités et organisations est l'office fédéral. Toutefois, conformément au système adopté pour l'ensemble de la loi (cf. art. 7, al. 1, 13, al. 1, 14, al. 1), les autorités désignées par les cantons pour accomplir les tâches de sûreté, en d'autres termes les organes de sûreté des cantons, peuvent agir pour le compte de la Confédération et récolter directement les renseignements auprès des autorités et organisations tenues de renseigner, puis les transmettre à l'office fédéral. S'il surgit un différend au sujet d'une obligation de renseigner, celui-ci opposera cette autorité ou cette organisation à l'office fédéral et non à l'autorité cantonale qui aura recueilli le renseignement pour le compte de la Confédération (cf. aussi art. 13b).

La sécurité des experts du Pool d'experts suisse pour la promotion civile de la paix et des collaborateurs mis à la disposition d'organisations humanitaires ou œuvrant pour les droits de l'homme doit être garantie pendant les missions qu'ils effectuent à l'étranger. Il faut aussi tenir compte de façon appropriée des éventuelles clauses de confidentialité, des codes de conduite et des procédures d'opération permanentes. Les circonstances liées à chaque cas sont déterminantes.

Al. 2
Pour des raisons évidentes liées à la primauté du droit, il n'appartient pas aux organes de sûreté de déterminer eux-mêmes quelles organisations sont tenues par un devoir de renseigner. Il incombe par conséquent au Conseil fédéral de désigner chacune des organisations tenues de renseigner par voie d'ordonnance.

Al. 3
Les services mentionnés aux al. 1 et 2 sont aussi autorisés à communiquer spontanément aux autorités chargées de la protection de l'Etat de la Confédération et des cantons les faits pour lesquels ils supposent qu'ils pourraient être liés au terrorisme, au service de renseignements politiques ou militaires prohibé, au commerce illicite d'armes et de substances radioactives, et au transfert illégal de technologie. Les services mentionnés aux al. 1 et 2 sont ainsi libérés de toute accusation de violation du secret de fonction. Pour reprendre l'exemple cité précédemment, cette disposition permettra au MROS (voir commentaires de l'al. 1) de communiquer spontanément des informations aux organes de sûreté. Cela dit, il n'existe aucun devoir de fournir systématiquement des renseignements.

Intérêt public et proportionnalité
Comme nous l'avons déjà dit précédemment, l'art. 13a entend transposer définitivement dans la loi la règle de l'art. 13, al. 3, qui permet au Conseil fédéral d'étendre, "pour une période limitée", le devoir de renseigner à d'autres autorités que

celles qui sont énumérées à l'art. 13, al. 1. Le Conseil fédéral a fait usage de cette faculté en édictant l'ordonnance du 7 novembre 2001 concernant l'extension du devoir de renseigner et du droit de communiquer d'autorités, d'offices et d'organisations visant à garantir la sécurité intérieure et extérieure. Or la durée de validité de cette ordonnance, qui a déjà été prolongée deux fois, arrivera à échéance le 31 décembre 2008 (cf. RO 2005 5423).

Depuis l'adoption de cette ordonnance, la situation de la Suisse sous l'angle de la menace terroriste n'a pas fondamentalement changé. Selon l'appréciation actuelle, notre pays ne représente pas une cible directe et première du terrorisme. Cependant, la menace générale d'attentats terroristes demeure élevée au niveau international, et la Suisse est aussi concernée par cette menace, tout comme d'autres pays. Par ailleurs, les terroristes n'utilisent plus le bassin méditerranéen et l'Europe continentale uniquement comme base arrière. En tout état de cause, les organisations terroristes seraient prêtes à viser des intérêts occidentaux si l'occasion se présentait. Cette situation devrait perdurer; il n'est pas possible d'estimer, pour l'heure, quand la menace terroriste prendra fin.

En décembre 2002, le Conseil fédéral a chargé le DFJP d'examiner l'efficacité de l'ordonnance concernant l'extension du devoir de renseigner et du droit de communiquer d'autorités, d'offices et d'organisations visant à garantir la sécurité intérieure et extérieure et de lui présenter un rapport. Une enquête a été menée auprès des corps de police des cantons et des villes de Berne et de Zurich. Son objectif principal n'était pas de juger du nombre de renseignements fournis en termes de quantité, mais d'évaluer le contenu des communications en termes de qualité (la qualité est plus importante que la quantité).

Lors de l'évaluation de l'ordonnance, il a été décidé de signaler par une marque spéciale dans ISIS les communications liées aux nouvelles compétences. Cette mesure s'est toutefois révélée (beaucoup) trop coûteuse, et a dû être abandonnée. Par ailleurs, on a remarqué que par le simple fait de marquer les communications, l'impact de ladite ordonnance au niveau cantonal n'avait pas du tout été enregistré, ou l'avait été de manière insuffisante. Notamment dans les cas où les compétences élargies conférées par l'ordonnance permettaient de résoudre les communications plus facilement au niveau cantonal, sans faire de communication spéciale au SAP.

L'évaluation a en outre montré que l'ordonnance était bien connue de la police, mais insuffisamment des personnes autorisées à fournir des renseignements ou de celles tenues de le faire. Afin de parer à cette lacune, une circulaire d'information a été diffusée à large échelle à l'occasion de la dernière prolongation de l'ordonnance.

D'une manière générale, le nombre de communications est faible, mais la qualité de leurs contenus s'est largement améliorée. A ce jour, l'existence même de cette ordonnance et le devoir qui en découle suffisent en soi, même s'ils sont jugés plus importants que leur finalité pratique. Cela dit, les organes d'exécution cantonaux ont rejeté catégoriquement l'abrogation de cette disposition. En effet, la simple existence de l'ordonnance est essentielle à leurs yeux, bien que ses effets concrets ne puissent être établis de manière détaillée, car seul un nombre très limité de communications relèvent exclusivement des compétences élargies. En revanche, les coûts engendrés par l'ordonnance sont faibles.

En résumé, la portée de l'ordonnance s'est révélée non négligeable tant sur le plan de la politique intérieure qu'extérieure (politique intérieure: volonté du Conseil fédéral de lutter contre le terrorisme; politique extérieure: signal de la Suisse qu'elle est prête à assumer son rôle dans la communauté internationale pour lutter contre le terrorisme). En d'autres termes, sa prolongation ou sa reprise dans le droit "ordinaire" constitue un intérêt public prépondérant.

La mesure peut être qualifiée de proportionnée car le nombre de communications est faible, mais d'une qualité élevée.

2.8 Art. 13b Différends relatifs au devoir de renseigner

L'art. 13b s'applique lorsque l'office fédéral ou un organe cantonal de sûreté accomplissant des tâches sur son mandat demande la communication de renseignements sur la base des art. 13 ou 13a et que le destinataire de la demande s'y oppose.

Al. 1
Si ce différend implique uniquement des autorités de l'administration fédérale centrale (cf. art. 7 OLOGA, RS 172.010.1), il appartient à l'autorité commune de surveillance, c'est-à-dire au chef du département de tutelle ou au Conseil fédéral, de le trancher (cf. art. 9, al. 3, de la loi fédérale sur la procédure administrative, RS 172.021). Par exemple, un différend relatif à une demande de renseignements adressée par l'Office fédéral de la police à l'Office fédéral des migrations sera tranché par le chef du Département fédéral de justice et police.

Al. 2
Dans tous les autres cas où l'autorité appelée à fournir des renseignements ne donne pas suite à la demande, l'office fédéral peut, s'il ne parvient pas à un accord avec cette autorité, déférer le différend au Tribunal administratif fédéral par la voie de l'action en lui demandant d'obliger l'organe intimé à fournir l'information requise. Le Tribunal administratif fédéral rend alors une décision qui est définitive (cf. art. 83, let. a, de la loi du 17 juin 2005 sur le Tribunal administratif fédéral[3]). La voie de l'action est ouverte à l'office fédéral non seulement lorsque c'est lui qui a requis les renseignements, mais aussi lorsque la demande a été présentée par un organe de sûreté d'un canton. En effet, les organes de sûreté des cantons agissent dans ce domaine sur mandat de l'office fédéral. Il est donc juste qu'en cas de différend la compétence de déférer le litige au Tribunal administratif fédéral soit réservée à l'office fédéral.

L'action au Tribunal administratif fédéral se substitue à la voie de la plainte au Tribunal pénal fédéral (voir l'actuel art. 13, al. 4, LMSI), car les autres litiges en matière d'application de la LMSI relèveront de la compétence du Tribunal administratif fédéral (voir l'art. 29a nouveau).

Les différends susceptibles d'une action peuvent impliquer des autorités ou unités administratives cantonales, des organisations accomplissant des tâches de service public ou des organes de la Confédération qui ne relèvent pas de l'administration centrale, tels que le Ministère public de la Confédération (art. 8 OLOGA).

[3] FF 2005 3875. Cette loi entrera vraisemblablement en vigueur le 1er janvier 2007.

2.9 Art. 13c Devoir de renseigner incombant aux transporteurs commerciaux

Cette disposition introduit un devoir de renseigner, comparable à celui prévu à l'art.13a, mais qui vise non pas des autorités ou des organisations accomplissant des tâches de service public, mais des entreprises commerciales fournissant des prestations dans le domaine des transports. Comme celui de l'art. 13a, ce nouveau devoir de renseigner incombant aux transporteurs commerciaux ne porte que sur certains types de menaces (terrorisme, service de renseignements politiques ou militaires prohibés, commerce illicite d'armes et de substances radioactives, transfert illégal de technologie).

Sont visés les transporteurs privés, tels que les entreprises de taxi, les compagnies aériennes, les entreprises de location de véhicules, les entreprises de chemins de fer privés, les transporteurs routiers, etc.

Quant aux types de données qui doivent être fournies sur demande, il s'agit de celles que les transporteurs recueillent déjà maintenant pour leurs propres besoins. En d'autres termes, cette disposition n'introduit pas l'obligation pour eux de recueillir des donnés supplémentaires. La fourniture de ces données existantes n'impliquant pas d'efforts particuliers pour le transporteur, la loi ne prévoit pas l'obligation, pour les organes de sûreté, d'indemniser le transporteur pour des frais éventuels.

Enfin l'expression "dans un cas particulier" signifie, ici encore, que le transporteur n'est tenu de fournir un renseignement que dans un cas concret et sur la base d'une demande précise que lui adressent l'office fédéral ou les organes de sûreté cantonaux agissant pour son compte ; voir déjà le commentaire de l'art. 13a, al.1.

Intérêt public et proportionnalité
Conformément à l'art. 14, al. 2, let. b, LMSI, les organes de sûreté peuvent demander des renseignements pour exécuter leurs tâches. S'ils s'adressent pour cela à des particuliers (des personnes physiques ou morales), ils sont souvent confrontés à des refus de fournir les renseignements requis, les particuliers invoquant alors la législation sur la protection des données. Pour surmonter cet obstacle, nous proposons d'introduire un devoir de renseigner visant les transporteurs commerciaux. Ce devoir de renseigner constitue, d'une part, une intrusion dans la sphère professionnelle du transporteur et, d'autre part, une atteinte à la sphère privée de la personne qui est ainsi observée. Il s'agit donc de voir si cette atteinte est proportionnée aux intérêts publics qui sont en jeu. A cet égard, il faut relever que, pour les organes de sûreté, l'accès à des informations que peuvent détenir les transporteurs revêt souvent un caractère déterminant pour prendre la mesure d'une menace potentielle et déceler son degré de vraisemblance: par exemple, l'identification des déplacements de certaines personnes ou de certains biens, l'observation de la fréquence de tels déplacements, la mise en relation de certains déplacements sont autant d'informations qui permettent aux organes de sûreté de vérifier ou d'infirmer certains indices concrets qu'ils possèdent déjà. On ne saurait donc nier que l'accès à ce type d'informations constitue une mesure adéquate et nécessaire à l'accomplissement des tâches de prévention de l'office fédéral.

Quant au caractère proportionné de l'atteinte, même s'il est difficile à établir de manière abstraite, nous considérons que les éléments suivants doivent être pris en considération: en ce qui concerne le transporteur, on peut admettre, dès lors qu'il

n'est pas tenu de collaborer activement à la récolte d'informations et que son rôle se limite à fournir des renseignements dont il a de toute façon connaissance, que le devoir qui lui incombe ne porte pas, a priori, atteinte de manière disproportionnée à sa sphère professionnelle; ne tombant, par ailleurs, pas sous le coup d'un secret professionnel particulièrement protégé, il est en droit d'admettre que ses clients n'ont pas non plus une grande attente quant à l'intensité de la relation de confiance qui s'établit dans le cadre de ce contrat de transport.

En ce qui concerne la personne observée, dans la mesure où les données récoltées résultent d'une observation dans un lieu quasi public, on peut admettre que l'atteinte portée à sa sphère privée n'est pas disproportionnée au regard de l'intérêt public majeur qu'il s'agit de protéger. Mais il est clair que c'est dans le cas concret que la pesée entre l'intérêt public à protéger et l'intérêt privé à sauvegarder prendra tout son sens et qu'il sera réellement possible de déterminer lequel des deux l'emporte.

2.10 Art. 13d Secret professionnel

Certaines professions ne peuvent être exercées correctement et parfaitement si le public n'a pas la garantie absolue que les professionnels sont soumis au secret professionnel (ATF 84 IV 108). Cette condition est doublement garantie: premièrement par le fait que toute violation du secret professionnel est punissable (p. ex. art. 321 CP, RS 311.0; art. 35 LPD, RS 235.1) et, deuxièmement, par le droit de refuser de fournir aux autorités les renseignements soumis au secret professionnel. Cette norme vise ainsi à protéger une relation de confiance particulière, relation qui ne doit pas être respectée uniquement dans les procédures judiciaires, mais aussi et toujours lorsque des particuliers sont tenus de fournir des renseignements à des autorités. Cette disposition prévoit ainsi que les personnes tenues au secret professionnel recevant une demande de renseignements de l'office fédéral disposent du même droit de refus que dans le cadre d'une procédure pénale menée par la Confédération. En revanche, les obligations de garder le secret découlant uniquement d'un contrat ne sauraient tomber sous le coup du droit de refuser de fournir des renseignements, même lorsque ces obligations se fondent matériellement sur l'activité professionnelle de la personne tenue de garder le secret.

2.11 Art. 14, al. 3

L'art. 14 LMSI énumère exhaustivement les moyens auxquels peuvent actuellement recourir les organes de sûreté pour accomplir leurs tâches. Il s'agit de moyens qui ne portent pas d'atteinte grave aux droits fondamentaux. Ces moyens gardent toute leur importance et doivent rester les instruments ordinaires des organes de sûreté, le recours aux moyens spéciaux pour la recherche d'informations du chapitre 3a étant réservé à des circonstances particulières et ne pouvant être employés qu'à titre subsidiaire.

Al. 3
Dans le droit actuel, cette disposition est déterminante car c'est elle qui pose l'interdiction générale, pour les organes de sûreté, de recourir à des mesures de contrainte et à l'observation de faits dans des locaux privés. Or la présente révision introduit, à certaines conditions précises, l'usage de mesures de contrainte dénommées désormais moyens spéciaux de recherche d'informations. On passe donc d'un système d'interdiction générale à un système d'"autorisation", ce qui

implique l'abrogation de l'al. 3, bien qu'il ne s'agisse pas de moyens de contrainte au sens de la procédure pénale, mais de moyens spéciaux de recherche d'informations relevant des services de renseignements.

Le recours aux moyens spéciaux de recherche d'informations n'est possible que si les conditions définies aux art. 18a et suivants sont remplies. Plus concrètement cela signifie, en particulier, que des moyens spéciaux ne pourront être utilisés que dans les domaines pour lesquels ils sont prévus, à savoir le terrorisme violent, le service de renseignements politiques ou militaires prohibé, le commerce illicite d'armes et de substances radioactives ou le transfert illégal de technologie, mais qu'en revanche ils ne pourront pas être employés pour déceler ou prévenir des menaces liées à l'extrémisme violent ou au renseignement économique prohibé (cf. commentaire de l'art. 13, al. 3). Ils ne pourront pas davantage être utilisés si la menace ne revêt pas un caractère suffisamment grave, si les soupçons ne sont pas suffisamment concrets ou s'ils reposent sur des faits insuffisamment précis ou trop anciens.

2.12 Article 14a Exploration radio

Les organes de sûreté de la Confédération explorent depuis des décennies les rayonnements de signaux des services de renseignements étrangers pouvant être liés à des activités d'espionnage contre la Suisse. Ces rayonnements continuent d'être émis principalement en ondes courtes et ne disposent pas de moyens spéciaux les protégeant d'une réception par des tiers (cf. à ce sujet le rapport sur la protection de l'Etat 2000, p. 149 s). Au moment de la rédaction de la LMSI, cette activité d'exploration a été codifiée dans la disposition relative à la recherche d'informations dans le cadre de l'observation de faits dans des lieux publics et librement accessibles (art. 14, al. 2, let. f, LMSI).

Au cours des dernières années, le DDPS a développé, dans le cadre du projet ONYX, les capacités d'exploration des télécommunications transmises par satellites au niveau international, en répertoriant et en analysant les rayonnements des satellites sur la terre. Ceux-ci sont normalement aussi répertoriés et transmis par les prestataires de télécommunications. Depuis avril 2001, le SAP utilise aussi le système ONYX dans le cadre d'un test. Une base légale a été créée à cet effet à l'art. 9a OMSI. Cette disposition doit être transférée dans la LMSI dans le cadre de la présente révision. Ce transfert permettra de répondre à une demande de la Délégation des commissions de gestion, qui réclame expressément une base légale pour l'utilisation d'ONYX. La loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM; RS 510.10) est parallèlement modifiée pour permettre aux services de renseignements du DDPS d'utiliser ONYX (cf. modification du droit en vigueur, ch. 3, art. 99, al. 1 et 1^{bis} et art. 99a, LAAM).

Le nouvel article 14a correspond largement à la réglementation actuelle de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI; RS 120.2). Il a été complété pour permettre l'éventuelle surveillance de cibles en Suisse, qui est autorisée sous réserve des conditions et de la procédure prévues aux nouveaux art. 18d ss. Il serait en effet contradictoire qu'une personne dont les raccordements de télécommunication peuvent être surveillés en Suisse ne puisse pas en même temps faire l'objet d'une exploration de signaux.

Al. 1
Cet alinéa pose, d'une part, le principe selon lequel l'Office fédéral de la police peut recourir à l'exploration radio pratiquée sur des cibles situées à l'étranger et définit, d'autre part, ce qu'il faut entendre par "exploration radio". La définition inclut toutes les sortes de rayonnements électromagnétiques émanant de l'étranger. Compte tenu de l'évolution extrêmement rapide des techniques de télécommunication dans l'ensemble de ce domaine, il ne serait pas judicieux, tant sur le plan matériel que juridique, de limiter l'exploration à des applications techniques précises, telles que les ondes courtes ou ONYX.

Al. 2
La première phrase porte sur la recherche d'informations techniques concernant des rayonnements émanant de la Suisse, p. ex. les fréquences utilisées, les puissances ou les périodes d'émission, c'est-à-dire sur des données qui ne sont pas protégées par le secret des télécommunications au sens de l'art. 13, al. 1, Cst. et de la législation d'exécution. En revanche, si l'exploration radio sert à surveiller des communications qui sont protégées par ce secret (cf. communications établies avec un portable), l'al. 2, phrase 2, rappelle, à des fins de clarté et de transparence, que cette exploration constitue un moyen spécial au même titre que la surveillance de la correspondance par poste ou télécommunication. Dès lors c'est la procédure du chapitre 3a qui s'applique (cf. art. 18a et suivants, en particulier art. 18k). Ainsi, les cas dans lesquels l'appui technique de prestataires de télécommunications n'est pas exigé pour exécuter la surveillance sont aussi clairement soumis aux réglementations plus strictes.

Al. 3
Cette disposition, qui autorise l'office fédéral à collaborer avec d'autres instances *fédérales ou cantonales* pour procéder à l'exploration de signaux, consacre la pratique actuelle. L'Office fédéral de la police n'exploite que dans une moindre mesure des installations qui lui sont propres pour capter des ondes de signaux courtes et charge généralement la Division de la conduite de la guerre électronique du DDPS de rechercher des informations précises. En revanche, en vertu de cette disposition, un raccordement à un système étranger de exploration radio (p. ex. à "ECHELON") n'est toujours pas possible.

Al. 4
Cet alinéa garantit que les instruments de contrôle prévus aux art. 99 ss LAAM sont toujours appliqués dans le domaine de l'exploration radio permanente (cf. modification du droit en vigueur, ch. 3 LAAM, notamment l'art. 99a). Afin d'éviter les disparités au profit des services de renseignements du DDPS, qui pratiquent l'exploration radio dans une mesure bien plus large, le contrôle de l'exploration des cibles situées exclusivement à l'étranger doit continuer d'être effectué par la même autorité de contrôle indépendante (ACI). En ce qui concerne les éventuelles cibles sises en Suisse, la procédure visée aux art. 18d et 18e (cf. ci-après) doit toutefois être appliquée, dans la mesure où l'exploration de signaux porte sur des communications protégées par le secret des télécommunications.

Intérêt public et proportionnalité
L'exploration radio constitue un moyen de recherche d'informations à partir de sources publiques. En ce sens, elle ne porte pas une atteinte importante à la sphère

privée, notamment au secret des télécommunications. Si, en revanche, l'exploration de signaux porte sur des communications protégées par le secret des télécommunications, elle porte une atteinte grave et est alors soumise au régime de la recherche spéciale d'informations, notamment à celui de la surveillance de la correspondance par poste et télécommunication, réglée à l'art. 18k. Nous renvoyons donc au commentaire relatif à cet article.

2.13 Art. 14b Informateurs

Pour accomplir leurs tâches, les organes de sûreté dépendent des communications de personnes qui ont accès aux informations pertinentes. Conformément au principe de la légalité consacré dans la nouvelle Constitution fédérale, les dispositions importantes qui fixent des règles de droit doivent figurer dans la loi formelle (cf. art. 164, al. 1, Cst.). Or la LMSI ne contient aucune règle relative au recours à des informateurs, à leurs droits, à leurs obligations, ainsi qu'aux prestations que l'Etat leur accorde, alors même que le principe du recours à leurs services y est implicitement admis (cf. en particulier l'art. 14, al. 2, let. b et d). Il s'agit donc de combler cette lacune.

Al. 1
Cet alinéa, d'une part, autorise expressément l'office fédéral à recourir à des informateurs et, d'autre part, définit ce qu'est un informateur. L'informateur est une personne qui décide, quasi unilatéralement, de collaborer avec les organes de sûreté sans qu'il s'établisse pour autant un rapport de travail au sens de l'art. 319 du code des obligations (CO; RS 220). Le fait qu'un informateur puisse occasionnellement percevoir une prime ou qu'il soit indemnisé de ses frais (cf. al. 2) ne suffit en soi pas à transformer ce rapport en un rapport de travail. Il faudrait réunir, pour cela, d'autres éléments caractéristiques, tels que l'existence d'un rapport de subordination juridique qui placerait l'informateur dans la dépendance de l'office fédéral sous l'angle personnel, organisationnel et temporel, ce qui n'est absolument pas le cas dans la pratique.

Al. 2
Afin qu'ils ne subissent pas de pertes financières, les dépenses des informateurs qui fournissent plus ou moins régulièrement des informations aux organes de sûreté de l'Etat leur sont remboursées. Ces dédommagements ne représentent pas un revenu ou un salaire imposable au sens de la législation sur l'AVS. Il s'agit des frais découlant des activités menées par les informateurs.

Par ailleurs, les informateurs peuvent recevoir une prime dans certains cas, lorsqu'ils ont transmis des informations particulièrement importantes. Conformément à la pratique courante, ces primes ne dépassent pas quelques milliers de francs par an et sont loin de constituer un revenu permettant de subvenir aux besoins d'une personne. Ainsi, l'incitation financière ne doit pas être déterminante pour les informateurs afin qu'ils ne se sentent pas faussement obligés d'agir. Les primes sont accordées lorsque la personne peut donner des informations qui facilitent largement les recherches d'informations ultérieures ou l'établissement de l'appréciation de la menace.

Al. 3
La relation entre les organes de sûreté et les informateurs se fonde sur la confiance réciproque et sur la confidentialité de l'existence de cette relation envers des tiers. Les informateurs peuvent être exposés à de grands risques dans leurs activités liées à la protection de l'Etat, lorsque les personnes cibles ont connaissance qu'ils travaillent pour le compte des organes de sûreté. Ils ne peuvent donc ni figurer dans les dossiers concernant le personnel de l'office, ni être inscrits aux assurances sociales, même s'il ne s'agit que de constater qu'ils sont libérés de l'assurance obligatoire. En revanche, le DFJP et la Délégation des commissions de gestion, qui est l'organe de contrôle ordinaire de la LMSI, contrôlent aujourd'hui déjà la légalité et l'opportunité de leur engagement. L'al. 3 précise que les éventuelles indemnisations ne sont pas imposables, dans la mesure où cette non-imposition est nécessaire pour garantir la protection des sources ou d'autres recherches d'informations. Ceci n'affecte ni l'informateur concerné ni la collectivité au vu des modestes sommes en jeu.

2.14 Art. 14c Protection des informateurs

Le but de ces mesures est de protéger les personnes qui prennent des risques en vue de rechercher des informations aux fins de la LMSI. On distingue notamment deux groupes de personnes: d'une part celles qui coopèrent d'elles-mêmes avec les organes de sûreté et qui doivent être protégées en raison des représailles auxquelles elles pourraient être exposées; d'autre part celles qui sont prêtes à déposer, et qui doivent jouir d'une protection adéquate facilitant cette coopération et leur permettant de collaborer avec les autorités. Grâce à ces mesures, la Suisse évite - comme cela s'est déjà produit à plusieurs reprises - que des informateurs particulièrement efficaces et prêts à déposer "passent" à des services de renseignements étrangers parce que ceux-ci peuvent garantir leur protection.

Les personnes qui collaborent d'elles-mêmes avec les organes de sûreté prennent dans certains cas d'énormes risques et peuvent craindre des représailles, soit de membres de leur entourage (p. ex. les informateurs appartenant à des groupes extrémistes violents en Suisse), soit d'Etats étrangers (p. ex. les informateurs qui se sont engagés seulement pour apparence mais qui travaillent en réalité pour les autorités suisses). La menace qui pèse sur ces personnes peut être comparée à celle à laquelle les agents infiltrés sont exposés, qui disposent d'une excellente protection. La mise en place d'une protection efficace pour les informateurs se justifie donc, pour ne pas dire qu'elle s'impose.

Les réglementations relatives à la protection de personnes se distinguent clairement de celle du "témoin de la Couronne", issue du code de procédure pénale anglo-saxon. Cette dernière prévoit que des personnes qui sont certes considérées comme coupables d'une infraction témoignent contre leurs complices en échange de la garantie qu'elles échapperont à une condamnation, obtiendront une réduction de peine ou d'autres avantages liés à la procédure. Dans son rapport intitulé "Unification de la procédure pénale", une commission d'experts de la Confédération est arrivée à la conclusion que l'introduction en Suisse de la réglementation du "témoin de la Couronne" n'était pas indiquée tant au niveau de la procédure pénale qu'au niveau préventif. En effet, l'idée d'une suppression de peine au sens de cette réglementation ne fait pas l'objet de débats dans notre pays. Au niveau préventif, l'accent n'est pas mis sur la recherche d'infractions, qui devrait être facilitée grâce à certaines

déclarations de témoins, mais sur l'obtention d'informations importantes pour la sûreté. Ces informations permettront d'identifier et d'écarter des menaces et, peut-être, d'éviter des délits.

Par ailleurs, les mesures prévues ne devraient être mises en œuvre que dans les rares cas où les informations fournies par un informateur pourraient se révéler précieuses. Pensons à la protection des personnes qui peuvent communiquer des informations importantes permettant d'écarter des dangers élevés en matière de sûreté. Il pourrait s'agir d'informations concernant la planification ou la préparation d'attentats terroristes, des actes concrets d'espionnage commis au détriment de la Suisse, ou des réseaux visant à acquérir des armes de destruction massive en se servant de la Suisse. Afin de minimiser les risques liés à la collaboration de ces personnes, les premiers contacts seraient par exemple suivis de discussions approfondies et une convention de protection serait négociée sous réserve de certaines conditions, impliquant des droits et des obligations réciproques. La coopération se fonderait ensuite sur cette base.

Al. 1
Cet alinéa pose le principe de l'octroi d'une protection aux informateurs et fixe exhaustivement le type de mesures que l'office est tenu de prendre pour protéger leur vie ou leur intégrité corporelle: par protection rapprochée, nous pensons à des mesures telles que le recours à des gardes du corps ou à la protection physique de lieux, de véhicules ou d'appareils déterminés; par éloignement géographique, nous pensons, après accord de la personne concernée, à un déplacement en des lieux plus sûrs, en Suisse ou à l'étranger. Offrir des mesures de protection adaptées à une personne déplacée à l'étranger signifie que cette personne, en raison du contexte général, ne peut disposer de telles mesures en Suisse. Afin de compenser les frais que cela implique, et éventuellement une perte de gains, la mesure en question doit être assortie d'un soutien financier limité dans le temps.

L'office fédéral peut soit prendre lui-même certaines de ces mesures, soit les financer. A cet égard, il faut relever que, dans la pratique, peu de mesures pourront être réalisées en Suisse même. En effet, en raison de la taille de notre pays, il ne serait guère possible, en présence de certaines menaces, de déployer des mesures de protection complète. Il conviendrait donc d'acheter à l'étranger des programmes de protection, ce qui permettrait aussi de prévoir les coûts. Des formes de protection partielle pourraient aussi être envisagées, par exemple celle consistant à garantir à l'informateur qu'il obtiendra un permis de séjour (en Suisse ou dans un Etat tiers ami), ce que la seconde phrase de l'al. 1 prévoit expressément.

Al. 2
Pour des raisons analogues à celles énoncées précédemment, l'office fédéral doit aussi pouvoir prendre des mesures de protection en faveur des proches des informateurs, lorsque leur sécurité en dépend. La disposition, qui est ici potestative, laisse une certaine marge de manœuvre à l'office pour apprécier les circonstances du cas d'espèce.

Al. 3
Cette disposition prévoit une mesure de protection qui, à la différence des mesures des al. 1 et 2, ne peut être prise qu'au moment où l'office *met un terme* à ses

contacts avec l'informateur et renonce totalement à utiliser cette source. Dans la mesure où la sécurité de l'informateur est gravement menacée en raison du rôle qu'il a joué dans une affaire pour le compte de l'office fédéral, celui-ci est autorisé à lui constituer une identité d'emprunt pour le protéger et, par conséquent, l'informateur est en droit de l'utiliser aux conditions que l'office fédéral fixe d'entente avec lui.
L'octroi d'une identité d'emprunt est soumise à deux conditions préalables: un avis positif du Tribunal administratif fédéral et l'autorisation du chef du département (voir ci-après).

En revanche, cette disposition ne couvre pas le cas du recours à une identité d'emprunt destiné à assurer une recherche d'informations, lequel constitue un moyen spécial qui ne peut être employé que si les conditions, la procédure et les modalités fixées pour la recherche spéciale d'informations sont respectées ; voir ci-après, sur cette autre hypothèse, l'art. 14d.

Ajoutons que, conformément à l'art. 27, al. 1bis, le département doit rendre compte régulièrement au Conseil fédéral et à l'organe de contrôle parlementaire du nombre d'identités d'emprunt constituées, de celles utilisées et de leur finalité respective. Il en va de même des identités d'emprunt prévues à l'al. 3.

Al. 4
Cet alinéa fixe le principe selon lequel les mesures de protection sont limitées dans le temps. Cette durée n'est pas déterminable abstraitement dans la loi. A titre exceptionnel, le chef du département peut renoncer à une telle limitation, si les risques encourus sont particulièrement graves et qu'il y ait tout lieu de les tenir pour permanents.

2.15 Art. 14d Identités d'emprunt

Les services de renseignements doivent avoir recours à des identités d'emprunt pour accomplir leurs tâches et protéger leurs collaborateurs lors de la recherche d'informations dans des milieux précis. La constitution d'une identité d'emprunt doit se faire sur le long terme et ne peut que rarement être attribuée seulement au moment où un cas précis survient. Pour cette raison, la réglementation sur les identités d'emprunt ne figure pas sous le chapitre consacré aux moyens spéciaux de recherche d'informations, laquelle est soumise à des conditions très strictes. Depuis 1998, le Service de renseignement stratégique a la possibilité de constituer des identités d'emprunt pour ses agents dans leurs contacts avec l'étranger, en s'appuyant sur l'art. 99 LAAM (cf. Rapport annuel 2002/2003 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, du 23 janvier 2004; FF 2004 1594).

Il appartiendra donc au chef du département de décider de l'octroi de telles identités d'emprunt. Auparavant, le Tribunal administratif fédéral prévu (art. 18d) devra vérifier si la mesure est conforme au droit, c'est-à-dire si les conditions légales de cet octroi sont réunies. Le chef du département pourra ensuite évaluer la décision sur le plan politique et, si opportun, donner son accord.

Dans certains secteurs, il serait en théorie possible de trouver à la fois des personnes actives dans les domaines relevant de la LMSI, des collaborateurs du Service de renseignement stratégique et des agents infiltrés des polices judiciaires

de la Confédération ou des cantons, ces derniers opérant conformément à la loi fédérale du 20 juin 2003 sur l'investigation secrète (LFIS; RS 312.8). Au sein de l'Office fédéral de la police, ce problème peut être résolu grâce au pouvoir de surveillance de la direction. Les conflits pouvant survenir avec le Service de renseignement stratégique lorsque celui-ci a recours à des identités d'emprunt en Suisse doivent être évités conformément à la décision du Conseil fédéral du 22 juin 2005 de coordination entre le Service d'analyse et de prévention et le Service de renseignement stratégique.

Al. 1
Cette disposition pose le principe de l'octroi d'une identité d'emprunt à des fins de recherche d'informations et de sécurité. Relevons d'abord que les identités d'emprunt sont généralement utilisées dans le cadre de la recherche générale d'informations, à savoir pour les mesures visées à l'art. 14, al. 2, LMSI. En revanche, lorsque des mesures précises impliquant des moyens spéciaux de recherche d'informations doivent être déployées, qui nécessitent l'utilisation d'une identité d'emprunt (p. ex. pour une observation dans des lieux non accessibles au public, avec identité d'emprunt), la procédure de moyens spéciaux de la recherche d'informations prévue aux art. 18a ss est applicable. Par ailleurs, l'al. 1 détermine exhaustivement le cercle des personnes qui peuvent être dotées d'une identité d'emprunt:

Let. a et b
Les organes de sûreté visés par la LMSI sont étroitement liés aux forces de police suisses et peuvent mener ouvertement la majorité de leurs recherches au nom de la police. Pour établir des contacts avec des organisations, notamment dans le domaine du terrorisme ou du service de renseignements prohibé, il est toutefois nécessaire de pouvoir recourir à une identité d'emprunt. De telles mesures visent aussi et surtout à protéger les collaborateurs des organes de sûreté et leurs familles.

Let. c
Les tiers (informateurs) doivent aussi pouvoir être dotés d'une identité d'emprunt si cela est indispensable pour la recherche de renseignements. Pensons notamment aux personnes engagées par l'Office fédéral de la police dans une opération déterminée, pour lesquelles l'identité d'emprunt est le seul moyen de s'infiltrer plus facilement dans certains milieux importants pour la protection de l'Etat, et qui ont besoin de cette identité d'emprunt pour leur protection. Bien que les informateurs soient placés sous la direction des officiers traitants des organes de sûreté pour leurs recherches d'informations, ils ne sont pas directement sous la surveillance des organes de sûreté. La constitution d'identités d'emprunt pour les informateurs doit donc être limitée dans le temps et l'espace; elle n'est en outre possible que dans le contexte d'une opération bien précise.

Relevons enfin que la constitution d'une identité d'emprunt implique aussi le droit de créer des structures de couverture au nom desdites personnes. En effet, la personne dotée d'une telle identité possède la pleine personnalité juridique et peut donc s'engager contractuellement (location de locaux, de véhicules ou de raccordements de télécommunication, création de structures de couverture telles que des sociétés ou d'autres personnes morales).

Al. 2
Afin de mieux pouvoir contrôler les risques liés à l'usage d'une identité d'emprunt, nous proposons de limiter la durée de cet usage. Cette mesure est particulièrement nécessaire en ce qui concerne les identités d'emprunt octroyées à des informateurs, lesquels, n'étant pas des employés de l'office fédéral, échappent à son pouvoir disciplinaire.

Al. 3
L'al. 3 garantit que les identités d'emprunt ne sont utilisées que pour des raisons de service. Rappelons encore que, conformément à l'art. 27, al. 1^{bis}, let. a, du présent projet, la constitution et l'utilisation d'identités d'emprunt doivent faire l'objet d'un contrôle politique intense et ciblé, raison pour laquelle le département doit renseigner annuellement le Conseil fédéral et la Délégation des commissions de gestion à ce sujet.

2.16 Art. 15, al. 6

La disposition date de l'ancienne police fédérale, où la répression et la prévention n'étaient pas distinctes. La mise en œuvre de la séparation des aspects répressif et préventif rend cette disposition obsolète. Selon le droit et son interprétation actuels, lorsque des données utilisées à des fins de répression sont transférées à des fins de prévention, il s'opère un changement dans le but du traitement des données; les données ainsi transférées deviennent des données relevant de la prévention et doivent être traitées conformément au droit applicable dans le domaine de la prévention. L'abrogation ne signifie toutefois pas qu'il n'est plus possible d'échanger des données.

2.17 Art. 16, al. 3, 2^{e} phrase

Conformément à l'art. 16, al. 3, 2^{e} phrase, LMSI, les données traitées par les organes de sûreté des cantons en vertu de la présente loi sont soumises au droit fédéral sur la protection des données. Par ailleurs, la 2^{e} phrase stipule que les prérogatives de surveillance prévues par le droit cantonal sont réservées. En d'autres termes, le droit fédéral sur la protection des données est en principe applicable pour le traitement, par des organes cantonaux, de données issues des activités prévues dans la LMSI (relevant donc du droit fédéral). Lorsqu'il prévoit une surveillance spéciale, le droit cantonal prévaut cependant sur le droit fédéral, au sens d'une dérogation.

Dans la pratique, la réserve de la prérogative de surveillance des cantons s'est révélée problématique pour deux raisons: premièrement, une autorité de surveillance cantonale - par exemple une commission de gestion - peut demander l'accès à des dossiers opérationnels de la Confédération, même si les dossiers sont classifiés au niveau fédéral. Deuxièmement, la formulation de la disposition pourrait induire une (fausse) interprétation, selon laquelle les données collectées de manière "prétendument" indépendante par un canton dans le cadre d'un vaste mandat (p. ex. liste d'observation) sont considérées comme des données cantonales avant d'être transmises aux autorités fédérales. Dans les deux cas, des intérêts en termes de sûreté peuvent néanmoins justifier le rejet d'un droit de consultation. Dès lors, l'art. 16, al. 3, de la LMSI doit préciser que le Conseil fédéral sera désormais responsable de déterminer quels dossiers de la Confédération les autorités de contrôle

cantonales peuvent consulter. Le Conseil fédéral fixera donc l'étendue des prérogatives de surveillance des cantons; les intérêts légitimes des cantons pourront ainsi aussi être pris en considération.

2.18 Art. 17, al. 3, let. e et al. 7

Al. 3, let. e

Les clearings font partie des activités traditionnelles du SAP dans ses relations avec l'étranger. Ainsi, sur demande d'un service étranger, il effectue un contrôle de sécurité relatif à des Suisses ou à des étrangers qui ont un domicile fixe en Suisse, grâce auquel ces personnes peuvent ensuite collaborer à des projets étrangers classifiés (ou être engagés dans ces projets). Pour cela, l'Etat étranger requérant assure par écrit au SAP qu'il a obtenu l'accord de la personne concernée pour effectuer le clearing.

Le SAP s'est toujours fondé sur l'art. 17, al. 3, let c, LMSI pour effectuer les clearings. Cela dit, cette base juridique a été remise en cause par diverses instances par le passé. Il convient donc à présent de créer une base légale formelle pour le clearing. Cette étape est nécessaire car elle permet de prendre en compte les services de l'Office fédéral de la police qui effectuent les clearings dans le projet législatif de l'Office fédéral de la justice relatif à la nouvelle réglementation des droits d'accès de l'Office fédéral de la police à VOSTRA (banque de données pour les extraits du casier judiciaire). En effet, du point de vue du droit sur la protection des données, une base juridique claire doit figurer aux art. 359 ss CP pour que l'Office fédéral de la police ait accès à VOSTRA aux fins du clearing. La présente modification de la LMSI ne constitue donc qu'une base permettant d'établir, à l'avenir, une réglementation claire concernant l'accès aux données figurant dans le casier judiciaire. Les extraits du casier judiciaire représentent en effet un élément d'appréciation important pour l'opération de clearing. Sans ces extraits, les clearings effectués par le SAP pour l'étranger perdraient une grande partie de leur valeur, ce qui impliquerait aussi des effets négatifs pour la personne sur laquelle le clearing porte. Car même en cas d'appréciation positive, l'intéressé ne serait plus considéré comme une personne de confiance pour collaborer à l'étranger à des projets secrets ou confidentiels.

Al. 7

L'activité des services de renseignements se fonde essentiellement sur la recherche et la diffusion d'informations. Pour obtenir des informations, les services de renseignements ont recours à différents types de recherches, dont la "human intelligence", aussi appelée HUMINT. La notion de "human intelligence" signifie la recherche ou la fourniture d'informations sensibles par des personnes (sources humaines). Bon nombre d'informations importantes ne sont communiquées que si les autorités compétentes peuvent assurer que des tiers n'auront pas connaissance de la source d'une information (protection des sources).

Selon l'art. 17, al. 7, LMSI, la protection des sources doit dans tous les cas être assurée dans les relations avec *l'étranger*. S'agissant de la Suisse, l'art. 17, al. 1, LMSI indique que le Conseil fédéral désigne par voie d'ordonnance les destinataires accomplissant une tâche de service public en Suisse auxquels l'office fédéral peut, dans des cas particuliers, communiquer des données personnelles lorsque cela est nécessaire au maintien de la sûreté intérieure ou extérieure ou au contrôle de l'exécution des tâches dudit office fédéral. Dans notre pays, la question de la

protection des sources se pose donc, notamment dans les cas de transmission d'informations.

En vertu de l'art. 99, al. 4, LAAM, en vigueur depuis le 1er janvier 2004, les sources du Service de renseignement stratégique jouissent d'une protection absolue: "La protection des sources doit dans tous les cas être assurée."

Il faut dès lors se demander s'il se justifie de traiter différemment le problème de la protection des sources, selon qu'il s'agit du renseignement extérieur ou du renseignement intérieur. Or il y a des arguments qui plaident pour le maintien de la différence et d'autres pour une harmonisation dans le sens de la législation militaire. En faveur du statu quo, nous invoquerons les raisons mêmes qui ont conduit le législateur de 1997 à exclure la protection des sources sur le plan interne: il s'est refusé à consacrer une règle qui a pour conséquence que les autorités s'engagent, à l'égard de la personne qui leur livre une information, à ne jamais révéler l'origine de cette information, alors même que cette personne aurait commis une infraction pénale. Dans le message accompagnant le projet de loi, le Conseil fédéral écrivait: "... lorsque les sources proviennent du pays, il ne sera pas possible de prendre dans chaque cas un engagement strict à cet égard, notamment si l'informateur s'est rendu coupable d'une infraction. Par contre, une protection absolue des sources doit fonctionner vis-à-vis des services étrangers" (cf. FF 1994 II 1185).

En revanche, la protection absolue des sources pour le Service de renseignement stratégique prévue par la LAAM a fait ses preuves, ce qui parle en faveur d'une harmonisation. Elle répond d'une part aux besoins opérationnels des organes de sûreté et correspond à la ligne que le SAP a toujours suivie en matière de protection des sources. Compte tenu des expériences acquises dans le domaine du renseignement extérieur, nous sommes d'avis que l'argument opérationnel est, dans ce domaine très particulier qu'est le renseignement, déterminant. C'est pourquoi nous proposons d'abandonner la conception de la loi de 1997 et d'harmoniser le régime de la protection des sources de la LMSI sur celui de la législation militaire. Quant à la formulation, nous avons repris celle de l'art. 99, al. 4, LAAM.

Ajoutons enfin que la protection des sources implique aussi bien le maintien du secret en ce qui concerne la personne qui a révélé une information que celui du contenu de l'information révélée.

2.19 Chapitre 3a Recherche spéciale d'informations

Le chapitre 3a constitue l'une des principales innovations du projet de loi. Il doit permettre aux organes de sûreté d'employer à des fins de prévention des moyens de recherche, dénommés ici "moyens spéciaux".

Le titre du chapitre, "Recherche spéciale d'informations", traduit l'idée que la recherche dont il est question ici est celle qui emploie des moyens spéciaux. Elle se distingue de la "recherche générale d'informations", réglée dans le chapitre 3 et qui se pratique avec les moyens ordinaires qui y sont énumérés. Il y a donc synonymie entre une "recherche spéciale" et l' "emploi de moyens spéciaux". En revanche, l'expression "mesures de contrainte" ("Zwangsmassnahmen"), qu'on trouve dans la loi actuelle, ne nous paraît pas couvrir tous les moyens spéciaux prévus par le projet de loi. Elle disparaîtra d'ailleurs de la loi par l'abrogation de l'art. 14, al. 3.

Le chapitre 3a est divisé en deux sections. La première section contient des dispositions générales, par quoi on entend des dispositions applicables à l'ensemble des moyens spéciaux. La seconde section traite des différents moyens spéciaux.

2.20 Art. 18a Principe

Cette disposition pose le principe du recours à des moyens spéciaux de recherche d'informations, en définit les domaines et énumère les différents moyens. Ce faisant, elle pose le cadre général dans lequel s'inscrit une recherche spéciale d'informations.

Al. 1
Cet alinéa indique le but dans lequel les moyens spéciaux peuvent être employés. Ils peuvent l'être "pour déceler ou prévenir une menace concrète contre la sûreté intérieure ou extérieure". Mais la disposition, pour être comprise, doit être mise en relation avec la let. a de l'art. 18b. Il faut *qu'avant* d'utiliser des moyens spéciaux de recherche d'informations pour chercher à "déceler" ou à "prévenir" une menace, les organes de sûreté puissent déjà fonder des soupçons contre une personne, une organisation ou un groupement (ATF 109 Ia 273, 288-289: "die Ueberwachung darf nicht dazu dienen, einen Verdacht überhaupt erst zu begründen").

Les domaines de criminalité où les moyens spéciaux de recherche d'informations peuvent être employés sont: le terrorisme, le service de renseignements politiques ou militaires prohibé, le commerce illicite d'armes et de substances radioactives ainsi que le transfert illégal de technologie. Sur ces domaines, nous renvoyons au commentaire de l'art. 13a, al. 1, et notamment au terme "terrorisme" mentionné au ch. 1.2.1.

Al. 2
L'al. 2 annonce, par souci de clarté, les moyens spéciaux qui seront traités dans la seconde section. L'énumération est exhaustive. Nous renvoyons au commentaire relatif à ces différents moyens.

2.21 Art. 18b Conditions

L'emploi de moyens spéciaux de recherche d'informations est subordonné à la réunion de cinq conditions cumulatives.

Al. 1
Les quatre premières conditions sont de nature matérielle et doivent répondre aux exigences de l'art. 36 Cst. Elles ont pour objet de définir l'*intérêt public* qui, en l'espèce, peut seul justifier l'atteinte à des droits fondamentaux (let. a), ainsi que les divers aspects du principe de la *proportionnalité (let. b à d)*.

Pour l'intérêt public, il s'agit du maintien de la sûreté intérieure ou extérieure et de la protection de la sécurité de collaborateurs de l'office fédéral contre les personnes, organisations et groupements dont on soupçonne qu'ils les menacent (ci-après dénommés „perturbateurs présumés"; cf. let. a).

Pour le principe de la proportionnalité, il s'agit, dans la mesure où on peut les distinguer, des différents éléments qui le composent: l'adéquation (Geeignetheit) à la

let. d in initio, selon laquelle le moyen doit être propre à atteindre le but d'intérêt public ; la nécessité (Erforderlichkeit) à la let. c et à la let. d in fine, selon laquelle tout autre moyen non spécial serait inefficace; la proportionnalité au sens étroit (Verhältnismässigkeit i. e. S) à la let. b, selon laquelle l'intérêt public pèse plus lourd que l'atteinte subie par la personne concernée.

2.22 Art. 18c Surveillance de tiers et protection du secret professionnel

Cette disposition règle deux formes particulières de la surveillance: d'une part, celle de tierces personnes qui sont impliquées dans une surveillance sans que la recherche soit dirigée contre elles et, d'autre part, celle de personnes tenues au secret professionnel au sens de l'art. 321 CP et à l'égard desquelles certaines précautions particulières doivent être prises.

Al. 1
Cette disposition vise le cas d'une implication indirecte. Il arrive que le perturbateur présumé et qui, pour cette raison, fait l'objet d'une recherche impliquant des moyens spéciaux de recherche d'informations, utilise au service de son dessein, c'est-à-dire pour y poursuivre l'activité qui fait qu'on le suppose menaçant, des choses ou des lieux qui ne lui appartiennent pas, mais dont un tiers a la disposition, par exemple un appareil téléphonique, un local privé ou un système informatique. L'utilisation se fera parfois même à l'insu de ce tiers. Cet appareil ou ce local doit toutefois pouvoir être surveillé.

Le texte précise bien que ce n'est pas le tiers qui est surveillé pour lui-même, dans la mesure où il n'est supposé menaçant. C'est plutôt son "environnement" qui est surveillé.

Al. 2
Cette disposition ne se limite pas aux tiers. Elle vise toute implication, directe ou indirecte, d'une personne liée par un secret professionnel, d'un avocat par exemple, et se soucie de la protection de ce secret. Elle concerne donc aussi bien le tiers dont l'environnement est surveillé conformément à l'al. 1 que la personne qui fait elle-même l'objet d'une recherche d'informations impliquant des moyens spéciaux. Le texte est inspiré de l'art. 4, al. 6, de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT; RS 780.1). Conformément à la jurisprudence de la Cour européenne des droits de l'homme (arrêt Kopp c. Suisse, du 25 mars 1998), le tri doit être opéré sous la surveillance d'une autorité judiciaire. C'est pourquoi nous proposons qu'un juge du Tribunal administratif fédéral soit chargé de cette tâche (sur cette question, voir aussi le message du 1er juillet 1998 concernant les lois fédérales sur la surveillance de la correspondance postale et des télécommunications et sur l'investigation secrète, FF 1998 3689, 3714).

2.23 Art. 18d Tribunal administratif fédéral

L'emploi de moyens spéciaux de recherche d'informations ne porte pas seulement une atteinte aux droits fondamentaux, notamment au droit au respect de la vie privée garanti par l'art. 8 CEDH et par l'art. 13 Cst. Il a encore ceci de particulier qu'il est, par définition, pratiqué à l'insu de la personne qui en est l'objet et qui se trouve ainsi

dans l'impossibilité de se défendre pendant que le moyen est utilisé à son encontre. Il est donc nécessaire que la loi subordonne son emploi à des règles aussi précises qu'il est possible et que l'observation de ces règles soit strictement *contrôlée*.

Le contrôle s'exerce en général de deux manières, en des temps différents. Dans la mesure où l'emploi des moyens spéciaux de recherche d'informations doit être, après qu'il a eu lieu, porté à la connaissance de la personne touchée, celle-ci pourra recourir auprès d'un tribunal (contrôle a posteriori). Ce système de communication et de recours est prévu, dans le projet de loi, aux art. 18i et 29a.

Mais il ne suffit pas: d'une part, il est tardif car au moment de la communication, l'atteinte au droit fondamental a déjà été consommée ; d'autre part, il peut être incomplet, du fait que la loi permet, à certaines conditions, de renoncer provisoirement, voire durablement, à la communication (cf. art. 18i, al. 2). Ce contrôle a posteriori doit donc être complété par un contrôle a priori exercé au moment même où l'emploi du moyen spécial de recherche d'informations est demandé.

En procédure *répressive*, le double contrôle est normalement prescrit par la loi et assumé par une autorité judiciaire (procureur, juge d'instruction, juge du fond). Quand les moyens spéciaux sont employés à des fins de *prévention*, comme c'est le cas dans le présent projet, il n'y a aucune raison de faire l'économie du double contrôle. Dans l'arrêt de principe du 9 novembre 1983, le Tribunal fédéral l'a clairement dit: "Missbräuche können im präventiven Bereich noch weit mehr als bei der repressiven Überwachung schädliche Folgen für die freiheitliche, demokratische Ordnung haben" (ATF 109 I 295). La seule question qui se pose est alors de savoir si, dans une action *préventive*, le contrôle a priori doit être nécessairement réservé à une autorité judiciaire ou s'il peut être confié à un organe *quasi judiciaire* qui aurait pour caractéristique minimale d'être *indépendant de l'administration*.

A cette question, la Cour européenne des droits de l'homme (CEDH) et le Tribunal fédéral ont donné deux réponses qui ne convergent pas vraiment: la Cour a dit clairement qu'elle se contentait d'un organe *quasi judiciaire*, le Tribunal fédéral paraît exiger l'intervention d'une autorité judiciaire.

Dans l'arrêt Klass c. Allemagne, du 6 septembre 1978, la Cour a jugé qu'en matière de surveillance préventive, une loi allemande qui soumettait les écoutes téléphoniques à l'approbation préalable d'un comité de trois membres, eux-mêmes élus par une commission du Bundestag et statuant en pleine indépendance, satisfaisait aux exigences de l'art. 8, al. 2, CEDH en tant que celui-ci n'admettait d'ingérence de l'Etat dans la vie privée des particuliers que si elle constituait une mesure justifiée par diverses fins d'intérêt public (sécurité nationale, sûreté publique, etc.) et nécessaire dans une société démocratique (cf. notamment Klass, § 21, 53 et 60) et à celles de l'art. 13 CEDH qui garantit le droit à un recours effectif.

Certes la Cour a-t-elle ajouté qu'il était "en principe souhaitable que le contrôle soit confié à un juge en un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique", mais elle a estimé que, tout compte fait, le système allemand du comité indépendant, quoique non judiciaire, "ne transgressait pas les limites de ce qui peut passer pour nécessaire dans une société démocratique" (ibid., § 56).

Dans l'arrêt de principe de 1983, précité, le Tribunal fédéral, confronté à un problème du même genre, a tenu un langage un peu différent. Ayant à se prononcer sur la conformité d'une loi de surveillance à la fois préventive et répressive (en l'espèce, de Bâle-Ville) à l'art. 8 CEDH ainsi qu'à l'art. 36, al. 4, de l'ancienne Constitution fédérale garantissant le secret de la correspondance, il a déclaré notamment : "Bei der Beurteilung dieses Verfahrens ist insbesondere in Betracht zu ziehen, dass eine richterliche Behörde die Ueberwachung genehmigen muss … Diese weitgehende obligatorische Kontrolle durch eine richterliche Behörde bietet dem Betroffenen … einen hinreichenden Schutz" (ATF 109 Ia 273, 296). Douze ans plus tard, il a confirmé, en se référant expressément à l'arrêt de 1983, que "die Telephonüberwachung als geheim durchgeführte Massnahme … bedarf einer richterlichen Prüfung" (ATF 122 I 182, 190, T., du 2 mai 1996). Dans le second cas, le recours aux mesures de surveillance a cependant fait l'objet d'un débat lors de la procédure pénale formelle.

Ce qui, toutefois, n'est pas tout à fait clair, c'est si le Tribunal fédéral s'est borné à décrire la législation de Bâle-Ville, en concluant qu'elle était parfaitement conforme à la Convention et à la Constitution fédérale, ou s'il a implicitement voulu dire que la Constitution fédérale exige l'intervention d'un juge, même si la Convention européenne n'en fait pas de même (cf. arrêt Klass). En d'autres termes, ce qu'on ne sait pas de façon certaine, c'est si, pour le Tribunal fédéral, l'intervention du juge, considérée comme "souhaitable" dans le cadre de la CEDH, est "obligatoire" dans le système constitutionnel suisse, ou si les législations qui l'imposent ne vont pas plus loin que ne le requièrent et la Convention européenne et la Constitution fédérale.

Devant cette incertitude, le présent projet de loi a retenu la "solution du Tribunal fédéral"; il prévoit que le Tribunal administratif fédéral contrôle si l'utilisation de moyens spéciaux de recherche d'informations est conforme au droit.

Al. 1
Cet alinéa fixe, d'une part, la première étape pour l'utilisation de moyens spéciaux de recherche d'informations: la demande doit être déposée par l'office fédéral. Il indique, d'autre part, que le Tribunal administratif fédéral est responsable du contrôle juridique de ces demandes et décrit la manière dont cet examen doit se dérouler:

Let. a
Le Tribunal administratif fédéral a pour tâche principale de vérifier que l'emploi de moyens spéciaux de recherche d'informations envisagé par l'office fédéral est "conforme au droit", notamment aux conditions d'intérêt public et de proportionnalité énoncées à l'art. 18b et au respect de la légalité des dispositions de la loi qui s'appliquent à chacun d'eux. En d'autres termes, le contrôle implique un examen de la légalité et de la proportionnalité de l'utilisation de moyens spéciaux de recherche d'informations.

Let. b
Une autre tâche du Tribunal administratif fédéral est de contrôler si les conditions prévues par la loi pour ajourner la communication prévue à l'art. 18i ou y renoncer sont remplies. Là également, il s'agit d'un contrôle juridique et non pas d'opportunité politique, ce dernier aspect relevant de la compétence du chef du DFJP.

Let. c
Une troisième tâche du Tribunal administratif fédéral est de juger du caractère conforme au droit de la constitution d'identités d'emprunt (cf. art. 14c, al. 3 et 4, et art. 14d). Il s'agit d'un contrôle juridique, c'est-à-dire que le Tribunal administratif fédéral doit vérifier si les conditions légales fixées à l'art. 14c, al. 3, et art 14d, al. 1 et 2, sont remplies. Il ne se prononce, en revanche, pas sur l'opportunité de la constitution de telles identités, la décision appartenant au chef du DFJP. Rappelons qu'en ce qui concerne les identités d'emprunt, l'avis du Tribunal administratif fédéral a un caractère impératif: la constitution d'une identité d'emprunt implique que la commission a donné un avis positif (cf. art. 14c, al. 3 et art. 14d, al. 1).

Al. 2
L'alinéa 2 précise que, concernant tous les cas prévus à l'al. 1, le Tribunal administratif fédéral ne doit rendre sa décision qu'en connaissance de toutes les bases pertinentes. Cela signifie que dans ses demandes relatives à l'utilisation de moyens spéciaux de recherche d'informations, l'office fédéral doit décrire le but visé conformément à l'art. 18a, les conditions conformément à l'art. 18b et les détails relatifs à l'exécution selon l'art. 18f, al. 2; dans ses demandes de dérogation à l'obligation de communiquer, l'office fédéral doit exposer ses motifs selon l'art. 18i, al. 2, et dans ses demandes de création d'une identité d'emprunt, il doit définir les motifs précis et les domaines dans lesquels l'identité d'emprunt pourra être employée conformément aux art. 14c et 14d.

Al. 3
Le Tribunal administratif fédéral examine si la demande de l'office fédéral est conforme au droit. Il rend, par écrit, son avis dûment motivé dans les 72 heures à l'office fédéral; il peut aussi demander des explications ou un complément d'informations à l'office fédéral avant de rendre son avis. Enfin, il peut accepter partiellement la demande ou assortir son avis de charges.

L'avis entièrement ou partiellement positif du Tribunal administratif fédéral est une condition nécessaire, quoique non suffisante, de l'emploi de moyens spéciaux de recherche d'informations (art. 18e). C'est le "feu vert" qui permet la suite de la procédure d'approbation, mais il faudra encore, de surcroît, une décision du Conseil fédéral.

La dernière phrase de l'al. 3 dispose que le Tribunal administratif fédéral doit communiquer au département tous les avis négatifs qu'il rend. Cette procédure d'information doit permettre à la direction du département d'avoir une vue d'ensemble des demandes déposées par l'office fédéral et non pas seulement des avis positifs.

Al .4
Cet alinéa octroie une marge de manœuvre suffisante au Tribunal administratif fédéral s'agissant de son organisation interne et précise uniquement qu'une chambre spécifique, qui traite régulièrement de questions relevant de la protection de l'Etat, doit être désignée, qui garantira la continuité de la jurisprudence. Les exigences liées au maintien du secret nécessaire sont mentionnées, ce qui justifie notamment le fait que cette chambre doive disposer de son propre secrétariat.

Au vu des intérêts et des biens juridiques en jeu, il paraît clair, même sans qu'il existe pour cela de base légale spéciale, que seuls les juges compétents peuvent traiter ces cas (on renoncera donc à impliquer des secrétaires juridiques, des greffiers, etc.).

2.24 Art. 18e Décision quant à l'utilisation de moyens spéciaux de recherche d'informations

Al. 1
L'office fédéral ne peut soumettre, pour approbation, une demande d'utilisation de moyens spéciaux de recherche d'informations au département ou au Conseil fédéral que si le Tribunal administratif fédéral a préalablement rendu un avis positif concernant cette demande.

Al. 2 et 3
Si le Tribunal administratif fédéral a rendu un avis positif concernant les aspects juridiques de l'utilisation de moyens spéciaux de recherche d'informations, un examen sous l'angle politique est alors effectué: avec l'avis positif du Tribunal administratif fédéral, le dossier est transmis au chef du DFJP. Ce dernier consulte obligatoirement le chef du DDPS en sa qualité de président de la Délégation du Conseil fédéral pour la sécurité. S'ils sont tous les deux d'accord pour l'utilisation des moyens spéciaux de recherche d'informations, le chef du DFJP prend alors la décision finale. En cas de désaccord, c'est le Conseil fédéral qui décide. Par ailleurs, le chef du DFJP ou le Conseil fédéral peut renoncer, totalement ou en partie, à la mesure demandée, même si le Tribunal administratif fédéral a rendu un avis positif au sujet de cette demande.

Le chef du DFJP ou le Conseil fédéral doit respecter les charges dont le Tribunal administratif fédéral peut assortir un avis positif (cf. art. 18d, al. 3).

Al. 4
Si le chef du DFJP ou le Conseil fédéral juge opportun de recourir à des moyens spéciaux de recherche d'informations, il en précise les modalités (let. a à e), notamment:

- le but à atteindre;
- le perturbateur présumé;
- les moyens pouvant être utilisés selon l'art. 18a, al. 2;
- la durée de l'utilisation des moyens: la loi prévoit un délai maximal de six mois (cf. al. 4). Certaines opérations (comme la perquisition d'un système d'information) ne s'étendent pas dans le temps mais sont, en quelque sorte, immédiatement consommées. Pour ce type de cas, le projet prévoit la fixation d'un délai: il s'agira de déterminer dans quel délai l'opération devra être exécutée. En d'autres termes, le moyen lui-même ne dure pas, mais c'est l'autorisation d'y recourir qui a une durée déterminée; et les charges liées à l'application (rapports réguliers).

Al. 5
Si le Tribunal administratif fédéral rend un avis positif, la durée fixée par le chef du DFJP ou par le Conseil fédéral peut être prolongée de trois mois à deux reprises, ce

qui signifie qu'un moyen spécial peut être utilisé pendant douze mois au maximum (6 + 3 + 3); l'office fédéral ou le département doit formuler une nouvelle demande s'il est nécessaire d'utiliser le moyen en question plus longtemps.

Al. 6
Cet alinéa décrit la relation avec les compétences constitutionnelles du Conseil fédéral et est purement déclaratoire. La procédure prévue par la LMSI ne supplante pas les compétences constitutionnelles du Conseil fédéral fondées directement sur la Constitution fédérale (Cst.). Elle vient, en quelque sorte, s'y ajouter, en tant qu'elle définit une procédure légale pour régler les cas ordinaires. Dans des cas extraordinaires, le Conseil fédéral pourra donc toujours recourir aux compétences que lui confèrent notamment l'art. 185, al. 3, Cst. et ordonner, si les conditions prévues par la Constitution sont remplies, des moyens spéciaux de recherche d'informations pour faire face à une menace contre la sûreté intérieure ou extérieure. Ainsi peut-il théoriquement arriver que l'emploi de moyens spéciaux ne puisse pas être ordonné parce que les conditions légales fixées dans la LMSI ne sont pas remplies et que le Tribunal administratif fédéral a, de ce fait, donné un avis juridique négatif. Si néanmoins le chef du département considère que la situation est tellement grave que ces moyens doivent pouvoir être utilisés, il pourra proposer au Conseil fédéral d'ordonner les mesures jugées nécessaires. Si donc le besoin se fait sentir, compte tenu de circonstances particulières, de procéder par un acte de gouvernement, il appartiendra au Conseil fédéral agissant en collège et conformément aux conditions fixées notamment à l'art. 185, al. 3, Cst., de prendre lui-même la responsabilité politique d'ordonner l'emploi d'un moyen spécial.

2.25 Art. 18f Procédure d'urgence

L'art. 18f règle les cas exceptionnels où il y a péril en la demeure. Il faut pouvoir agir rapidement dans les cas où le fait d'attendre l'avis du Tribunal administratif fédéral, du chef du DFJP ou du Conseil fédéral compromet les moyens spéciaux de recherche d'informations ou les rend impossibles. Cela peut être le cas lorsqu'une personne cible importante entre inopinément en Suisse et doit faire l'objet d'une surveillance de tous les instants dès son arrivée, par exemple si un contrôle des télécommunications doit aussi être mise en place.

Al. 1
Dans les cas d'urgence, le directeur de l'office fédéral ordonne directement les moyens spéciaux de recherche d'informations afin qu'ils puissent être immédiatement mis en œuvre. Même en cas d'urgence, les conditions matérielles liées à l'emploi d'un moyen spécial (art.18b, al.1, let. a à d) doivent être remplies. Il appartient au directeur de l'office fédéral de s'en assurer. Le département doit être informé dans le même temps.

Al. 2
Le directeur de l'office fédéral est tenu de soumettre la demande habituelle au Tribunal administratif fédéral dans les 24 heures, en motivant dûment l'urgence de la mesure. La procédure suit ensuite son cours ordinaire. Comme dans la procédure "ordinaire", le Tribunal administratif fédéral doit rendre son avis dans les 72 heures.

Al. 3
Pour que l'office fédéral puisse soumettre a posteriori une demande d'approbation de l'utilisation de moyens spéciaux de recherche d'informations au Conseil fédéral, il faut que le Tribunal administratif fédéral ait rendu un avis positif. La demande doit être soumise immédiatement (rapidement).

Al. 4
Si le Tribunal administratif fédéral ne donne pas un avis positif ou si le chef du DFJP ou le Conseil fédéral ne donne pas son approbation ultérieure aux moyens spéciaux de recherche d'informations ordonnés en urgence, l'office fédéral doit immédiatement détruire toutes les données collectées jusqu'alors dans le cadre de cette recherche d'informations (cf. la disposition analogue; art. 7, al. 4, LSCPT).

2.26 Art. 18g Arrêt de l'utilisation de moyens spéciaux de recherche d'informations

Lorsque la recherche spéciale d'informations n'est plus nécessaire (let. a), se révèle vaine (let. b), n'est pas prolongée (let. c) ou lorsque, dans le cadre d'une procédure d'urgence, le Tribunal administratif fédéral estime qu'elle n'est pas légale ou que le chef du DFJP ou le Conseil fédéral a refusé son approbation (let. d et e), l'office fédéral l'interrompt immédiatement. Si l'approbation d'une recherche déjà en vigueur est refusée, les éléments issus de cette recherche ne peuvent pas être utilisés. Si l'office fédéral a déjà communiqué des données issues de cette recherche à d'autres organes ou autorités, il doit leur demander de procéder à leur destruction. Ces règles concrétisent les principes généraux applicables en matière de traitement de données personnelles.

2.27 Art. 18h Traitement des données personnelles récoltées grâce à des moyens spéciaux de recherche d'informations

Cette disposition règle le traitement des données personnelles recueillies par l'emploi de moyens spéciaux de recherche d'informations.

Al. 1
Cette disposition précise le régime général de la conservation des données fixé à l'art. 15 LMSI. Les données recueillies doivent être détruites dans les 30 jours qui suivent la fin de l'emploi des moyens spéciaux s'il apparaît qu'elles n'ont pas de lien avec la menace qui est à l'origine de l'utilisation des moyens spéciaux de recherche d'informations.

Al. 2
Cet alinéa indique que le traitement des données personnelles récoltées grâce à des moyens spéciaux de recherche d'informations est régi par l'art. 3, al. 1 à 3, et les art. 15, 16 et 17 LMSI.

2.28 Art. 18i Obligation de communiquer

Cette règle est un des éléments déterminants du système mis en place: elle est l'amorce du contrôle juridique a posteriori (voir le commentaire de l'art. 18d in initio).

Si, après usage, l'office fédéral n'informe pas la personne touchée que des informations la concernant ont été récoltées grâce à des moyens spéciaux, celle-ci ne pourra en général pas l'attaquer, à moins qu'elle n'en ait eu connaissance par une autre voie. Le corollaire de la communication, c'est le droit de recours de la personne touchée auprès des tribunaux (cf. art. 29a).

L'obligation de communiquer est de nature constitutionnelle, c'est la conséquence implicite de la garantie du respect de la vie privée et du secret de la correspondance fondée sur les art. 8 CEDH et 13 Cst. Dans une procédure pénale, le droit d'être renseigné se confond avec le droit d'être entendu (art. 29 Cst.). Dans une opération de recherche *préventive* qui n'est pas suivie d'une action pénale, il peut cependant arriver que la loi qui lui sert de base omette de mentionner l'obligation de communiquer. C'est précisément ce qui s'est passé avec la législation de Bâle-Ville qui était en cause dans l'arrêt de novembre 1983, plusieurs fois cité. La loi disait sobrement : "Das Verfahren ist … gegenüber dem Betroffenen geheim" (ATF 109 Ia 273, 276). A quoi le Tribunal fédéral a répondu que la Constitution "verbietet es aber, dass von einer nachträglichen Bekanntgabe generell in jedem Fall abgesehen wird. … Demnach ist vielmehr zu fordern, dass den Betroffenen grundsätzlich von den durchgeführten Überwachungsmassnahmen nachträglich Kenntnis gegeben wird. Dies hat für die präventive und die repressive Überwachung sowie gegenüber den Angeschuldigten und Verdächtigten und Drittpersonen zu gelten. … Demnach ist grundsätzlich von der Pflicht auszugehen, Überwachungmassnahmen den Betroffenen bekanntzugeben" (ATF 109 Ia 273, 298-299). Il en concluait que le silence de la loi bâloise devait, par interprétation, être complété en ce sens.

Al. 1
Fondé sur cette jurisprudence, le présent projet de loi consacre le principe du droit d'être renseigné. L'office fédéral doit renseigner dès la fin de l'opération de recherche (sur la notion d'opération, voir l'art. 14 OMSI).

Al. 2
Un tel principe ne va, évidemment, pas sans *exceptions*. La CEDH l'a reconnu dans l'arrêt Klass précité (§ 57 à 59, voir le commentaire de l'art. 18d) : la communication ultérieure "pourrait bien compromettre le but à long terme qui motivait à l'origine la surveillance" ; elle risquerait aussi "de contribuer à révéler les méthodes de travail des services de renseignement, leurs champs d'observation et même, le cas échéant, l'identité de leurs agents". Les exceptions de la loi allemande ont donc été jugées acceptables.

Le Tribunal fédéral, dans l'arrêt de 1983, a emboîté le pas (ATF 109 Ia 273, 300-301). Il a admis à peu près le même genre d'exceptions. Tout au plus a-t-il ajouté que "diese Ausnahmen sind nun allerdings streng anzuwenden". Mais, malgré cette précaution un peu oratoire, dans la pratique, l'obligation de communiquer ou le droit d'être renseigné sont sensiblement relativisés par les nécessités des recherches policières. Précisons que les exceptions énumérées dans les let. a à d de l'al. 2 sont largement inspirées de celles qui figurent à l'art. 10, al. 3, LSCPT et à l'art. 22, al. 2, LFIS.

Les motifs justifiant la renonciation à l'obligation de communiquer ou l'ajournement de la communication sont mentionnés de manière exhaustive aux let. a à d.

Par ailleurs, la renonciation temporaire ou durable à la communication n'est pas de la compétence de l'office fédéral. Comme elle restreint la portée d'une règle constitutionnelle, la procédure doit garantir que l'intérêt d'un particulier à pouvoir se défendre contre les atteintes portées à sa sphère privée ne soit pas sacrifié sans qu'un intérêt public *prédominant* ne l'exige *absolument*. Aussi cette pesée des intérêts contraires, qui est d'autant plus délicate que la procédure de communication dépend aussi de la faculté de faire vérifier, par une autorité *judiciaire*, la conformité au droit de l'utilisation de moyens spéciaux de recherche d'informations, justifie de prévoir des règles strictes pour la renonciation à l'obligation de communiquer ou l'ajournement de la communication: au besoin, l'office fédéral dépose une demande dûment motivée indiquant pourquoi il conviendrait de renoncer à la communication. Le Tribunal administratif fédéral procède ensuite à un contrôle juridique de cette demande. S'il rend un avis positif, le chef du DFJP décide alors si la renonciation à communiquer est appropriée.

Grâce à l'obligation de consulter le chef du DDPS prévue à l'art. 18e, al. 2, du présent projet, les éventuels besoins du Service de renseignement stratégique (SRS) quant au maintien du secret peuvent être inscrits suffisamment tôt dans les dossiers et être pris en considération lors de la décision du Tribunal administratif fédéral ou du chef du DFJP.

Le droit d'accès au sens de l'art. 8 ss LPD est réglé par l'art. 18 LMSI.

2.29 Art. 18j Exécution par les cantons

Cette disposition rappelle que la recherche spéciale d'informations opérée par des organes de sûreté des cantons pour le compte de la Confédération est régie par la LMSI. En d'autres termes, si des organes de sûreté des cantons ne procèdent pas, à la demande de la Confédération, à une observation dans des lieux qui ne sont pas librement accessibles ou y installent de dispositifs de surveillance, c'est le régime des art. 18a ss du présent projet qui s'appliquera et non les dispositions du droit cantonal.

2.30 Section 2 Moyens spéciaux de recherche d'informations

Conformément aux art. 36, al. 1, et 164, al. 1, let. a, Cst., les atteintes graves aux droits fondamentaux doivent être prévues dans la loi formelle. A cet égard, il ne suffit pas d'énumérer simplement les différents moyens susceptibles de porter une telle atteinte. Encore faut-il décrire précisément la mesure de ces atteintes, en l'occurrence sur quoi elles peuvent porter, et définir les modalités spécifiques des opérations autorisées. Cette réglementation est d'autant plus importante que le contenu de ces moyens varie selon que l'on se trouve dans une procédure pénale ou dans le cadre d'une recherche d'informations des services de renseignements. Ainsi la perquisition de systèmes informatiques, qui, dans le cadre d'une enquête pénale, se mène, sauf certaines circonstances précises définies par la loi, en présence du suspect ou d'une personne qui le représente, peut, dans le domaine du renseignement, être pratiquée à l'insu de la personne qui en fait l'objet.

2.31 Art. 18k Surveillance de la correspondance par poste et télécommunication

La surveillance de la correspondance par poste et télécommunication à des fins de répression est réglée dans la LSCPT. Cela dit, la surveillance à titre préventif prévue dans le présent projet n'est pas effectuée à des fins de poursuite pénale, mais pour déceler des menaces concrètes liées au terrorisme, au service de renseignements politiques ou militaires prohibé, au commerce illicite d'armes et de substances radioactives et au transfert illégal de technologie. Elle doit donc être réglée dans la LMSI.

La LMSI doit toutefois se limiter à des règles spéciales, là où des modifications ou des précisions doivent être apportées par rapport à la LSCPT. Elle se réfère à la LSCPT pour les questions d'ordre technique et organisationnel, car il n'est pas prévu, en principe, de définir d'autres procédures et exigences techniques pour les surveillances menées à titre préventif. Il convient plutôt d'utiliser les structures qui ont fait leurs preuves.

Al. 1
Cet alinéa a pour but de décrire sur quoi porte la surveillance: elle vise les moyens de communication de manière générale et renonce à mentionner des moyens techniques déterminés afin de ménager la marge d'interprétation nécessaire dans un domaine où l'évolution technique est particulièrement rapide; il faut ensuite que des indices permettent de penser que le perturbateur présumé utilise lesdits moyens pour communiquer avec des personnes ou pour accomplir des actes qui ont un rapport direct avec une menace concrète contre la sûreté intérieure ou extérieure ; il faut enfin que les indices soient suffisamment clairs et actuels pour justifier une surveillance à un moment donné.

Al. 2
La disposition relative à la surveillance d'un poste public de télécommunication correspond à la disposition spéciale figurant à l'art. 4, al. 2, LSCPT. Dans la pratique, il s'agit par exemple de cas où l'observation d'une personne cible ou la mise en œuvre d'autres types de surveillance des télécommunications révèle qu'une personne cible utilise régulièrement une cabine téléphonique publique particulière ou, l'utilise pour une raison bien précise.

Al. 3
Si la surveillance d'une personne cible qui change de raccordement à intervalles rapprochés, par exemple en utilisant des cartes à prépaiement avec un téléphone portable, n'était ordonnée qu'après constatation des faits, la mesure interviendrait presque toujours trop tardivement. Dans de tels cas, une surveillance de tous les raccordements identifiés que la personne ou l'organisation utilise peut être ordonnée. Cette disposition correspond à l'art. 4, al. 4, LSCPT.

Al. 4
Il n'est pas nécessaire de créer une disposition parallèle à celle de la LSCPT pour la mise en œuvre des surveillances des postes et des télécommunications effectuées à titre préventif. La LSCPT et ses dispositions d'exécution sont donc applicables par analogie pour les formes de surveillance, leur mise en œuvre technique et les dédommagements.

Intérêt public et proportionnalité
La surveillance de la correspondance constitue une atteinte grave à la sphère privée. Conformément à l'art. 36 Cst., elle doit être justifiée par un intérêt public et proportionnée au but visé. Quant à la justification d'intérêt public, nous relèverons que, comme tous les autres moyens spéciaux, la surveillance de la correspondance ne peut intervenir que dans les trois domaines tenus pour les plus susceptibles de compromettre les fondements mêmes de notre société (cf. le commentaire relatif à l'art 13a, al. 1). On ne saurait donc nier que cette mesure est justifiée au regard de l'intérêt public. Pour juger de son caractère proportionné, il y a lieu d'examiner si elle est adéquate, nécessaire et proportionnée au sens étroit du terme. Quand il peut être établi, sur la base d'indices suffisants, que le perturbateur présumé utilise les moyens de communication à distance pour ses agissements, la surveillance de ces moyens constitue le moyen adéquat d'accéder aux informations utiles pour évaluer ladite menace, voire la prévenir.

En revanche, les organes de sûreté ne sont pas autorisés à surveiller de manière exploratoire, en quelque sorte "à tout hasard", les moyens de communication d'une personne du seul fait que cette personne est considérée, sur la base de certaines sources, comme susceptible de menacer la sûreté intérieure. Encore faut-il que, dans le cas concret, il y ait des indices suffisants pour penser qu'elle utilise précisément des moyens déterminés de communication à distance. Dès lors qu'un lien entre les agissements tenus pour menaçants et l'usage de tels moyens peut être établi avec une certaine vraisemblance, la mesure peut être tenue pour adéquate.

Quant au caractère nécessaire, il est évident que, pour connaître les contacts ou le contenu des communications à distance d'une personne tenue pour menaçante, il n'y a pas d'autre moyen à disposition que l'interception de cette communication. Le recours à un moyen ordinaire (art. 14, al. 2) ne permettrait pas, en l'occurrence, d'accéder à ces informations.

Enfin, en ce qui a trait à la proportionnalité au sens étroit, c'est-à-dire à la question de savoir si l'intérêt public en jeu mérite de l'emporter sur l'atteinte que subit la personne concernée, elle n'est guère appréciable de manière abstraite. C'est seulement en connaissance des circonstances du cas d'espèce que cette pesée peut être faite correctement. Ce qui importe ici, c'est que cette pesée juridique n'est pas laissée aux seuls organes de sûreté, mais qu'elle est confiée à une autorité judiciaire indépendante, qui est mieux à même de faire la balance entre le souci des professionnels de la sûreté, d'une part, et l'intérêt légitime du particulier à communiquer et entretenir des contacts sans ingérence étatique. Dans les limites décrites ci-dessus, nous pouvons donc admettre que la surveillance de la correspondance constitue, compte tenu des garde-fous que pose le projet de loi, une mesure proportionnée au but d'intérêt public qui la justifie.

2.32 Art. 18l Surveillance de lieux qui ne sont pas librement accessibles et surveillance au moyen d'appareils techniques

Actuellement, la LMSI autorise l'observation de faits, y compris au moyen d'enregistrement d'images et de sons, dans des lieux publics et librement accessibles (art. 14, al. al. 2, let. f). La présente disposition a pour but d'étendre l'observation à des lieux qui ne sont pas librement accessibles (logements, chambres d'hôtel, lieux de réunion, locaux professionnels, etc. ; cf. al. 1). En outre, elle étend

aussi la règle actuelle en ce qui concerne l'usage de dispositifs techniques de surveillance (cf. al. 2). En effet, ceux-ci ne peuvent, en vertu du droit en vigueur, être utilisés pour écouter ou enregistrer une conversation non publique (cf. art. 179bis et 179ter CP) ou pour observer un fait relevant du domaine secret ou privé d'une personne avec un appareil de prises de vue ou le fixer sur un porteur d'images (cf. art. 179^{quater} CP), quand bien même ce fait se déroulerait dans un lieu librement accessible. En d'autres termes, la loi actuelle n'autorise pas l'*observation individuelle* au moyen de dispositifs techniques (p. ex. l'enregistrement d'une conversation privée dans un restaurant, dans un hall de gare, dans une église) ; elle ne permet que l'enregistrement de faits qui peuvent être tenus pour publics (discours, prêches publics, propos destinés à interpeller le public, etc.).

Al. 1

Cet alinéa a pour but de décrire les modalités de l'observation: elle est, à la différence de celle qui peut être pratiquée dans le cadre d'enquêtes pénales, opérée en l'absence du perturbateur présumé ; mais il faut que des indices permettent de penser que ledit perturbateur utilise un lieu déterminé pour communiquer avec des personnes ou pour accomplir des actes qui ont un rapport direct avec une menace concrète contre la sûreté intérieure ou extérieure. En outre, il faut, là également, que ces indices soient suffisamment clairs et actuels pour justifier une telle observation.

Al. 2

L'utilisation d'appareils techniques de surveillance correspond, en termes de réglementation et de portée, à l'art. 66, al. 2, de la loi fédérale du 15 juin 1934 sur la procédure pénale (RS 312.0). Il s'agit d'appareils d'observation et d'enregistrement acoustiques et optiques. Ces dispositifs peuvent être employés dans un espace privé en présence de certaines conditions; ils peuvent aussi être employés pour saisir des faits qui, tout en se déroulant dans un espace ouvert au public, ne sont pas destinés à être publics (p. ex. une conversation privée dans un restaurant).

Intérêt public et proportionnalité

L'observation dans un lieu qui n'est pas librement accessible au public ou au moyen de dispositifs techniques de surveillance constitue une atteinte grave à la sphère privée. Comme nous l'avons vu précédemment, il faut, conformément à l'art. 36 Cst., que cette atteinte soit justifiée par un intérêt public et proportionnée au but visé. En ce qui concerne la justification d'intérêt public de ce moyen spécial, nous renvoyons au commentaire des art. 13a et 18k. Quant à sa proportionnalité, nous retiendrons ce qui suit : s'il peut être établi, sur la base d'indices suffisants, que le perturbateur présumé utilise un lieu déterminé pour ses agissements, l'observation des faits qui s'y passent constitue un moyen adéquat d'accéder aux informations intéressantes pour évaluer ladite menace, voire la prévenir. Les organes de sûreté ne sont, en revanche, pas autorisés à observer de manière générale tout l'environnement d'une personne du seul fait que cette personne est considérée, sur la base de certaines sources, comme susceptible de menacer la sûreté intérieure. L'observation doit se concentrer sur une cible déterminée, parce qu'il y a lieu de penser que celle-ci constitue un point stratégique des activités du présumé perturbateur. Dès lors que ce lien entre les agissements tenus pour menaçants et l'usage d'un lieu peut être établi avec une certaine vraisemblance, la mesure peut être tenue pour adéquate. Quant à son caractère nécessaire, il est évident que pour identifier des faits se déroulant en des lieux privés, aucun des moyens ordinaires ne s'y prête, hormis le recours à un informateur pour recueillir des informations générales selon l'art. 14, al. 2, LMSI.

Mais ce recours n'est pas toujours possible. Enfin, quant à la proportionnalité au sens étroit, c'est-à-dire savoir si l'intérêt public en jeu mérite de l'emporter sur l'atteinte que subit la personne concernée, elle n'est, comme nous l'avons déjà dit, guère appréciable de manière abstraite. Il appartiendra au Tribunal administratif fédéral de procéder à cette pesée dans le cas concret et d'admettre ou de nier le caractère prépondérant de l'intérêt public en cause.

En ce qui concerne l'usage de dispositifs techniques de surveillance, nous relèverons que ce moyen constitue, davantage qu'un moyen de surveillance autonome, une modalité de l'observation de faits relevant de la sphère privée. En effet, avec l'observation pratiquée à l'aide de dispositifs techniques, on ne fait que substituer ces dispositifs à l'observateur physique qui s'introduirait dans des lieux privés. Il s'ensuit que, pour les raisons mêmes qui permettent de tenir pour proportionnelle l'observation de faits dans un lieu privé, on peut admettre que l'observation pratiquée à l'aide de dispositifs techniques constitue un moyen qui, a priori, peut être considéré comme conforme au principe de la proportionnalité. C'est dans le cas d'espèce qu'il sera possible de déterminer si l'intérêt public en jeu est prépondérant.

2.33 Art. 18m Perquisition secrète d'un système informatique

Les moyens informatiques modernes occupent une place toujours plus importante dans notre vie quotidienne. Internet joue désormais un rôle-clé dans l'échange d'informations. Etant donné que les organes de sûreté consultent de plus en plus Internet pour rechercher des informations, les groupes recherchés (comme les organisations terroristes) se sont adaptés à cette évolution et diffusent leurs messages dans des domaines dont l'accès est protégé, par exemple par des mots de passe. Bien que les spécialistes soient en mesure de s'introduire dans ces domaines protégés, ils ne le font pas car cette opération est répréhensible sur le plan pénal (art. 143bis CP; accès indu à un système informatique).

La disposition décrit en quoi consiste le moyen spécial et comment il peut être employé. Par analogie aux dispositions correspondantes du CP (cf. art. 143 et 143bis CP), son champ d'application s'étend aux données enregistrées électroniquement ou selon un mode similaire, qui sont spécialement protégées contre tout accès indu de tiers. En outre, la perquisition est, à la différence de celle pratiquée dans le cadre d'une enquête pénale, opérée à l'insu du perturbateur présumé. Enfin des indices suffisamment clairs et actuels doivent permettre de supposer que ladite personne utilise une installation déterminée pour ses agissements. Relevons aussi que le moyen est conçu comme un instrument passif, c'est-à-dire que la disposition ne permet pas d'implanter dans le système des éléments susceptibles de le bloquer, de le brouiller ou d'y détruire des données (comme la recherche d'adresses dans l'ordinateur portable d'un perturbateur présumé ou le décodage d'un courriel chiffré).

Intérêt public et proportionnalité

La perquisition d'un système informatique constitue une atteinte grave à la sphère privée. Comme nous l'avons vu précédemment, il faut, conformément à l'art. 36 Cst, que cette atteinte soit justifiée par un intérêt public et qu'elle soit proportionnée au but visé. En ce qui concerne la justification d'intérêt public de ce moyen spécial, nous renvoyons au commentaire des art. 13a et 18l. Quant à la proportionnalité, il faut

considérer ce qui suit : dès lors qu'il est établi avec une certaine vraisemblance que le perturbateur présumé utilise un système et des réseaux informatiques pour stocker, pour lui-même ou à l'intention de tiers, des informations propres à constituer une menace concrète pour la sûreté intérieure ou extérieure, la perquisition d'un tel système est un moyen adéquat et nécessaire pour accéder auxdites données. Il faut, en particulier, relever ici qu'aucun autre moyen que celui de l'intrusion dans le système même ne permettrait de récolter lesdites informations. Si nous avons limité l'instrument de la perquisition à celle des seuls systèmes informatiques et renoncé à la perquisition de locaux ou de véhicules, c'est que, dans ces derniers cas, l'objectif de recherche peut être atteint par le recours à d'autres instruments de la recherche d'informations, en particulier à celui de l'observation physique ou au moyen de dispositifs techniques de surveillance. Comme on le voit, le choix même des moyens spéciaux autorisés traduit cette idée de proportionnalité qui doit inspirer l'ensemble du projet de révision. Quant à la proportionnalité au sens étroit, c'est-à-dire savoir si l'intérêt public en jeu mérite de l'emporter sur l'atteinte que subit la personne concernée, elle n'est, comme nous l'avons déjà dit, guère appréciable de manière abstraite. Il appartiendra au Tribunal administratif fédéral de procéder à cette pesée dans le cas concret et d'admettre ou de nier le caractère prépondérant de l'intérêt public qui sera en jeu.

2.34 Chapitre 3b Interdiction d'activités

Ce chapitre introduit un type de mesures nouveau, à savoir l'interdiction d'activités. En effet, la loi de 1997 se limite, comme on a déjà eu l'occasion de le dire, à régler le problème du traitement des données personnelles par les organes de sûreté et à poser des règles d'entraide administrative. En revanche, elle n'a, jusqu'à maintenant, pas eu pour objet de fixer des règles de comportement pour les particuliers. Le projet de révision de la LMSI (propagande incitant à la violence, violence lors de manifestations sportives) approuvé par le Parlement le 24 mars 2006, qui propose des mesures contre la propagande incitant à la violence et contre la violence lors de manifestations sportives, est un premier pas dans ce sens puisqu'il propose d'introduire plusieurs règles qui prescrivent des obligations de comportement pour le particulier (cf. interdiction de périmètre, interdiction de se rendre dans un pays donné, obligation de se présenter à la police, garde à vue). Dans une perspective comparable, la présente révision propose de renforcer la prévention en dotant les autorités fédérales d'instruments leur permettant d'agir directement sur le comportement des particuliers et d'améliorer ainsi les effets de la prévention.

2.35 Art. 18n

Cette disposition octroie au chef du département la compétence de prononcer des interdictions administratives d'activités qui sont présumées menacer concrètement la sûreté intérieure ou extérieure. De telles interdictions ne peuvent actuellement être prononcées que sur la base de la Constitution même, laquelle habilite le Conseil fédéral à édicter des ordonnances et à prendre des mesures pour sauvegarder les intérêts du pays dans ses relations internationales (art. 184, al. 3, Cst.) ou pour parer à des troubles existants ou imminents menaçant gravement la sûreté intérieure (art. 185, al. 3, Cst.). Les ordonnances fondées sur ces deux dispositions constitutionnelles doivent cependant être limitées dans le temps. Or de telles mesures ne peuvent être prolongées indéfiniment au risque sinon de vider la règle constitutionnelle de toute sa substance. Dès lors, nous proposons d'introduire, au

niveau de la loi, une règle permettant d'interdire les activités dont on pourra établir qu'elles constituent une menace concrète contre la sûreté intérieure ou extérieure.

La nouvelle règle ne modifie rien aux compétences du Conseil fédéral fondées sur les art. 184, al. 3, et 185, al. 3, Cst. Ces compétences constitutionnelles demeurent inchangées et coexisteront dans la pratique avec la nouvelle compétence introduite par la révision de la LMSI (cf. commentaire relatif aux art. 18e in fine et 29a, al. 1).

Enfin, en ce qui concerne les voies de droit, les interdictions prononcées par le Conseil fédéral en vertu de la Constitution et celles prononcées par le chef du département selon la LMSI n'obéiront pas au même régime: les décisions du Conseil fédéral, lesquelles constituent de véritables actes de gouvernement, ne peuvent être portées devant une juridiction fédérale que dans l'hypothèse où le droit international confère un droit à ce que la cause soit jugée par un tribunal[4]. En dehors de ces cas, les décisions du Conseil fédéral sont définitives. En revanche, les décisions fondées sur la LMSI constituent des actes administratifs parfaitement justiciables et pourront, de ce fait, être portées devant le Tribunal administratif fédéral puis le Tribunal fédéral (cf. les commentaires relatifs aux art.18e et 29a).

Al. 1

Cette disposition permet de prononcer l'interdiction d'une activité déterminée. Ainsi, certaines activités, telles que les collectes destinées à des fonds pour veuves et orphelins dans des régions en crise à l'étranger, semblent à première vue anodines, et paraissent même tout à fait louables. Il n'est pourtant pas rare que ces collectes soient accompagnées de pressions relevant de l'extorsion et du chantage (p. ex. lorsque l'on indique aux membres d'une diaspora vivant en Suisse que des membres de leur famille restés au pays pourraient être lésés s'ils refusent de faire un don). Par ailleurs, les fonds ainsi collectés, ou du moins une partie de ces fonds, seront selon toute vraisemblance utilisés à une toute autre fin que celle indiquée initialement lors de la collecte, pour l'achat d'armes par exemple au profit de mouvements de résistance dans les régions en crise. Cela dit, la preuve directe de tels agissements est souvent difficile à établir car les personnes contraintes de faire des dons en Suisse se taisent par crainte pour elles-mêmes ou pour leurs proches, amis et connaissances dans leur pays d'origine. En outre, la trace de l'argent se perd à cause des multiples transferts, ou parce que les certificats étrangers précisant l'utilisation de l'argent sont soit imprécis ou falsifiés, soit vrais mais avec un faux contenu car établis contre rémunération; mais les raisons de la perte de la trace des fonds peuvent aussi être d'une toute autre nature.

L'interdiction doit définir précisément quelle activité est visée, dans quels lieux et dans quelles circonstances son exercice est interdit. L'autorité ne saurait se contenter de formuler une interdiction globale. L'art. 292 CP règle les sanctions juridiques en cas de violation d'une interdiction. Il n'est pas nécessaire de mentionner cette norme pénale dans la loi, car cette mention n'aurait qu'un caractère déclaratoire.

[4] Voir ATF 125 II 417 ss; cette jurisprudence est dorénavant expressément consacrée à l'art. 83, let. a, de la loi sur le Tribunal fédéral, FF 2005 3829, et à l'art. 32, al. 1, let. a, de la loi sur le Tribunal administratif fédéral, FF 2005 3875. Ces lois entreront vraisemblablement en vigueur le 1er janvier 2007.

Le chef du département doit décrire aussi précisément que possible l'étendue et le contenu de l'interdiction. Là également, les sanctions juridiques de la violation d'une telle interdiction sont régies par l'art. 292 CP. Un rappel de cette disposition n'est pas nécessaire (cf. ci-dessus, al. 1).

Al. 2
Vu l'impact de ces mesures d'interdiction sur l'exercice des droits fondamentaux des personnes touchées, il est important qu'elles soient limitées dans le temps afin d'obliger les autorités à vérifier si les conditions d'une interdiction sont toujours réunies. Si tel est le cas, l'interdiction pourra être prolongée autant de fois qu'il est nécessaire. Cette limitation dans le temps ne poursuit donc pas la même finalité que celle qui est prévue aux art. 184, al. 3, et 185, al. 3, Cst., où il s'agit de s'assurer qu'une mesure prise dans l'urgence en raison de son caractère imprévisible, grave et concret soit transférée, si elle est destinée à durer, dans le droit "ordinaire", c'est-à-dire approuvée par le législateur. En d'autres termes, alors que cette clause de limitation dans le temps répond principalement à une préoccupation liée au principe de la séparation des pouvoirs et au respect de la procédure législative ordinaire, la limitation dans le temps que nous prévoyons ici se justifie pour des raisons matérielles liées à la gravité de l'atteinte portée aux droits fondamentaux. Corollaire de cette limitation dans le temps, le projet de loi prévoit aussi l'obligation pour l'autorité de s'assurer régulièrement (c'est-à-dire pendant la durée de l'interdiction) de la nécessité de maintenir l'interdiction et, si cette dernière n'est plus justifiée, de lever d'elle-même cette interdiction sans attendre que la personne concernée le demande. L'autorité doit donc se montrer active non seulement lorsqu'il s'agit d'interdire mais aussi s'il y a lieu de lever l'interdiction.

Intérêt public et proportionnalité
L'interdiction d'activités est une mesure susceptible de porter une atteinte grave à différents droits fondamentaux dans la mesure où ces droits protègent lesdites activités. Pensons notamment à la liberté d'association (art. 23 Cst.), à la liberté de conscience et de croyance (art. 15, al. 3, Cst.), à la liberté d'opinion et d'information (art.16 Cst.), à la liberté de réunion (art. 22 Cst.), voire à la liberté personnelle (art. 10 Cst.) et à la garantie de la propriété (art. 26 Cst.). Conformément à l'art. 36 Cst., une telle atteinte doit notamment être justifiée par un intérêt public et proportionnée au but visé. Relevons, à cet égard, que la prévention du terrorisme et de l'extrémisme violent constitue une justification d'intérêt public non discutable et expressément consacrée dans la LMSI. Au regard de la proportionnalité, nous considérons qu'une interdiction d'activités, n'est, dans la mesure où elle est accompagnée des cautèles ici prévues, pas a priori disproportionnée. Toute la question sera de savoir si, dans le cas concret, l'interdiction prononcée reposera sur un intérêt public prépondérant avéré.

2.36 Art. 27, al. 1bis

En complément de l'obligation d'informer régulièrement le Conseil fédéral et l'organe parlementaire compétent sur la conduite de la politique en matière de sûreté intérieure ou extérieure, nous proposons d'introduire une obligation spécifique de faire rapport sur la manière dont les organes de sûreté auront usé des nouveaux instruments. Vu la gravité des atteintes susceptibles d'être portées aux droits fondamentaux de la population de notre pays, une telle obligation se justifie pleinement. Cette obligation d'information spéciale porte sur les mesures les plus

graves au regard de notre régime fondé sur la liberté et la confiance, à savoir la constitution et l'usage d'identités d'emprunt, les moyens spéciaux de recherche d'informations et les interdictions d'activités. Notons que bien qu'aucune loi ne le prévoie expressément, des rapports complets sont aujourd'hui déjà soumis au département (rapports d'opérations).

2.37 Art. 29a

La LMSI actuelle ne contient guère de disposition spécifique relative aux procédures et aux voies de droit, mis à part l'art. 18 qui règle le droit d'être renseigné quant aux données personnelles traitées dans le système d'information des organes de sûreté. Or, avec l'introduction des moyens spéciaux de recherche d'informations, moyens qui sont susceptibles de porter des atteintes graves aux droits fondamentaux, la question des voies de droit doit être reconsidérée et réglée de manière conforme aux exigences de la Constitution et de la CEDH, notamment à l'art. 29a Cst., qui garantit l'accès au juge, et à l'art. 13 CEDH qui garantit le droit à un recours effectif (cf. aussi le commentaire relatif à l'art. 18j).

Al. 1
Cette disposition introduit la possibilité de recourir au Tribunal administratif fédéral contre l'emploi d'un moyen spécial, après la communication prévue à l'art. 18i. Le recours est également possible contre une interdiction fondée sur l'art. 18n, après la notification de celle-ci. Ainsi, l'art. 29a, al. 1, que nous proposons, précise l'art. 32, al. 1, let. a, de la loi sur le Tribunal administratif fédéral (LTAF; FF 2005 3875), en tant qu'il dispose que les actes fondés sur la LMSI constituent des décisions administratives *justiciables*, qui n'entrent pas dans la catégorie des "actes de gouvernement"; ces derniers étant, comme on le sait, en principe exclus du recours au Tribunal administratif fédéral (cf. aussi le commentaire relatif à l'art. 18n).

Dans la mesure où, à l'art. 18i, al. 1, c'est la communication ultérieure de l'office fédéral qui est l'objet du recours devant le Tribunal administratif fédéral, l'attribution au Conseil fédéral de la compétence de décider de l'utilisation de moyens spéciaux de recherche d'informations n'a pas d'influence sur la procédure de recours.

Al. 2
En ce qui concerne le recours contre une décision communiquée conformément à l'art. 18i, al. 1, il se justifie, compte tenu de la particularité des actes ici en cause et de la difficulté qu'il y aurait à reconstituer les faits, de déroger au régime ordinaire prévu à l'art. 49 de la loi fédérale sur la procédure administrative (PA; RS 172.021) et de limiter le motif du recours au grief de la violation du droit (contrôle de la légalité et de la proportionnalité). En revanche, pour les recours contre une décision d'interdiction fondée sur l'art. 18o, une telle dérogation ne se justifie pas et les motifs du recours sont ceux de l'art. 49, al. 2, PA, donc également la constatation inexacte ou incomplète des faits pertinents ainsi que l'inopportunité.

Al. 3
Par souci de clarté, cette disposition rappelle, comme cela se fait dans les autres lois fédérales, que toutes les questions relatives aux droits et aux obligations des particuliers et des autorités, notamment la question des délais de recours, sont régies par les dispositions générales de la procédure fédérale.

2.38 Loi du 17 juin 2005 sur le Tribunal administratif fédéral[5]

L'introduction de l'art. 13b LMSI, qui consacre la compétence du Tribunal administratif fédéral de trancher les différends entre l'office fédéral, d'une part, et les autorités et unités administratives cantonales, les organisations accomplissant des tâches de service public ainsi que les organes de la Confédération qui ne font pas partie de l'administration centrale, d'autre part, nécessite une adaptation de la loi sur le Tribunal administratif fédéral (voir aussi le commentaire de l'art. 13b).

2.39 Code pénal suisse [6], art. 179^octies^ et 317^bis^

*Art. 179^octies^*
La violation du secret de la correspondance par poste ou télécommunication et celle du domaine privé et secret, notamment au moyen d'appareils d'écoute, d'enregistrement ou de prises de vues, constituent des infractions au sens des art. 179 ss CP. L'art. 179^octies^ réserve toutefois le cas des mesures officielles de surveillance exécutées en conformité à la LSCPT.
Il convient dès lors d'adapter cette disposition pénale afin de réserver aussi les nouveaux cas de surveillance autorisés en vertu de la LMSI.

*Art. 317^bis^*
Les faux dans les titres constituent des infractions pénales (cf. art. 251, 252, 255, 317 CP). L'art. 317^bis^ réserve toutefois le cas où de tels faux sont constitués et utilisés pour assurer une identité d'emprunt dans le cadre d'une investigation secrète autorisée par le juge. Il convient dès lors d'adapter cette disposition pénale afin de réserver aussi les nouveaux cas de constitution et d'usage d'identités d'emprunt autorisés en vertu de la LMSI.

2.40 Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM)[7], art. 99, al. 1, 2^e^ phrase, al. 1^bis^ et 2 et art. 99a

*Art. 99, al. 1, 2^e^ phrase, al. 1^bis^*

Al. 1, 2^e^ phrase
La limitation (de principe) de l'exploration radio à des cibles situées à l'étranger prévue à l'art. 99, al. 1, du projet de loi répond à la recommandation n^o^ 1 du rapport du 10 novembre 2003 de la Délégation des Commissions de gestion des Chambres fédérales relatif au projet ONYX. Par exploration radio contre des cibles à l'étranger, on entend le fait de répertorier des rayonnements électromagnétiques à l'étranger. Actuellement, cette opération est effectuée au moyen du système ONYX pour les communications par satellites ou au moyen d'installations de réception en ondes courtes pour ce spectre de fréquences. Les développements techniques détermineront à l'avenir quels moyens et systèmes seront utilisés pour l'exploration radio visant l'étranger. C'est pour cette raison que le législateur a délibérément choisi d'employer la notion générale d'exploration radio.

[5] RO ... (FF 2005 3875)
[6] RS **311.0**
[7] RS **510.10**

*Al. 1^bis^*
Conformément à l'al. 1, 2^e^ phrase, l'exploration radio est dirigée, en principe, contre des cibles à l'étranger. Cela dit, l'armée a toujours des besoins en matière d'exploration radio en Suisse. Etant donné que la réglementation visée à l'al. 1, 2^e^ phrase, a caractère de principe et sachant que toute limitation des droits fondamentaux et du respect de la sphère privée nécessite une base légale formelle, le recours à l'exploration radio en Suisse contre des civils doit être explicitement réglementé. Dès lors, l'al. 1^bis^ prévoit deux cas dans lesquels l'armée est autorisée à recourir, en Suisse, à l'exploration radio contre des civils.

La *let. a* règle la surveillance de fréquences. Ainsi, l'armée doit pouvoir vérifier si des utilisateurs civils utilisent éventuellement les fréquences qui lui sont attribuées. Si nécessaire, elle identifie et filtre les civils qui utilisent ses fréquences. En effet, l'armée doit disposer de ses moyens de communication pour accomplir sa mission, et doit, de ce fait, écarter les utilisateurs civils qui la gênent dans l'exécution de ses tâches.
La *let. b* règle la sauvegarde de la souveraineté sur l'espace aérien. En vertu de l'ordonnance du 23 mars 2005 sur la sauvegarde de la souveraineté sur l'espace aérien (OSS; RS 748.111.1), les Forces aériennes doivent garantir la souveraineté sur l'espace aérien. A ce titre, elles doivent pouvoir capter, au moyen de l'exploration radio, les radiocommunications entre les avions militaires et civils et les stations terriennes (civiles ou militaires). Grâce à cette disposition, il est possible de capter et d'identifier les avions ou autres engins aériens non identifiés, et de déployer, au besoin, les moyens de défense appropriés. De plus, les Forces aériennes ont aussi recours à l'exploration radio pour surveiller l'espace aérien d'une manière générale et pour établir la situation aérienne (art. 5 OSS).

Par ailleurs, l'armée est aussi autorisée à recourir à l'exploration radio contre des cibles civiles en Suisse (ou à l'étranger) dans le cadre de la légitime défense ou de l'état de nécessité, par exemple pour protéger des militaires d'une attaque imminente par des civils. Il s'agit là d'une justification classique qui ne doit pas figurer explicitement dans la LAAM, car ce cas de figure est déjà suffisamment réglé aux art. 25 et 26 du code pénal militaire du 13 juin 1927 (CPM; RS 321.0).

Art. 99a
Conformément à l'art. 164, al. 1, Cst., les règles de droit importantes doivent figurer dans la loi formelle. Tel est le cas du régime de contrôle applicable à l'exploration radio. Or, actuellement, ce régime n'est défini qu'au niveau de l'ordonnance. Il s'agit donc de donner à ce régime une base légale adéquate.

Al. 1
Cette disposition consacre, au niveau de la loi, l'autorité de contrôle indépendante (ACI), dont la base légale se trouve actuellement aux art. 14 ss de l'ordonnance du 15 octobre 2003 sur la conduite de la guerre électronique (OCGE; RS 510.292).

L'ACI ne contrôle en principe que les mandats d'exploration radio qui ne nécessitent pas d'autorisation (unique) spéciale au niveau politique, comme cela est le cas pour les mandats d'exploration radio permanente (p. ex. du Service de renseignement stratégique du DDPS). En outre, une exploration radio à l'étranger (par l'armée) peut aussi être effectuée dans le cadre d'un service de promotion de la paix. Dans de tels cas, la décision parlementaire correspondante inclut l'autorisation pour l'exploration

radio. Etant donné qu'il existe une autorisation des autorités politiques compétentes pour ces cas, l'ACI ne procède pas à une vérification supplémentaire du mandat d'exploration radio.

L'ACI exerce un contrôle portant sur la conformité au droit de l'exploration radio permanente, ce qui implique un contrôle de la proportionnalité de la mesure. En revanche, elle ne se prononce pas sur l'opportunité de celle-ci.

Afin de garantir son indépendance, l'ACI agit, dans l'exercice de son mandat, sans instructions.

Al. 2
Cet alinéa délègue au Conseil fédéral le soin de régler les questions d'organisation concernant cette autorité.

2.41 Loi sur les télécommunications[8], art. 44

L'art. 44 de la loi du 30 avril 1997 sur les télécommunications (LTC) doit être complété car la surveillance de la correspondance par télécommunication n'est désormais plus uniquement régie par la LSCPT, mais aussi par la LMSI.

La surveillance de la correspondance par télécommunication prévue par la LSCPT a lieu dans le cadre d'une procédure pénale de la Confédération ou d'un canton, ou dans le cadre de l'exécution d'une demande d'entraide judiciaire au sens de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (loi sur l'entraide pénale internationale, EIMP; RS 351.1). Les surveillances de la correspondance par poste et télécommunication effectuées sur la base de la LMSI visent à déceler les menaces liées au terrorisme, au service de renseignements politiques ou militaires prohibé, au commerce illicite d'armes et de substances radioactives et au transfert illégal de technologie.

[8] RS **784.10**

3. Conséquences

3.1 Conséquences pour la Confédération

3.1.1 Conséquences financières

Les conséquences financières seront fonction non seulement du type et de l'aménagement des différentes mesures, mais aussi des besoins qui en découleront.

3.1.2 Effets sur l'état du personnel

La mise en œuvre des mesures doit se fonder autant que possible sur les structures existantes de la Confédération (Tribunal administratif fédéral, Service d'analyse et de prévention) et des cantons (services de renseignements cantonaux). Environ 40 postes seront nécessaires pour les tâches exécutées par le Tribunal administratif fédéral et le Service des tâches spéciales (STS) du DETEC (pour la surveillance de la correspondance par poste et télécommunication), et pour la mise en œuvre, aux plans juridique, opérationnel et administratif, des nouveaux moyens de recherche, ainsi que pour le traitement des résultats obtenus auprès de l'Office fédéral de la police. Ces postes devront être compensés en interne au sein du DFJP.
Les postes supplémentaires sont donc pour l'essentiel nécessaires dans les domaines suivants:

- Renforcement des structures opérationnelles, notamment dans les services de police qui se chargeront de rechercher et de traiter les informations (policiers, interprètes, techniciens, analystes opérationnels);
- Renforcement des structures informatiques, notamment dans le domaine de la saisie des données, de l'assurance-qualité et de la correspondance avec l'étranger;
- Renforcement des structures étrangères aux services de renseignements, telles que celles du STS DETEC (chargé des aspects techniques et de l'administration) ou du Tribunal administratif fédéral (chargé du secrétariat).

La mise en œuvre des nouvelles compétences n'entraînera donc que de faibles besoins supplémentaires en ressources.

3.1.3 Autres conséquences

Les autres conséquences relèveront du type et de l'aménagement des mesures.

3.2 Conséquences pour les cantons et les communes

Le niveau de sécurité dans les cantons et les communes s'améliorera. L'accroissement éventuel des obligations de renseigner et de communiquer sera compensé par les diminutions de travail à moyen et long terme (clarifications facilitées, les moyens spéciaux de recherche d'informations remplaceront en partie les observations nécessitant d'importants moyens en termes de personnel et de finances, etc.), qui ne sont pas encore chiffrables au stade actuel. En fonction du type et de l'aménagement des nouvelles mesures, il y aura peut-être un accroissement du volume de travail dans les cantons. C'est pourquoi ceux-ci devront décider, en fonction de la situation, d'augmenter leurs effectifs.

3.3 Conséquences économiques

Les directives du Conseil fédéral du 15 septembre 1999 sur l'exposé des conséquences économiques des projets d'actes législatifs fédéraux (FF 2000 986) prescrivent d'examiner les points suivants:

3.3.1 Nécessité et possibilité d'une intervention de l'Etat

Le projet permet notamment de mettre en œuvre des interventions parlementaires. Le Conseil fédéral a chargé le DFJP de lui soumettre les projets nécessaires aux révisions de lois. Par ailleurs, la Confédération est compétente en la matière.

3.3.2 Impact du projet sur les différents groupes de la société

Les normes proposées contribueront à renforcer la sûreté intérieure et à améliorer ainsi la protection de la population.

3.3.3 Implications pour l'économie dans son ensemble

Il n'y aura pas d'implications directes pour l'économie dans son ensemble. Le contexte rendu plus sûr aura pour effet indirect d'améliorer les conditions générales.

3.3.4 Autres réglementations entrant en ligne de compte

Chaque canton est responsable au premier chef de la sûreté intérieure sur son territoire. Dans la mesure où, aux termes de la Constitution fédérale et de la loi, la Confédération est responsable de la sûreté intérieure, les cantons l'assistent sur les plans de l'administration et de l'exécution. En vertu du droit en vigueur, la Confédération est compétente notamment pour détecter précocement les dangers liés au terrorisme, au service de renseignements prohibé, à l'extrémisme violent, au commerce illicite d'armes et de substances radioactives ainsi qu'au transfert illégal de technologie (non-prolifération). Elle soutient les autorités compétentes de police et de poursuite pénale en leur fournissant des renseignements sur le crime organisé. La Confédération légifère ainsi dans le cadre de son domaine de compétences; aucune autre réglementation n'entre en ligne de compte.

3.3.5 Aspects pratiques de l'exécution

La mise en œuvre du projet interviendra sur la base des structures actuelles des organes de sûreté, lesquelles ont fait leurs preuves. Rien ne change en ce qui concerne le concept global de responsabilité commune de la Confédération et des cantons en matière de protection de l'Etat.

3.4 Autres conséquences

3.4.1 Conséquences sur les relations internationales

La révision de loi proposée n'affecte formellement aucun engagement international. Par ailleurs, l'harmonisation des standards apportera une pierre solide à l'édifice de la coopération internationale.

3.4.2 Conséquences sur l'image de la Suisse

Ce projet, qui vise avant tout à lutter efficacement contre le terrorisme international, aura à long terme un impact positif sur la réputation de la Suisse à l'étranger.

4. Aspects juridiques

4.1 Base constitutionnelle

La LMSI se fonde sur la compétence inhérente de la Confédération en matière de maintien de la sûreté intérieure et extérieure de la Suisse. La présente révision de loi s'inscrit pleinement dans ce cadre, puisqu'elle reste dans les limites des domaines visés à l'art. 2, al. 1 et 2, LMSI. Pour certaines mesures, elle reste même en-deçà du mandat de l'art. 2, dès lors que le projet restreint leur champ d'application aux domaines du terrorisme, du service de renseignements politiques ou militaires prohibé, au commerce illicite d'armes et de substances radioactives ainsi qu'au transfert illégal de technologie et qu'il ne vise ni l'extrémisme violent, ni le renseignement économique prohibé ou le crime organisé.

4.2 Compatibilité avec les droits fondamentaux

Le présent projet de révision de la LMSI prévoit des atteintes possibles à plusieurs droits fondamentaux, tout particulièrement à la protection de la sphère privée (art. 13 Cst.) et à la liberté d'association (art. 23); peuvent aussi être touchées la liberté de conscience et de croyance (art. 15, notamment al. 3), la liberté de réunion (art. 22), la garantie de la propriété (art. 26).

L'art. 36 Cst. dispose que toute restriction d'un droit fondamental doit être fondée sur une base légale, doit être justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui et doit être proportionnée au but visé. Il précise en outre que l'essence des droits fondamentaux est inviolable. Les restrictions de droits fondamentaux sont permises lorsque les biens juridiques concrets de tiers ou de la communauté sont gravement menacés ou violés.

Les moyens et mesures proposés se fondent sur une loi au sens formel, la LMSI. L'intérêt public réside dans la protection de la sûreté intérieure ou extérieure et dans le dépistage précoce des menaces telles que le terrorisme, le service de renseignements politiques et militaires prohibé, le commerce illicite d'armes et de substances radioactives et le transfert illégal de technologie. L'existence d'un intérêt public légitime ne saurait donc être contesté. Quant au caractère proportionné des nouvelles mesures, nous renvoyons aux commentaires relatifs aux différents articles (cf. notamment à ceux relatifs aux art. 13a, 13c, 13d, 18k, 18l, 18m, 18n). Il faut aussi rappeler ici que les différentes cautèles qui accompagnent les nouvelles mesures (cf. les conditions prévues en dernier ressort auxquelles elles sont subordonnées, la procédure de décision garantissant un contrôle a priori des conditions juridiques et politiques, la garantie d'un contrôle judiciaire, etc.) sont autant d'éléments qui mettent en oeuvre le principe de la proportionnalité de l'ingérence étatique. En outre, il ressort clairement des conditions de l'art. 18b, notamment let. c, que les moyens les plus attentatoires aux droits fondamentaux ont un caractère subsidiaire, c'est-à-dire que leur emploi ne doit intervenir qu'en dernier ressort, si les autres moyens, moins contraignants, ne suffisent pas à obtenir le renseignement nécessaire à la prévention d'une menace grave contre la sûreté intérieure ou extérieure ("ultima ratio").

Les moyens et mesures prévus dans le projet sont conformes à la Constitution. La LMSI est destinée à renforcer la sûreté de la Suisse et de ses habitants.

4.3 Compatibilité avec les engagements internationaux de la Suisse

La Suisse, qui est partie à différents accords internationaux en faveur des droits de l'homme et à différentes conventions, est tenue de rendre régulièrement compte aux organes de contrôle internationaux de la mise en œuvre de ses obligations de droit international. A cet égard, l'approbation des moyens et mesures proposés dans le projet constitue également une contribution importante à la lutte contre le terrorisme et d'autres menaces graves pour la sécurité dans le monde, ce qui est propice à la réputation de la Suisse au plan international.

Le présent projet de loi est conforme aussi bien dans ses orientations générales que dans ses dispositions, à la CEDH et au Pacte international du 16 décembre 1966 relatif aux droits civils et politiques (Pacte II; RS 0.103.2).

Rappelons notamment qu'au regard de la CEDH, l'exercice d'un droit fondamental (en l'occurrence, principalement l'art. 8, droit au respect de la vie privée et familiale, et l'art. 11, liberté de réunion et d'association) peut être limité pour autant que l'ingérence de l'Etat soit prévue dans une loi, qu'elle poursuive un but légitime et qu'elle soit nécessaire dans une société démocratique. La présente législation remplit les conditions liées à la notion de loi matérielle au sens de la CEDH. En particulier, les dispositions nouvelles définissent, compte tenu des conditions générales de l'art. 18b et des conditions particulières fixées aux art. 18k à 18n, avec suffisamment de précision la catégorie de personnes visées, les circonstances dans lesquelles les mesures peuvent être prises (cf. art. 18a et 18b), ainsi que les garanties de procédure (art. 18c, 18d et 18i). Quant aux deux autres conditions (but légitime et nécessité dans une société démocratique), leur examen se recoupe avec celui de l'intérêt public et de la proportionnalité dont nous avons parlé ci-dessus.

La protection que le Pacte II garantit, eu égard aux droits fondamentaux dont il est ici question (cf. art. 17 et art. 22 Pacte II), se recoupe avec celle assurée par la CEDH ainsi que par la Constitution fédérale.

Enfin, les moyens proposés sont parfaitement compatibles avec les accords et conventions visant à lutter contre le terrorisme.

5. Annexes

5.1 Annexe 1

Projets législatifs en cours dans le domaine de la sûreté intérieure

Conventions internationales

Titre	**Contenu**	**Point de la situation**	**Recoupements importants avec la présente révision**
Accords bilatéraux en application de l'accord de Schengen	Accords bilatéraux portant sur la mise en œuvre de l'acquis de Schengen	Examen de l'opportunité	non
Europol: déclaration d'intention en vue de l'extension du mandat et modification des prescriptions de classification	Extension du champ d'application à d'autres délits	Projet	non
Europol: Accord de stationnement avec les Pays-Bas	Stationnement d'attachés suisses aux Pays-Bas	Projet	non
Déclaration d'intention CH-RFA relative à la CM06 (protocole d'entente)	Collaboration à la Coupe du monde de football 2006	Signature prévue en mai 2006	non
Accord avec la Slovénie sur la collaboration policière transnationale	Collaboration bilatérale en matière de police	Discussion au Conseil des États	non
Accord avec la Lettonie / Tchéquie sur la collaboration policière transnationale	Collaboration bilatérale en matière de police	Discussion au Conseil national	non
Accord avec l'Albanie / Macédoine / Roumanie sur la collaboration policière transnationale, et adaptation des traités internationaux conclus avec la France et l'Italie, et collaboration avec le Liechtenstein, et traités internationaux avec la Bosnie-Herzégovine / Lettonie / Monténégro / Serbie / Slovénie / Tchéquie / Turquie / Ukraine / États-Unis	Collaboration bilatérale en matière de police	Conseil fédéral: note de discussion sur la stratégie relative à la coopération policière internationale	non

Lois

Titre	Contenu	Point de la situation	Recoupements importants avec la présente révision
Code de procédure pénale suisse	Unification du droit de la procédure pénale suisse	Message	Réglementation des enquêtes policières préalables et de la transmission des informations relatives aux procédures pénales
Loi sur la police	Création des bases légales nécessaires aux organes fédéraux chargés de tâches policières	Avant-projet	Évent. reprise ultérieure de la LMSI dans la LPol
Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)	Lutte préventive contre les actes de violence, notamment lors de manifestations sportives	Adoptée par le Parlement; date de l'entrée en vigueur non définie	oui (subdivision de la loi)
Loi fédérale sur les armes, les accessoires d'armes et les munitions (loi sur les armes)	Amélioration de la prévention des abus, et adaptation à l'accord de Schengen	Commission au Conseil des Etats	non
Loi fédérale sur les systèmes d'information de police de la Confédération	Harmonisation des bases légales formelles relatives aux systèmes d'information de police gérés par la Confédération	Évaluation de la procédure de consultation	non
Loi fédérale sur l'usage de la contrainte dans le cadre du droit des étrangers et des transports de personnes ordonnés par une autorité fédérale	Harmonisation des conditions-cadres concernant l'usage de la contrainte physique, le recours à des moyens tels que l'immobilisation à l'aide de liens ou d'entraves, ainsi que l'emploi des armes	Message	non
Loi fédérale instituant des mesures contre le racisme	Interdiction d'emblèmes racistes, et possibilité de procéder à la surveillance des communications dans le cadre d'une procédure pénale au sens de l'art. 261bis CP	Évaluation de la procédure de consultation	non

Ordonnances

Titre	Contenu	Point de la situation	Recoupements importants avec la présente révision
Ordonnance instituant des mesures visant au maintien de la sûreté intérieure	Mise en œuvre de la LMSI	Projet	non
Ordonnance sur le système de traitement des données relatives à la protection de l'État	Réglementation de l'échange des données avec Europol	Évaluation de la consultation des offices	non
Ordonnance SIRENE	Réglementation des tâches du bureau SIRENE	Projet	non
Ordonnance sur le système informatisé de la Police judiciaire fédérale	Adaptation à Europol	Évaluation de la consultation des offices	non
Ordonnance sur les armes, les accessoires d'armes et les munitions	Adaptation à la loi révisée	Projet	non
Ordonnance SIS	Mise en œuvre de l'art. 351^{decies} CP et réglementation du traitement des données	Projet	non
Ordonnance sur l'exportation, l'importation et le transit des biens utilisables à des fins civiles et militaires et des biens militaires spécifiques	Adaptation à Schengen	Projet	non
Ordonnance sur le matériel de guerre	Adaptation à la loi révisée	Projet	non
Ordonnance concernant l'entrée et la déclaration d'arrivée des étrangers	Adaptation à Schengen	Projet	Bulletin d'arrivée similaire aux actuelles "fiches d'hôtel"
Ordonnance sur le traitement des données signalétiques	Adaptation à Dublin (Eurodac)	Projet	Non
Ordonnance sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police	Adaptation à Europol	Projet	Non

5.2 Annexe 2

Droit comparé (Allemagne, Autriche, France, Italie, Luxembourg, Pays-Bas, UE)

1. Allemagne

La République fédérale d'Allemagne est un État fédéral. Le droit constitutionnel fédéral allemand attribue en principe aux Länder la souveraineté en matière de police sur leur territoire. Parallèlement, la loi fondamentale prévoit des compétences originaires de l'État fédéral dans certains domaines importants concernant la police. C'est notamment le cas en matière de collaboration de l'État fédéral et des Länder pour les affaires de police judiciaire ainsi qu'en matière de lutte internationale contre le crime. En outre, l'État fédéral assure la sécurité aux frontières du pays, ainsi que celle des chemins de fer et du trafic aérien. Pour mener à bien ses tâches, il édicte ses propres lois et dispose de forces de police qui relèvent de sa seule responsabilité. Au vu de cette répartition des compétences, l'Allemagne dispose non seulement des corps de police des seize Länder, mais aussi des autorités de police de l'État fédéral, à savoir l'Office fédéral de la police judiciaire et la Police fédérale. Ces deux entités relèvent de la compétence du ministère fédéral de l'Intérieur.
La tâche principale des autorités de l'État fédéral et des Länder, chargées de défendre la Constitution, consiste à recueillir des informations sur les activités suivantes et à les évaluer: tentatives visant à compromettre l'ordre constitutionnel libéral et démocratique ou susceptibles de porter atteinte à la sécurité, activités des services secrets, actions touchant au champ d'application de la loi relative à la défense de la Constitution (Bundesverfassungsschutzgesetz)[9].
L'État fédéral et les Länder sont tenus de collaborer dans les affaires concernant la défense de la Constitution. L'État fédéral dispose d'un Office fédéral pour la protection de la Constitution (Bundesamt für Verfassungsschutz, BfV), subordonné au ministre de l'Intérieur. Cet office est habilité à se procurer les informations nécessaires à l'accomplissement de ses tâches, et même à utiliser des données personnelles, pour autant que les dispositions de la loi fédérale sur la protection des données ou des règles particulières de la loi relative à la défense de la Constitution ne s'y opposent pas. Il peut également recueillir des données et des informations auprès des autorités chargées de la répression[10]. Inversement, le Service fédéral de renseignement est autorisé à transmettre des informations aux autorités nationales, lorsque cela est indispensable à l'accomplissement de ses tâches ou lorsque les données sont nécessaires à la sécurité publique[11]. Ces données peuvent être utilisées à des fins de poursuites pénales.
Le nouveau centre de lutte contre le terrorisme est entré en fonction en décembre 2004. Le Service fédéral de renseignement, les offices de police judiciaire et de protection de la Constitution des Länder, le Service de protection des frontières

[9] Loi sur la collaboration de l'État fédéral et des Länder en matière de défense de la Constitution et sur l'Office fédéral pour la protection de la Constitution (Bundesverfassungsschutzgesetz; BVerfSchG)
[10] § 18 BVerfSchG
[11] § 9 Loi sur le service de renseignement de l'État fédéral du 20 décembre 1990 (BNDG)

fédérales, l'Office de police judiciaire des douanes (Zollkriminalamt) et le Service de contre-espionnage militaire (Militärischer Abschirmdienst, MAD) collaborent aux travaux de ce centre.

Les activités de l'Office fédéral pour la protection de la Constitution (BfV) sont soumises à la surveillance d'un organe parlementaire de contrôle, qui doit être informé régulièrement sur l'activité générale du BfV et sur les événements d'une importance particulière[12]. Sur demande, le gouvernement fédéral doit accorder à l'organe parlementaire de contrôle le droit de consulter les dossiers et fichiers et l'autoriser à auditionner les collaborateurs du BfV. Ce dernier est tenu de fournir gratuitement à toute personne qui le demande des renseignements sur les données la concernant, pour autant que celle-ci se réfère à un état de fait concret et qu'elle justifie d'un intérêt particulier [13]. Les données enregistrées doivent être rectifiées dans la mesure où elles sont inexactes. Au plus tard après cinq ans, le BfV doit examiner au cas par cas si les données doivent être rectifiées ou effacées. Les données doivent être effacées quinze ans au plus tard après la date de la dernière inscription, à moins que les directeurs administratifs n'en décident autrement[14].

Seules les dispositions du droit fédéral allemand sont commentées ci-dessous.
Pour accomplir ses tâches, le BfV peut, au cas par cas, recueillir des données sur les télécommunications et les prestations effectuées à distance[15]. A cet effet, le président du BfV ou son suppléant doit présenter une demande écrite et motivée au ministère fédéral chargé par le Chancelier fédéral de se prononcer sur ce genre d'affaires. Ce ministère informe chaque mois la commission G 10 sur les demandes légitimes avant d'y donner suite. S'il y a péril en la demeure, le ministère fédéral peut ordonner que sa décision soit exécutée avant même que la commission en ait été informée[16]. Le ministère fédéral compétent renseigne l'organe parlementaire de contrôle (PKGr) au moins tous les six mois sur le déroulement des recherches d'informations. En outre, le BfV est habilité à recourir à des personnes de confiance ou à des agents infiltrés. Il peut également procéder à des observations, à des prises d'images et de son (écoutes de logements privés) et utiliser des identités d'emprunt ainsi que des signes conventionnels de camouflage[17]. Ces mesures doivent être décrites dans un règlement de service qui est également soumis à l'approbation du ministre de l'Intérieur. Ce dernier informe l'organe de contrôle parlementaire. Si des renseignements sont demandés à la personne concernée, celle-ci doit être informée des motifs de l'enquête.
Par ailleurs, le BfV est autorisé, à certaines conditions, à prendre des renseignements auprès des banques[18]. Lorsqu'il recherche des informations sur les moyens de communication de groupes terroristes, le BfV peut aussi demander aux fournisseurs de prestations des services postaux des renseignements, tels que les noms, les adresses et les indications relatives aux cases postales et aux télécommunications (identification, numéros de téléphone, données et localisation)[19]. Enfin, le BfV a le droit d'utiliser des dispositifs récepteurs de l'identité internationale de la station mobile (IMSI-catcher) afin d'identifier des appareils et des numéros de

[12] § 2 Loi sur le contrôle parlementaire de l'activité de renseignement de l'État fédéral
[13] § 15 BVerfSchG
[14] § 12 BVerfSchG
[15] § 8 al. 8 BVerfSchG.
[16] § 8 al. 9 BVerfSchG
[17] § 8 al. 2 BVerfSchG
[18] § 8 al. 5 BVerfSchG
[19] § 8 al. 6 BVerfSchG et § 8 al. 8 BVerfSchG

carte de téléphone mobiles[20]. Les conditions applicables sont identiques à celles prévues pour les écoutes téléphoniques.
Par contre, les autorités allemandes de protection de la Constitution n'ont aucune compétence policière. Elles ne sont pas autorisées à procéder à des perquisitions, ni à confisquer des objets.

2. Autriche

Le système étatique autrichien est organisé de manière fédéraliste. Son ordre juridique fait en principe une différence entre le domaine de la répression et celui de la prévention. L'Office fédéral pour la protection de la Constitution et la lutte contre le terrorisme (BVT) exerce la fonction de service de renseignement civil en Autriche[21]. Sa tâche consiste essentiellement à protéger l'État et ses institutions constitutionnelles, en luttant contre le terrorisme international, les mouvements extrémistes, l'espionnage, le trafic international d'armes et de matériel nucléaire, ainsi que la criminalité organisée dans ces divers domaines. Le BVT fait partie de la Direction générale pour la sécurité publique du Département fédéral de l'intérieur.
Cet office se compose d'une direction administrative et de trois divisions. La division 1 est responsable des affaires de personnel, de la formation, du budget et des questions économiques. Elle s'occupe également de toutes les questions juridiques fondamentales touchant à la protection de l'État.
La plus grande unité d'organisation du BVT est la 2^{e} division (recherche d'informations, analyse et enquête). Elle comprend cinq sections (extrémisme, terrorisme et extrémisme d'origine étrangère, contre-espionnage, prolifération des armes de destruction massive et trafic d'armes, analyse stratégique et soutien opérationnel) et coordonne sur l'ensemble du territoire l'activité des offices pour la protection de la Constitution et la lutte contre le terrorisme des neuf Länder (LVT) dans les affaires touchant à la protection de l'État.
La 3^{e} division organise et coordonne, sur l'ensemble du territoire, les mesures de protection des personnes et des objets et elle évalue régulièrement si les mesures prises en matière de sécurité sont adaptées à des menaces potentielles. Elle procède également à des contrôles de sécurité.

Pour accomplir ses tâches de défense de la Constitution, chaque Land dispose d'un Office pour la protection de la Constitution et la lutte contre le terrorisme (LVT), subordonné à la Direction de la sécurité. Par ailleurs, il incombe à l'Office fédéral (BVT) d'organiser et de coordonner, par l'intermédiaire des offices des Länder (LVT) la mise en œuvre des mesures de protection des personnes et des choses ainsi que de veiller à la sécurité des représentants d'États étrangers, d'organisations internationales et d'autres sujets de droit international.
Les autorités chargées de la protection de l'État ont accès aux données des autorités chargées de la répression. Ces dernières leur transmettent leurs informations. Les personnes concernées ont le droit d'avoir connaissance des données personnelles enregistrées à leur sujet. Elles peuvent en demander la rectification ou la destruction et interjeter recours auprès de la Commission de protection des données. Ces renseignements peuvent leur être refusés si des intérêts inhérents à la protection de l'État l'exigent.

[20] § 9 al. 4 BVerfSchG
[21] Loi fédérale sur l'organisation de la sécurité et l'activité de la police administrative du 31 octobre 1992 (Sicherheitspolizeigesetz; SPG)

Les autorités de sûreté, qui procèdent à des investigations étendues en matière de risques, doivent communiquer sans délai au ministère fédéral de l'Intérieur les mesures qu'elles ont prises. Si le délégué à la protection juridique (*Rechtsschutzbeauftragter*) le demande, le Ministère doit lui donner l'occasion de se prononcer sur ces mesures.
Lorsque le délégué à la protection juridique constate que des données personnelles ont été utilisées à l'insu des intéressés et en violation de leurs droits, il est autorisé à les en informer. Si, pour quelque raison que ce soit, il ne lui est pas possible de leur communiquer cette information, il est habilité à interjeter recours auprès de la Commission de protection des données.
Le délégué à la protection juridique adresse un rapport annuel au ministre fédéral de l'Intérieur sur les activités déployées dans le cadre des investigations étendues en matière de risques (observation de groupes de personnes)[22]. Si le sous-comité permanent du Conseil national demande à consulter ce rapport, le ministre doit le lui remettre.

Les autorités de protection de l'État sont autorisées, à certaines conditions, à demander des renseignements aux exploitants de services publics de télécommunication. Seules les autorités chargées de la répression peuvent ordonner la surveillance du courrier et des télécommunications. Il est possible de mener des investigations secrètes, accompagnées d'un enregistrement sonore[23]. Toutefois, il n'est pas permis de procéder à un enregistrement sonore en l'absence de l'agent infiltré. Le délégué à la protection juridique est chargé de contrôler le suivi de l'investigation secrète et de l'utilisation dissimulée d'appareils de prise de vue ou de son. Le délégué à la protection juridique doit être informé de ce genre d'investigations et des motifs qui les justifient en substance, dans la mesure où l'identité des intéressés est connue. Par ailleurs, les autorités de protection de l'État peuvent saisir séquestrer et confisquer des objets[24], observer des locaux privés[25] et y pénétrer[26], ordonner des interrogatoires et y procéder[27]. Dans certains cas, les intermédiaires financiers sont tenus de fournir des renseignements aux autorités compétentes[28].

Selon l'art. 52a B-VG, l'activité du BTV est soumise au contrôle parlementaire. Après avoir épuisé les voies de droit administratives, il est possible d'interjeter recours auprès de la Cour du tribunal constitutionnel ou administratif.

Même en Autriche, le 11 septembre 2001 n'est pas resté sans conséquences. Les structures ont été renforcées et les dispositions légales se sont durcies. Dans la foulée, les autorités de protection de l'État ont obtenu des compétences plus étendues.

Depuis l'entrée en vigueur, en 2002, de la nouvelle loi sur la police administrative, la protection des personnes susceptibles de fournir des renseignements sur une attaque dangereuse ou une association criminelle s'étend aussi aux proches de ces

[22] § 21 al. 3 SPG
[23] § 54 SPG
[24] § 42 SPG
[25] § 54 al. 2 SPG
[26] § 39 SPG
[27] § 28a SPG
[28] § 38 Loi sur les banques (BWG)

personnes. Les bases légales relatives au camouflage des mesures de soutien utilisées lors d'opérations d'observation ou d'investigation secrète ont également été modifiées. Au vu de l'évolution survenue dans les milieux extrémistes, des dispositions concernant les investigations étendues en matière de risques, ainsi que des règles de protection juridique y relatives, ont été ancrées dans la loi (SPG) le 1er octobre 2000 [29]. Ces dispositions permettent désormais aux autorités de sûreté d'observer des groupements, dès lors que l'on peut s'attendre à ce que cela dégénère en actes criminels, entraînant un grave danger pour la sécurité publique. Auparavant, les autorités de sûreté n'étaient autorisées à observer des groupements extrémistes que s'ils avaient déjà eu un comportement criminel.

Le 1er décembre 2002, l'Office fédéral pour la protection de la Constitution et la lutte contre le terrorisme (BVT) a été intégré à la section II du ministère fédéral de l'Intérieur[30]. Il est directement subordonné au directeur général de la sécurité publique. Cet office exerce son activité dans le cadre de la loi sur la police administrative (SPG) et, lorsqu'il agit au service de la justice pénale, il est lié par les dispositions du code de procédure pénale (StPO).

3. France

La France est une démocratie organisée de manière centralisée. Contrairement aux cantons suisses, les 26 régions ne disposent d'aucune autonomie.
Le premier ministre est directement compétent en matière de sécurité intérieure. Il est assisté dans cette tâche par le Secrétariat général de la défense nationale (SGDN) et par un cabinet de militaires. Divers services étatiques sont en charge de la sécurité intérieure. Il n'y a de ce fait pas de véritable séparation entre la prévention et la répression.

La France dispose de deux services de sécurité indépendants: la police et la Gendarmerie nationale. La gendarmerie est compétente pour les régions rurales et la police s'occupe des villes. La Gendarmerie mobile veille au maintien de l'ordre public et elle est chargée de la lutte contre le terrorisme, le crime organisé et les sectes. La police nationale est subordonnée au ministère de l'Intérieur et elle est dirigée par la Direction générale de la police nationale (DGPN). Elle comprend de nombreuses sous-directions, comme par exemple la Direction de la surveillance du territoire (DST), la Direction centrale des renseignements généraux (RG) et l'Unité de coordination de la lutte antiterroriste.
La DST assume la fonction de service de renseignement et sa tâche consiste à lutter contre les crimes visant la sécurité de l'État[31]. Son organisation et ses fonctions sont réglées de manière détaillée dans un décret du 8 mars 1993 (classé secret). En tant que service central, la DST collecte et traite toutes les informations qui lui sont transmises par les RG, puis les communique au ministère. Elle participe en outre à la protection de domaines sensibles et de secrets relatifs à la défense du territoire. Les RG exploitent un système d'information auquel la DST a également accès [32].L'Unité de coordination de la lutte antiterroriste coordonne les travaux de tous les services mobilisés dans le pays et à l'étranger.

[29] §§ 21 al. 3, 53 al. 1 ch. 2a, 54 al. 2 et 62a SPG
[30] § 7 al. 1 et 9 de la loi sur les ministères fédéraux (Bundesministeriengesetz)
[31] Décret n° 82-1100 du 22 décembre 1982, actualisé le 15 septembre 2004
[32] Décrets n° 91-1052 et n° 91-1051

Le SGDN est une autorité interministérielle, responsable notamment de la sécurité des systèmes d'information, de la défense préventive contre le terrorisme, de la protection des structures de direction et de communication du gouvernement, de la lutte contre la prolifération des armes nucléaires et de la surveillance des exportations de matériel de guerre.
Par contre, la Direction générale de la sécurité extérieure (DGSE), en tant que service secret à l'étranger, est compétente en matière de sécurité extérieure de la France. Elle est subordonnée au Premier Ministre et elle accomplit des tâches d'intervention et de collecte d'informations.
Le droit de regard dans les systèmes d'information des RG est en principe régi par la procédure dite indirecte[33]. La demande de consultation des données doit être présentée à la Commission nationale de l'information et des libertés (CNIL). Cette commission indépendante vérifie les informations et informe l'intéressé des éventuelles rectifications effectuées. Les données peuvent être communiquées à l'intéressé si la sécurité intérieure n'est pas compromise. Lorsque la base de données contient des informations dont la transmission à l'intéressé ne compromet pas le but même de la base de données, le responsable de la base de données peut les communiquer directement à l'intéressé.
Des surveillances téléphoniques peuvent être ordonnées à titre préventif dans l'intérêt de la sécurité intérieure, de la protection économique de la France, de la prévention du terrorisme et de la lutte contre la criminalité organisée ainsi qu'à l'encontre de groupements illégaux[34]. Selon l'art. 4 de la Loi du 10 juillet 1991, l'autorisation est accordée par décret du Premier Ministre ou par deux personnes qu'il a lui-même désignées, sur proposition du ministre de la Défense, du ministre de l'Intérieur et du ministre des Douanes, ou de leurs suppléants. Le nombre de mesures ordonnées et exécutables simultanément est limité par des contingents définis par le Premier Ministre et dont la surveillance incombe à la Commission nationale de contrôle des interceptions de sécurité, indépendante de l'administration[35]. Cette commission est composée d'un président, élu par le Président de la République pour une durée de six ans, ainsi que d'autres personnes. L'autorisation est accordée pour une période de quatre mois au maximum et elle peut être prolongée de quatre mois aux mêmes conditions. Les résultats de la surveillance doivent être détruits au plus tard dix jours après la fin de l'opération, sous la surveillance du Premier Ministre.
Selon la Commission, toutes les informations relatives aux écoutes préventives doivent être classées "secret-défense". Cela signifie par exemple que les personnes mises sur écoute à titre préventif ne doivent pas en être informées, car cela pourrait causer de graves dommages à la défense nationale. En revanche, les autorités de protection de l'État ne sont pas autorisées à surveiller le trafic postal.
Par ailleurs, lorsque la sécurité intérieure l'exige, des confiscations peuvent être effectuées et des objets de valeur immobilisés dans des cas exceptionnels, par décret motivé[36]. Il est permis de procéder à des interrogatoires, ainsi qu'à des perquisitions de véhicules et de domicile, sans examen judiciaire[37]. S'agissant de criminalité organisée, les interventions sont également autorisées pendant la nuit.

[33] Loi pour la sécurité intérieure (Loi n° 2003-239 du 18 mars 2003; ci-après Loi du 18 mars 2003)
[34] Art. 3 de la Loi n° 91-646 du 10 juillet 1991 (Loi relative au secret des correspondances émises par la voie des télécommunications; ci-après Loi du 10 juillet 1991)
[35] Art. 5 de la Loi du 10 juillet 1991
[36] Art. 3 de la Loi du 18 mars 2003 et Loi n° 2005-750 du 4 juillet 2005 (Loi n° 2005-750)
[37] Loi n° 2004-204 du 9 mars 2004 (ci-après Loi du 9 mars 2004)

La Loi du 18 mars 2003 a introduit diverses compétences en ce qui concerne les investigations secrètes (prises d'images et de son, identités d'emprunt et signes conventionnels de camouflage. Elle a notamment permis l'accès direct aux systèmes d'information et les demandes de renseignements auprès de banques ou de particuliers. Dans certaines circonstances, des interdictions peuvent être prononcées, notamment à l'encontre de manifestations armées ou d'organisations qui compromettent la sécurité du pays[38]. Le recours à des agents infiltrés est prévu pour la lutte contre le crime organisé et le Procureur doit en être informé ultérieurement. Ils sont rémunérés grâce à des fonds spéciaux[39].
La France ne dispose pas d'un système de contrôle parlementaire, mais divers projets législatifs allant dans ce sens sont en cours. En attendant, le gouvernement doit rédiger des rapports rendant compte de ces activités, à l'intention du Parlement.
En France aussi, la lutte antiterroriste constitue une priorité absolue depuis les attentats du 11 septembre 2001. Bien que la France dispose notamment d'une longue expérience en la matière, elle a adopté toute une série de nouvelles lois et décrets.

4. Italie

Contrairement aux États fédéraux tels que la Suisse, l'Allemagne ou l'Autriche, l'Italie est un État unitaire décentralisé. Les régions disposent de vastes compétences dans des domaines spécifiques, comme l'agriculture, la santé, la formation et la surveillance de la police municipale.
En Italie, le maintien de la sécurité intérieure et extérieure repose sur trois piliers: le SISMI (Servizio per le informazioni e la sicurezza militare), le SISDE (Servizio per le informazioni e la sicurezza democratica) et la DIA (Direzione Investigativa Antimafia). Ces services relèvent de la compétence du ministère de l'Intérieur, auquel la "Direzione centrale per la Polizia di Prevenzione" est également subordonnée[40].
La Police de prévention poursuit les objectifs suivants: lutte contre les organisations terroristes, tant à l'intérieur du pays qu'à l'étranger, et contre les groupes paramilitaires et violents. Conformément à l'art. 6 de la Loi 121, il est permis de classifier des données, de les analyser et de les évaluer, afin de garantir la sécurité.
Le SISMI s'occupe des affaires qui ont lieu à l'étranger et le SISDE est compétent pour les affaires intérieures. Les tâches du SISDE consistent à combattre le terrorisme, l'immigration illégale, la criminalité informatique, l'espionnage économique, la survenance de nouvelles menaces et la criminalité organisée.
Le SISDE recueille des données pour la protection de la sécurité intérieure. En général, il existe un droit de regard[41]. Toutes les pièces et documents dont la publication pourrait compromettre la sécurité de l'État sont toutefois soumis au secret d'État[42]. Le préposé à la protection des données (Garante per la protezione dei dati personali) exerce son contrôle sur l'ensemble des données récoltées. Les autorités de protection de l'État collaborent avec la police judiciaire en ce qui concerne la sécurité informatique.

[38] Loi du 10 janvier 1936
[39] Loi du 9 mars 2004
[40] Loi n° 121 de 1981 "Nuovo ordinamento dell'Amministrazione della pubblica sicurezza"; ci-après Loi 121
[41] Décret législatif n° 196 du 30 juin 2003, ci-après Décret 196
[42] Art. 12 de la Loi du 24 octobre 1997

Les activités du SISMI et du SISDE sont surveillées par une commission parlementaire. Chaque semestre, le gouvernement doit remettre au Parlement un rapport portant sur les activités de ces services. Les activités des services de renseignement sont également soumises au contrôle de la justice.
La "Direzione Investigativa Antimafia" (DIA) prend des mesures contre la criminalité organisée. Elle organise des surveillances, procède à des écoutes téléphoniques et mène des enquêtes contre la mafia.[43] Elle peut se procurer des informations relatives à la situation financière des personnes soupçonnées d'appartenir à des organisations criminelles. La DIA transmet au SISDE et au SISMI les informations qu'elle a recueillies. Par ailleurs, la DIA travaille en collaboration avec les forces de police.
En principe, les données ne peuvent être traitées qu'avec l'accord de la personne concernée, sauf si le traitement des données est effectué sur la base d'un mandat légal[44].
Le décret-loi du 27 juillet 2005 donne aux autorités de protection de l'État toute une série de nouvelles compétences et de mesures supplémentaires[45]. Désormais, les écoutes téléphoniques préventives sont autorisées en présence d'un soupçon fondé de terrorisme ou de mise en danger de l'ordre étatique. En général, la demande motivée doit être déposée préalablement par le Premier Ministre. Celui-ci peut déléguer ses compétences aux services de renseignement. L'autorisation est accordée par le juge, avec l'approbation du Ministère public. S'il y a péril en la demeure, les mesures peuvent être ordonnées, même à défaut d'autorisation du juge. L'autorisation doit alors être demandée au juge dans les 24 heures selon la procédure ordinaire. Le juge dispose de 48 heures pour statuer sur la demande. Si ce délai ne peut être respecté, les résultats des mesures prises ne seront pas utilisables devant les tribunaux.
La Loi 675, dont la durée est limitée à fin décembre 2007, oblige en outre les sociétés de télécommunications et les fournisseurs d'accès à Internet à conserver les données relatives aux téléphones et à Internet. Désormais, les autorités de protection de l'État peuvent également procéder à l'audition de prisonniers en l'absence de leur avocat (colloquio investigativo), alors que cette mesure était jusqu'ici réservée aux délits de la mafia.
L'expulsion facilitée de suspects qui constituent une menace pour la sécurité publique ou qui soutiennent de quelque manière que ce soit une organisation terroriste a aussi été ancrée dans la loi. L'expulsion est exécutée sans délai, mais elle peut être contestée devant le Tribunal administratif. Lorsque la décision d'expulsion se fonde sur des sources émanant des services secrets, la tenue des débats peut être différée pendant deux ans. La décision d'expulsion peut être suspendue si l'intéressé collabore avec les autorités. Si sa coopération s'avère déterminante dans une enquête sur le terrorisme, il est possible de lui octroyer un permis d'établissement. En cas d'abus, ce permis d'établissement peut lui être retiré.
Enfin, la Loi du 27 juillet 2005 permet au ministère de l'Intérieur de créer des unités de lutte contre le terrorisme, composées de plusieurs forces de police (unità investigative interforze).

5. Luxembourg

[43] Loi n° 410 de 1991; ci-après Loi 410
[44] Art. 12 al. 1 de la Loi n° 675 du 31 décembre 1996 "Tutella delle persone e di altri soggetti rispetto al trattamento dei dati personali", ci-après Loi 675
[45] Texte du décret-loi n° 144 du 27 juillet 2005, coordonné par la loi de conversion du 31 juillet 2005 (ci-après Loi du 27 juillet 2005)

Le Luxembourg est une monarchie constitutionnelle sous forme de démocratie parlementaire. Il se compose de trois districts comprenant douze cantons et 118 communes. Le pouvoir exécutif appartient au Grand-Duc et au gouvernement. Ce dernier est composé comme suit: le Premier Ministre, douze ministres, un ministre délégué et une secrétaire d'État.
Au Luxembourg, trois institutions sont chargées de la protection préventive de l'État: le Service de renseignement de l'État (SRDE), autorité civile compétente en matière de sécurité intérieure, puis le Haut commissariat de la sécurité extérieure (HCSE), en charge de la sécurité extérieure, et enfin le Service de renseignement militaire[46]. Le SRDE est subordonné au ministère de l'Intérieur.
Le champ d'activité du SRDE comprend deux volets. D'une part, il lui appartient de lutter contre le terrorisme, l'espionnage et la prolifération d'armes non conventionnelles ainsi que les technologies y relatives, de même que la criminalité organisée dans les domaines qui relèvent de sa compétence. D'autre part, il s'occupe de toutes les activités susceptibles de compromettre l'intégrité, la souveraineté et l'indépendance du pays, la sécurité des institutions et le fonctionnement de l'État ou la sécurité du peuple[47]. Dans le cadre de ses attributions, le SRDE collabore, d'une part, avec les autorités policières, judiciaires et administratives et, d'autre part, avec le HCSE. La police, les autorités judiciaires et l'administration sont, quant à elles, tenues de transmettre au SRDE les informations prévues à l'art. 2 de la Loi d'organisation du 15 juin 2004.

Le traitement de données personnelles par le SRDE est régi par les dispositions de la Loi du 2 août 2002[48]. Le SRDE a accès à un nombre limité de bases de données, à savoir la base de données générale de la police, celle de la Police des étrangers et celle de la circulation[49]. La surveillance de ses activités incombe au Procureur général ou à l'un de ses délégués ainsi qu'à deux représentants d'une commission spéciale, nommés par le Ministre. Ces personnes ont accès aux données traitées par le SRDE. Elles procèdent aux rectifications nécessaires et informent les personnes concernées qu'elles ont traité conformément à la loi des informations à leur sujet.

Lorsqu'il s'agit d'affaires relatives à la criminalité organisée et à la sécurité extérieure, le Président du gouvernement peut, sur demande du SRDE, ordonner des écoutes téléphoniques préventives, avec l'accord d'une commission spéciale[50]. La surveillance doit être interrompue après trois mois, mais elle peut être prolongée de trois mois en trois mois. Les résultats obtenus lors de surveillances téléphoniques ne sont pas utilisables devant un tribunal, si la personne concernée est tenue au secret professionnel au sens de l'art. 458 du Code pénal et qu'elle n'est pas soupçonnée d'avoir commis d'acte répréhensible ou d'en planifier. Dans ce cas, le chef du SRDE doit détruire immédiatement les documents en question. Les décisions de la Commission doivent être transmises au directeur des services de télécommunication, qui charge alors un service prévu à cet effet de procéder aux écoutes téléphoniques et de les contrôler. Une fois la surveillance terminée, les intéressés reçoivent copie

[46] 2e Bureau de l'armée
[47] Loi du 15 juin portant organisation du Service de Renseignement de l'État (ci-après Loi d'organisation du 15 juin 2004)
[48] Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après Loi du 2 août 2002)
[49] Art. 4 de la Loi d'organisation du 15 juin 2004
[50] Art. 88-3 du Code pénal et selon la Loi du 26 novembre 1982

des résultats obtenus, pour autant que ceux-ci ne soient pas classés secrets. Si aucun résultat n'est obtenu pendant la période prévue, tous les documents doivent être détruits. Dans le cas contraire, ils ne seront détruits qu'à la fin de la procédure.

Les activités du SRDE sont soumises au contrôle de la Commission, composée des présidents des groupes politiques représentés à la Chambre des députés. Le directeur du Service de renseignement donne des informations sur les activités générales de son service. La Commission peut demander à consulter les dossiers et auditionner les agents chargés des enquêtes. Elle approuve un rapport final confidentiel, adressé au Premier Ministre, au chef du Service de renseignement et aux députés de la Commission de contrôle. Ce rapport contient également des observations, des conclusions et des recommandations. La Commission parlementaire de contrôle est informée tous les six mois sur les mesures prises dans le cadre des écoutes téléphoniques préventives.

Il n'est pas possible de procéder à des confiscations ou à des perquisitions, ni à des interrogatoires. Le Premier Ministre peut ordonner la surveillance de toutes sortes de communications à l'aide des moyens techniques appropriés, lorsqu'il soupçonne que la sécurité de l'État est compromise[51]. Les informations récoltées de cette façon ne peuvent être transmises aux services compétents que dans une mesure limitée. Seuls le nom, le prénom et, le cas échéant, l'adresse IP de l'intéressé peuvent leur être communiqués[52]. Les autorités ne peuvent pas prononcer d'interdiction à cet égard.

6. Pays-Bas

Les Pays-Bas sont une monarchie constitutionnelle. La reine est membre du gouvernement et elle nomme les ministres. Le Parlement est composé de deux chambres. La deuxième chambre constitue le Parlement au sens propre, en tant que représentant du peuple et organe de contrôle du gouvernement.
Les institutions suivantes font partie du Service de renseignement néerlandais: le service de renseignement civil (AIVD)[53], le Service de renseignement militaire, qui comprend le Service de renseignement militaire proprement dit (MIVD)[54], le Service spécial de la maréchaussée (BD)[55] et enfin le Service antiterroriste[56]. Depuis les attentats du 11 septembre 2001, la collaboration entre le Service de renseignement civil (AIVD) et la police s'est fortement intensifiée.
La lutte contre le terrorisme constitue l'un des principaux objectifs de l'AIVD.
L'AIVD et le MIVD procèdent à des investigations et à des contrôles de sécurité et ils prennent des mesures à l'encontre des personnes et des organisations soupçonnées de représenter un danger pour la sécurité, l'ordre démocratique ou d'autres intérêts essentiels de l'État[57]. Ils collaborent avec la police et les autorités de poursuite

[51] Art. 88-3 du Code de procédure criminelle
[52] Loi du 30 mai 2005 relative à la protection de la personne à l'égard du traitement de données à caractère personnel dans le secteur de communications électroniques
[53] „Algemene Inlichtingen- en Veiligheidsdienst " (General Intelligence and Security Service)
[54] „Inlichtingen- en Veiligheidsdienst" (Military Intelligence and Security Service)
[55] „Koninklijke Marechaussee, Bijzondere Dienst en Veiligheid" (Military policeSpecial section for intelligence and security)
[56] („Bijzondere Bijstands Eenheid" (Special Help Union Anti-Terrorist Service).
[57] „Act of 7 February 2002, providing for rule s relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002)"

pénale, par l'intermédiaire du Ministère public, en leur remettant des informations sous forme de rapport. L'AIVD est habilité à recourir aux services de la maréchaussée et du Service régional de renseignement (RID).
En principe, un droit de regard étendu est accordé, sur demande, aux personnes qui font l'objet d'un enregistrement de données les concernant. Toutefois, la source des données est protégée. Le droit de consulter les données est restreint dans la mesure où leur communication compromettrait la sécurité intérieure. La commission chargée de la surveillance doit être informée lorsqu'il n'est pas entré en matière sur une demande[58]. Cette commission surveille l'activité des services et en rend compte aux ministres compétents.
L'AIVD et le MIVD sont autorisés à surveiller les télécommunications et le trafic postal, à titre préventif. La demande à cet effet doit être présentée à l'avance par le chef de l'AIVD et du MIVD, avec l'autorisation du ministre de la Défense et l'approbation du ministre de l'Intérieur. S'il y a péril en la demeure, l'autorisation peut être accordée ultérieurement, à condition qu'elle soit demandée aussi vite que possible.
En outre, les services de renseignement peuvent procéder à des observations en recourant à des moyens techniques, avec l'autorisation écrite du ministre compétent. L'observation et la perquisition de locaux privés sont autorisées, d'entente avec le ministre de l'Intérieur ou le chef des services concernés. Lors de certaines opérations, l'utilisation d'identités d'emprunt est également prévue et cela permet d'ouvrir le courrier de tierces personnes, pour autant que le tribunal régional de La Haye accède à la demande du chef desdits services. Il est également permis de s'introduire dans des systèmes informatiques, avec l'accord du ministre de l'Intérieur ou du chef des services. Par contre, il n'existe pas de réglementation expresse en ce qui concerne la saisie, le séquestre et la confiscation d'objets. Il n'y a pas non plus de dispositions permettant d'interdire à des particuliers ou à des organisations d'exercer leur activité.
L'ombudsman national, indépendant du gouvernement, est notamment chargé de surveiller l'activité de ces services. Toutefois, son champ d'influence dans ce domaine a encore été restreint lors d'une révision de la loi[59]. Les documents des services peuvent être consultés, mais il n'est pas permis d'en faire des copies.
Le ministre compétent informe régulièrement la Commission de surveillance parlementaire sur les activités des services.

7. UE

Depuis les attentats du 11 septembre 2001, l'UE poursuit une politique ciblée en matière de lutte contre le terrorisme. Après les attentats à la bombe perpétrés à Londres, l'UE a organisé une réunion au sommet des ministres européens de l'intérieur et de la justice, qui a eu lieu à Bruxelles. À cette occasion, elle s'est prononcée en faveur d'une collaboration plus étroite des 25 pays membres dans la lutte contre le terrorisme et elle a préconisé une amélioration de la collaboration transnationale entre la police et les services secrets.
Le 21 septembre 2005, la Commission de l'UE a présenté un catalogue de mesures exhaustif, comprenant quatre points:
- elle a proposé une directive relative à la conservation des données de transmission par les fournisseurs d'accès.

[58] Supervisory committee
[59] „Act of 3 February 2005“

Cette proposition vise à harmoniser les obligations des fournisseurs de services publics de communication électronique et celle des exploitants d'un réseau de communication public, en introduisant des délais de stockage d'une année pour les données provenant d'un téléphone fixe ou mobile, et de six mois pour les données concernant l'utilisation d'Internet.
- elle a adopté un crédit de 7 millions d'euros pour un projet pilote relatif à la prévention d'attentats terroristes, ainsi qu'à la capacité de défense et de réaction dans ce domaine.
Ce crédit doit servir à créer un réseau entre les diverses autorités pénales, afin de faciliter l'échange d'informations et la gestion des situations de crise. Il permettra également de soutenir le programme européen pour la protection des infrastructures sensibles, déjà prévu auparavant.
- elle a proposé au Conseil de signer la Convention 198 du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme.
Cette proposition incite les 46 pays membres à introduire des prescriptions en matière de blanchiment, aussi sévères que celles déjà en vigueur dans l'UE, de manière à former un front uni dans la lutte contre le financement du terrorisme.
- elle a rédigé une communication intitulée "Le recrutement des groupes terroristes: combattre les facteurs qui contribuent à la radicalisation violente".
Cette communication constitue la contribution de la Commission, prévue en la matière par le plan d'action de La Haye. Le Conseil doit élaborer une stratégie d'ici à la fin de l'année. Cette communication envisage les solutions possibles, afin d'aborder efficacement cette question dans différents domaines, tels que Internet, la collaboration entre les autorités de poursuite pénale et les services secrets des pays membres, ainsi que les relations extérieures.