07.057

Message relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) (Moyens spéciaux de recherche d'informations)

du 15 juin 2007

Madame la Présidente,
Monsieur le Président,
Mesdames et Messieurs,

Par le présent message, nous avons l'honneur de vous soumettre, en vous proposant de l'adopter, le projet de révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure.

Nous vous prions d'agréer, Madame la Présidente, Monsieur le Président, Mesdames et Messieurs, l'assurance de notre haute considération.

15 juin 2007

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Micheline Calmy-Rey
La chancelière de la Confédération, Annemarie Huber-Hotz

Aperçu

La loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS 120*) est entrée en vigueur le 1er juillet 1998. Elle vise à assurer le respect des fondements démocratiques et constitutionnels de la Suisse ainsi qu'à protéger les libertés de sa population.*

Afin de détecter à temps les dangers qui pèsent sur la sûreté de la Suisse, il est nécessaire d'évaluer en permanence la situation de la menace. Le Conseil fédéral et le Parlement, tout comme les cantons, doivent être en mesure de détecter précocement les menaces pesant sur l'existence du pays, de les intégrer dans leur politique de sécurité et de prendre en temps voulu des mesures en vue de les contrer. La première tâche de la protection préventive de l'Etat est de mettre à disposition, en temps opportun, les informations nécessaires à cet effet (rapport sur la politique de sécurité de la Suisse 2000; RAPOLSEC 2000, pp. 33 et 55).

Or une analyse des risques ne peut être établie sans avoir à disposition des informations variées et un réseau d'informations solide. La recherche d'informations pertinentes en matière de sécurité relève des services de renseignements. A ce titre, le Service d'analyse et de prévention (SAP) de l'Office fédéral de la police est chargé de rechercher les informations concernant la Suisse. L'une de ses tâches est de 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 et au transfert illégal de technologie (prolifération). Des informations confidentielles doivent également être réunies pour ce faire.

La situation de la menace en Suisse s'est constamment dégradée au cours des dernières années, notamment en raison de la probabilité plus forte que des attentats terroristes islamistes soient commis. Depuis un certain temps, les besoins en renseignements ne peuvent plus être satisfaits; les informations pouvant être réunies ne permettent plus d'évaluer la situation et de prendre des décisions, ni de détecter à temps les dangers «cachés». Le dispositif de défense du renseignement présente des lacunes et ne correspond plus à la situation actuelle de la menace. Ni les moyens existants, ni une amélioration des flux d'informations et de la coordination entre les services de renseignements et les autorités de poursuite pénale, ni le développement du droit pénal formel et matériel ne pourront combler ces lacunes. Il faut plutôt améliorer la recherche d'informations par les services de renseignements de manière ciblée, dans un cadre clairement délimité, afin qu'elle soit performante et proche des standards européens en la matière.

Pour ce faire, les mesures suivantes seront notamment prises:

– *Les autorités et les unités administratives de la Confédération et des cantons seront tenues de fournir des renseignements dans des cas concrets, mais uniquement si cela est nécessaire pour prévenir des dangers graves (terrorisme, service de renseignements politiques ou militaires prohibé ou commerce illicite de substances radioactives). Aux mêmes conditions, les trans-*

porteurs commerciaux devront également communiquer les données en leur possession.

- *En dernier recours, les moyens spéciaux de recherche d'informations seront employés. Toujours uniquement dans les domaines du terrorisme, du service de renseignements politiques ou militaires prohibé et du commerce illicite de substances radioactives, il sera possible, en cas de menaces concrètes, de surveiller la correspondance par poste et télécommunication à titre préventif, de procéder à des observations de personnes dangereuses dans les lieux qui ne sont pas librement accessibles, y compris au moyen d'appareils techniques, et de perquisitionner secrètement des systèmes informatiques. L'utilisation de ces moyens est soumise à une double approbation (examen judiciaire par le Tribunal administratif fédéral, et contrôle sous l'angle de la politique de l'Etat de la part du chef du DFJP et du chef du DDPS).*
- *Le chef du DFJP recevra la compétence d'interdire des activités qui servent à promouvoir des agissements terroristes ou extrémistes violents et qui menacent concrètement la sûreté intérieure ou extérieure de la Suisse. Par ailleurs, le recours à des informateurs, leur protection et leur indemnisation reposeront sur une base légale formelle. Pour garantir la protection des informateurs et des collaborateurs du SAP dans le cadre de la recherche d'informations, il sera possible de les munir d'identités d'emprunt.*
- *Cette extension du champ de compétence entraîne un renforcement équivalent des voies de droit. Pour pouvoir ordonner l'utilisation de moyens spéciaux de recherche d'informations, il faudra qu'ils aient été soumis au préalable à l'approbation du Tribunal administratif fédéral et de l'exécutif. Les décisions relatives à l'obligation de communiquer et à l'interdiction d'activités seront soumises à un contrôle judiciaire probant effectué par le Tribunal administratif fédéral et le Tribunal fédéral.*

Les critères restrictifs mis en place et les contrôles multiples empêchent toute restriction illicite des droits fondamentaux de tiers.

Toutes les mesures sont conformes à la Constitution et compatibles avec les droits fondamentaux. Elles se fondent notamment sur un intérêt public prouvé et respectent le principe de la proportionnalité. Le projet est en outre compatible avec la CEDH et avec le Pacte international du 16 décembre 1966 relatif aux droits civils et politiques.

Les besoins en effectifs, les investissements et les frais d'exploitation seront couverts grâce à des compensations internes au DFJP.

Table des matières

Table des abréviations

ATF	Arrêt du Tribunal fédéral
BO	Bulletin officiel
CE	Conseil des Etats
CEDH	Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (RS *0.101*)
CGE	Division de la conduite de la guerre électronique (DDPS) et les autres services de l'administration fédérale chargés de la conduite de la guerre électronique
CN	Conseil national
CP	Code pénal suisse du 21 décembre 1937 (RS *311.0*)
CPM	Code pénal militaire du 13 juin 1927 (RS *321.0*)
CPS	Commission de la politique de sécurité
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS *101*)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFJP	Département fédéral de justice et police
EIMP	Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (RS *351.1*)
EuGRZ	Europäische Grundrechte-Zeitschrift
Europol	Office européen de police
fedpol	Office fédéral de la police
FF	Feuille fédérale
Interpol	Organisation Internationale de Police Criminelle
LAAM	Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (RS *510.10*)
LAVI	Loi fédérale du 4 octobre 1991 sur l'aide aux victimes d'infractions (RS *312.5*)
LCPI	Loi fédérale du 22 juin 2001 sur la coopération avec la Cour pénale internationale (RS *351.6*)
LFIS	Loi fédérale du 20 juin 2003 sur l'investigation secrète (RS *312.8*)
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (RS *120*)
LOC	Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (RS *360*)
Loi sur les profils d'ADN	Loi fédérale du 20 juin 2003 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (RS *363*)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (RS *235.1*)

LSCPT	Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (RS *780.1*)
LTC	Loi du 30 avril 1997 sur les télécommunications (RS *784.1*)
MPC	Ministère public de la Confédération
MROS	Bureau de communication en matière de blanchiment d'argent
OCGE	Ordonnance du 15 octobre 2003 sur la conduite de la guerre électronique (RS *510.292*)
ODM	Office fédéral des migrations
OMSI	Ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (RS *120.2*)
ONU	Organisation des Nations Unies
OOC	Ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police (RS *360.1*)
OSCPT	Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (RS *780.11*)
OSF	Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale (RS *120.72*)
P-CPP	Projet de code de procédure pénale suisse (FF *2006* 1373)
PJF	Police judiciaire fédérale (DFJP)
PPF	Loi fédérale du 15 juin 1934 sur la procédure pénale (RS *312.0*)
RPS	Revue Pénale Suisse
RS	Recueil systématique du droit fédéral suisse (et des accords internationaux)
SAP	Service d'analyse et de prévention (DFJP)
SFS	Service fédéral de sécurité (DFJP)
SRS	Service de renseignement stratégique (DDPS)
STS	Service des tâches spéciales (Secrétariat général du DETEC)
TEJUS	Traité du 25 mai 1973 entre la Confédération Suisse et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale (RS *0.351.933.6*)
TF	Tribunal fédéral
UE	Union européenne

Message

1 Bases du projet

1.1 Contexte

1.1.1 Genèse du projet

Depuis plusieurs années, le service de renseignements intérieur signale des insuffisances dans le domaine de la prévention des menaces, qui sont dues à des lacunes dans la palette des instruments disponibles pour détecter lesdites menaces. Forts de ce constat, l'Organe de direction pour la sécurité et la Délégation du Conseil fédéral pour la sécurité ont ordonné l'examen de mesures appropriées pour parer à ces lacunes.

Diverses interventions parlementaires ont été déposées suite aux attentats terroristes du 11 septembre 2001. Elles sollicitent un renforcement du rôle des organes de protection de l'Etat et des services de renseignements, ainsi que des moyens à leur disposition, et l'élaboration de rapports approfondis sur la situation en matière de sécurité (voir, entre autres, les motions PRD[1], Leu[2], Merz[3] et Burkhalter[4]; les interventions PRD[5], Fünfschilling[6], Suter[7], PDC[8], Leutenegger Oberholzer[9] et Pfister[10]).

Suite au dépôt de ces interventions parlementaires, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP), en novembre 2001, de lui soumettre un rapport présentant des mesures visant à améliorer la lutte contre le terrorisme. C'est ainsi qu'il a approuvé, en juin 2002, le rapport intitulé «Analyse de la situation et des menaces pour la Suisse à la suite des attentats terroristes du 11 septembre 2001» et qu'il a pris connaissance de la séparation des projets législatifs en deux volets distincts. Le second volet (c'est-à-dire la présente révision) est notamment consacré au terrorisme.

1 01.3545 Motion du groupe radical-libéral: Renforcer les services de renseignement et la sécurité de l'Etat
2 01.3626 Motion Leu: Donner aux services de renseignement les moyens de relever les défis d'aujourd'hui
3 01.3569 Motion Merz: Renforcer les services de renseignement et la sécurité de l'Etat
4 04.3216 Motion Burkhalter: Lutte contre le terrorisme. Mesures préventives
5 01.3552 Interpellation du groupe radical-libéral: Attentats terroristes. Appréciation de la situation actuelle
6 01.3576 Interpellation Fünfschilling: Attentats terroristes. Appréciation de la situation actuelle
7 01.3612 Interpellation Suter: Lutte antiterroriste. Conséquences pour la Suisse des décisions de l'UE
8 01.3702 Motion du groupe démocrate-chrétien: Maintien à distance des personnes indésirables en Suisse pour des raisons de sécurité; 01.3704 Motion du groupe démocrate-chrétien: Elimination des points faibles de la prévention du terrorisme; 01.3705 Motion du groupe démocrate-chrétien: Service de renseignement. Coopération et professionnalisme
9 01.3633 Postulat Leutenegger Oberholzer: Attentats terroristes. Réévaluation des risques en Suisse
10 01.1114 Question ordinaire Pfister: Attentats terroristes. Recherche par quadrillage

Après des travaux préliminaires approfondis et une première discussion, le Conseil fédéral a chargé le DFJP, le 20 octobre 2004, de lui soumettre un projet de consultation au cours de l'année 2005. L'avant-projet a été envoyé une première fois en consultation dans les offices en juillet 2005, et après remaniement, une seconde fois en février 2006. Le Conseil fédéral a discuté le 5 avril 2006 des points les plus critiqués lors des consultations des offices et a fixé la suite à donner au projet. Un projet de consultation a été établi sur cette base conformément au mandat. Le 5 juillet 2006, le Conseil fédéral a chargé le DFJP de mener une procédure de consultation.

Cette dernière s'est déroulée du 5 juillet au 15 octobre 2006. Au vu des avis parfois divergents émis lors de la consultation, le Conseil fédéral a reçu, dans un premier temps, le rapport sur les résultats de la procédure de consultation, ainsi qu'une proposition concernant la suite à donner au projet. Par décision du 4 avril 2007, il a pris connaissance des résultats de la procédure de consultation et a chargé le DFJP de l'élaboration du présent message tout en décidant des orientations.

1.1.2 Service d'analyse et de prévention (SAP): le service de renseignements intérieur civil

Tâches du SAP

Service de renseignements intérieur

Le Service d'analyse et de prévention (SAP), rattaché à l'Office fédéral de la police (fedpol), est le service de renseignements intérieur policier de la Suisse.

Les tâches du SAP sont définies dans la LMSI et les ordonnances afférentes. Sa fonction consiste à informer rapidement les organes dirigeants de l'Etat et les organes policiers de la Confédération, mais aussi des cantons, des menaces qui pèsent sur la sûreté intérieure, afin que des mesures préventives puissent être prises en temps utile. Sont visées en premier lieu les menaces qui vont à l'encontre de la sûreté de l'Etat dans son ensemble et de ses habitants. A ce titre, le SAP doit notamment détecter et analyser des activités relevant de la grande criminalité. Afin d'identifier ces risques pour les fondements de la démocratie et de l'Etat de droit, de même que pour les libertés fondamentales de la population suisse, le SAP est tenu à une observation continue de la situation ainsi qu'à des appréciations périodiques de la menace. Etant donné que la LMSI lie les mesures préventives, généralement secrètes, ainsi que les interventions qui s'y rapportent à la prévention des risques pour la sûreté de l'Etat, les activités du renseignement poursuivent un objectif préventif. En temps de paix, le SAP accomplit également les tâches relevant de la défense militaire.

Menaces pour la sûreté intérieure

Le maintien de la sûreté intérieure constitue une tâche primaire et originaire de l'Etat. Il équivaut à garantir les règles les plus fondamentales de la coexistence pacifique, à protéger les institutions étatiques, à défendre la société et les individus contre les menaces élémentaires, ainsi qu'à empêcher les crises sociales[11].

[11] Message relatif à une nouvelle constitution fédérale du 20 novembre 1996, p. 406.

La question de savoir si des comportements précis menacent la sûreté intérieure est en premier lieu une question d'appréciation politique qui dépend de la situation générale. Ainsi, une situation de la menace ne peut être invoquée uniquement sur la base d'un comportement concret en tant que tel, mais plutôt en fonction du contexte politique dans lequel elle se situe. En d'autres termes, un même comportement peut constituer un danger pour la sûreté intérieure dans certains cas, tandis qu'il ne représentera pas de danger dans un environnement différent et inversement.

Prenons l'exemple d'une organisation terroriste qui reprend le combat violent dans son pays d'origine après une longue trêve sans violence – pendant laquelle la menace pesant sur la sûreté de la Suisse n'est généralement que latente. Il se peut que cette reprise des combats ait rapidement des incidences concrètes sur la sûreté de la Suisse, avec notamment des actes terroristes en Suisse, des actes de violence commis entre membres de la diaspora, des fonds collectés en faisant pression sur les personnes puis transférés dans le pays d'origine pour financer les combats, ou encore le recrutement de membres ou de combattants. Par ailleurs, des ressortissants ou des intérêts suisses peuvent être menacés en tout temps par des actes terroristes commis à l'étranger.

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 pouvant peser sur l'existence du pays, sur l'ordre de sa société et sur ses institutions démocratiques.

L'art. 1 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.

Information du gouvernement et de l'opinion publique

Grâce aux renseignements obtenus, les autorités compétentes de la Confédération et des cantons peuvent intervenir à temps conformément à leur droit respectif. Le but de la détection précoce est de mettre au jour les structures dangereuses et de traiter les informations obtenues pour que les organes de la Confédération et des cantons responsables sur le plan politique puissent prendre les décisions nécessaires. Le directeur de fedpol et le chef du SAP sont membres permanents de l'Organe de direction pour la sécurité (Ordiséc) et sont donc directement impliqués dans les appréciations de la situation et les mesures de détection précoce des organes de conduite de la politique de sécurité.

La lutte contre les menaces terroristes doit agir en amont, très tôt, afin de déjouer les projets si possible au stade de la planification ou des préparatifs. Pour cela, des mesures d'observation des personnes et des groupes dangereux et une coopération internationale optimale sont nécessaires. Mais même après un attentat terroriste – comme le montrent les exemples à l'étranger – la qualité du renseignement joue aussi un rôle de premier plan pour une identification rapide des auteurs.

Cycle du renseignement

Les services de renseignements mènent leurs activités selon les principes du cycle du renseignement, qui comprend la planification (définition de la palette des informations pouvant s'avérer intéressantes), la recherche (p. ex. les discussions avec les informa-

teurs), l'appréciation (au sujet, p. ex., de la fiabilité d'une information), l'évaluation (p. ex. le traitement de rapports et d'indications des organes de recherche) et la diffusion (p. ex. l'élaboration de rapports à l'attention de l'exécutif). Si des faiblesses apparaissent dans le domaine de la recherche, tout le cycle en est directement perturbé.

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. La recherche d'informations qui ne sont pas publiques est une tâche centrale du service de renseignements. Les produits finaux résultant de l'activité des services de renseignements ne peuvent pas contenir davantage d'informations ni d'informations de meilleure qualité que celles que la loi permet de collecter.

Au niveau opérationnel, la recherche d'informations du SAP va de la conduite de sources humaines particulièrement sensibles à des contre-opérations avec des agents démasqués ou qui ont changé de camp. De nombreux cas sont traités conjointement avec les cantons et/ou les autorités étrangères, ce qui permet d'obtenir des informations indispensables pour la sécurité de la Confédération et des cantons.

L'échange d'informations avec les autorités étrangères revêt une importance particulière. Ainsi, on compte quelque 20 000 communications par an de nature confidentielle ou secrète. Cette coopération internationale est fondamentale également pour exécuter des tâches relevant de la police des étrangers. Si, par exemple, la France expulse des prédicateurs incitant à la haine, ceux-ci ne doivent pas pouvoir venir se réfugier en Suisse. Ou si un concert skinhead est prévu en Suisse auquel des groupes de musique allemands ou italiens connus doivent participer, il convient de les empêcher de propager leurs propos racistes publiquement dans notre pays. Dans les deux cas, le SAP est habilité à prononcer des interdictions d'entrée. Il dépend, pour examiner les conditions permettant de prononcer une telle interdiction, des informations des autorités étrangères.

Evaluation des informations

Par évaluation des informations, on entend le fait d'apprécier si les informations recueillies sont fiables, de les comparer entre elles et de les traiter de manière à pouvoir les exploiter. Les personnes habilitées à exploiter les données doivent également pouvoir y accéder rapidement, en toute sécurité, sous une forme appropriée et en tout temps.

Analyse et transmission des informations

Le domaine de l'analyse du SAP est le service central d'analyse à l'échelon national. Toutes les informations émanant des services de renseignements et des services de police judiciaire y sont évaluées intégralement. Ce domaine a connu des avancées qualitatives et quantitatives au cours des dernières années. Le SAP collabore étroitement avec les services concernés de la Confédération et des cantons.

L'analyse au sens étroit est la phase où les informations sont réunies en un tableau général. Les hypothèses sont alors confirmées ou infirmées et des conclusions sont tirées.

Les analyses peuvent prendre la forme d'analyses de la menace, d'analyses politiques comparatives ou encore présenter des évolutions, des phénomènes ou des scénarios.

Parmi les analyses les plus connues du SAP, du fait qu'elles sont rendues publiques, on trouve le Rapport sur la sécurité intérieure de la Suisse, publié annuellement, ainsi que le Rapport sur l'extrémisme. Cela dit, la majorité des produits du SAP sont confidentiels et ne se concentrent que sur des aspects spécifiques de la sécurité intérieure (p. ex. la lutte contre les idéologies extrémistes empreintes de violence sur les plans juridique, technique et idéologique). Ces rapports mettent par ailleurs en lumière les connaissances manquantes, et influencent ainsi l'orientation donnée à la planification de la recherche d'informations.

Le traitement et la transmission en permanence d'informations actuelles relatives à la situation contribuent également au maintien de la sécurité de la Suisse. A ce titre, le Centre fédéral de situation du SAP diffuse quotidiennement des appréciations et des rapports de situation actualisés à plus de 300 services de la Confédération et des cantons.

De plus, le poids d'Internet et la vulnérabilité des infrastructures suisses dans ce domaine ont été reconnus, ce qui a conduit à la création du SCOCI (Service de coordination de la lutte contre la criminalité sur Internet) et de MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information).

Recherche d'informations du SAP

Selon le droit en vigueur, le SAP évalue 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.

Le deuxième alinéa de l'art. 14 LMSI énumère de manière exhaustive 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.

Le législateur de 1997 a expressément interdit au SAP d'avoir recours à des mesures de contrainte et d'observer des faits dans des locaux privés, tel que cela est autorisé dans le cadre de procédures pénales. Ainsi, toute recherche préventive d'informations est actuellement impossible pour l'ensemble des communications en Suisse (notamment par poste, téléphone, fax, courriel).

1.1.3 Autres tâches et compétences dans le domaine de la sûreté

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.

En tant que service de renseignements extérieur, le SRS recherche, en vertu de l'art. 99, al. 1, de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM)[12], 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 dispose d'un mandat de base approuvé par 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 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 les services de renseignements au DDPS (Orens)[13].

Police

La police, essentiellement soumise à la souveraineté cantonale, veille à la sécurité et à l'ordre publics et lutte contre la criminalité générale. 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 peut diriger les engagements.

Poursuite pénale

La poursuite pénale vise à clarifier la présomption d'infraction et la question de la faute individuelle sur le plan judiciaire[14].

Délimitation des tâches et des moyens du service de renseignements intérieur de celles des autorités de poursuite pénale

Finalité de la recherche d'informations

Le travail des organes de poursuite pénale vise à élucider les soupçons pesant sur un individu dans un cas particulier. La recherche d'informations par les services de renseignements vise quant à elle à détecter précocement les dangers ou les troubles de nature à compromettre la sécurité, les intentions dangereuses et les actes préparatoires concrets. Si le SAP découvre de telles menaces, les autorités compétentes de

12 RS **510.10**
13 RS **510.291**
14 Une comparaison détaillée des tâches policières liées à la poursuite pénale et des tâches policières préventives est fournie au ch. 3.2.4, let. a, du rapport du Conseil fédéral donnant suite au postulat 05.3006 du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats «Lutter plus efficacement contre le terrorisme et le crime organisé» (FF **2006** 5421), ci-après «rapport donnant suite au postulat CPS».

la Confédération et des cantons prennent les mesures policières ou administratives qui s'imposent pour les réprimer ou les éliminer.

Moyens de la recherche d'informations

Les enquêtes de droit pénal sont menées dans le cadre d'une procédure pénale ou d'une enquête formelle lorsqu'il s'agit d'élucider des soupçons suffisamment concrets quant à la commission d'une infraction. Les autorités de poursuite pénale peuvent alors avoir recours à des mesures de contrainte (p. ex. citation, remise, interpellation, garde à vue, détention préventive, saisie et garde d'objets, séquestre, surveillance de la correspondance par poste et télécommunications, fouille de personnes, mesures signalétiques, observation, enquêtes sous couverture) si celles-ci s'avèrent nécessaires pour la procédure d'enquête pénale. En raison de la répartition des compétences en matière de poursuite pénale entre la Confédération et les cantons, 26 codes de procédure pénale et lois réglant l'activité de la police sont en principe applicables en sus de la réglementation fédérale; un code de procédure pénal fédéral unifié est en délibération au Parlement. Le législateur de 1997 a interdit au service de renseignements intérieur de recourir à des moyens comparables et d'observer des faits dans des locaux privés. La question de savoir si, et si oui dans quelle mesure, cette interdiction doit être maintenue – vu la menace que représentent aujourd'hui les organisations terroristes et en raison d'autres menaces qui ont vu le jour depuis lors – est l'objet de la présente révision partielle de la LMSI.

Compétences de détection précoce de la grande criminalité de nature terroriste ou mafieuse

Le SAP est chargé de la détection précoce des menaces pour la sûreté intérieure qui se caractérisent par le recours à la violence contre la société et l'Etat et qui répondent à des motivations de nature politico-idéologique. Les syndicats de type mafieux, qui poursuivent un but d'enrichissement et de reconnaissance sociale, ne s'y apparentent pas car les activités qu'ils déploient se déroulent essentiellement dans un contexte commercial; leur détection précoce fait donc partie de la sphère de compétences de la police judiciaire[15].

Tâches de police judiciaire

Il ne faut pas confondre la recherche d'informations dans le cadre de la détection précoce avec l'instruction d'une infraction et la poursuite de son auteur. Pour autant que la juridiction fédérale soit établie, la poursuite des infractions à connotation mafieuse incombe exclusivement à la Police judiciaire fédérale (PJF), sous la conduite du Ministère public de la Confédération (MPC)[16].

Limites de la poursuite pénale

Le but de la poursuite pénale est également la source de ses limites. L'élucidation de soupçons concrets dans un cas particulier ne permet pas de détecter précocement des menaces ou des liens entre certains éléments. Les éléments constitutifs d'infraction définissent le comportement punissable de manière exhaustive et ne sont nullement liés à une quelconque menace pesant sur un pays ou sa population. Au-delà de leur effet général de prévention, les éléments constitutifs d'infraction permettant de

15 Cf. le «rapport donnant suite au postulat CPS», ch. 3.2.4, let. c.
16 Cf. le «rapport donnant suite au postulat CPS», ch. 3.2.4, let. d.

poursuivre des organisations criminelles, les auteurs des actes principaux liés au terrorisme ou des cellules terroristes ne visent pas en priorité à prévenir des attentats. Les actes préparatoires ne sont pas non plus punissables du fait d'une situation de la menace précise, mais en tant qu'activités individuelles concrètes. Il apparaît ainsi que les instruments de la poursuite pénale ne sont ni conçus ni appropriés pour la détection précoce de menaces et de risques, d'individus ou d'organisations dangereux ou de leurs structures. C'est à cela que sert le travail des services de renseignements, qui s'attache aux situations de la menace et non aux infractions.

1.1.4 Echange d'informations et collaboration avec d'autres autorités

Organisation des autorités au sein du DFJP

En vue de l'extension de la juridiction pénale de la Confédération aux affaires de criminalité organisée, le Conseil fédéral a regroupé l'ancienne Police fédérale et le Service de sécurité de l'administration fédérale, le 1er septembre 1999, en les transférant du MPC à l'ancien Office fédéral de la police, devenu aujourd'hui fedpol. En réunissant tous les services de police du DFJP dans cet office, le Conseil fédéral a fait un pas en direction des cantons, qui souhaitaient un interlocuteur unique au niveau fédéral pour toutes les questions liées à la police. Il a également donné suite ainsi à une exigence formulée par la commission d'enquête parlementaire du DFJP, qui demandait que la fonction de procureur général de la Confédération, en tant qu'accusateur public, soit séparée de celle de premier responsable de l'ancienne Police fédérale, qui exerçait alors non seulement la fonction de police judiciaire mais également celle de service de renseignements intérieur, ce qui l'amenait à accomplir des tâches de nature préventive[17].

Ainsi, le 1er janvier 2001, à l'issue du projet de restructuration du domaine policier de la Confédération, les tâches de police préventive et de police judiciaire ont été séparées sur le plan organisationnel au sein de fedpol: la division «Offices centraux de police criminelle» et la «Police fédérale» ont été remplacées par les nouvelles divisions principales PJF et SAP. La première a la fonction de police judiciaire et exerce à ce titre les tâches de poursuite pénale, tandis que la seconde se concentre sur la prévention par le renseignement.

Collaboration avec le service de renseignements extérieur du DDPS

En présence de menaces liées à des phénomènes internationaux qui relèvent des domaines de compétence des deux services de renseignements, ceux-ci collaborent étroitement, comme ils le font déjà aujourd'hui dans le cadre des plateformes de coopération dans les domaines du terrorisme, du crime organisé et de la prolifération.

Collaboration avec d'autres organes du DDPS

Le SAP, le Renseignement militaire (RM), le Renseignement des forces aériennes (RFA), les autres organes de renseignement de l'armée ainsi que la Sécurité militaire se soutiennent mutuellement dans l'accomplissement de leurs tâches, notamment par

17 Rapport de la commission d'enquête parlementaire (CEP) du 22 novembre 1989, 89.006, Evénements survenus au DFJP, FF **1990** 593, chap. VII, ch. 1.

le biais de l'échange d'informations, de conseils réciproques pour des questions spécifiques et de la formation.

Collaboration entre le SAP et les organes de poursuite pénale de la Confédération

Nécessité d'un échange d'informations rapide et régulier en raison du recoupement thématique des domaines de compétences: le SAP et la PJF sont tenus de se transmettre immédiatement les informations qu'ils reçoivent et qui relèvent du domaine de compétences de l'autre division[18].

Transmission d'informations par le SAP à la PJF et au MPC: lorsque le SAP entre en possession d'informations concernant le crime organisé, il est tenu de les transmettre aux organes de poursuite pénale de la Confédération ou des cantons conformément à l'art. 2, al. 3, LMSI. Par ailleurs, il est tenu de transmettre immédiatement tout indice important pour la poursuite pénale aux autorités de poursuite pénale de la Suisse[19].

Transmission d'informations par la PJF et le MPC au SAP: le législateur a prévu une obligation réciproque pour le MPC et la PJF de transmettre des informations au SAP[20]. Tous deux sont tenus de communiquer spontanément des renseignements au SAP lorsqu'ils décèlent des menaces concrètes pour la sûreté intérieure ou extérieure[21]. Au-delà de la transmission d'informations opérationnelles, le MPC communique au SAP les jugements et les ordonnances de non-lieu qui touchent au champ d'application de la LMSI[22].

Echange d'informations en ligne: le SAP et la PJF disposent d'un accès limité réciproque aux systèmes d'information que chacun d'entre eux exploite. Dans la loi fédérale sur les systèmes d'information de police de la Confédération, il est prévu de créer un index national de police destiné à accélérer et à simplifier l'entraide administrative en matière de police[23].

Garanties de procédure dans l'entraide administrative: outre la protection des données, le service de renseignements intérieur et les autorités de poursuite pénale doivent prendre en considération les intérêts publics prépondérants, qui peuvent conduire à une limitation voire à une exclusion pure et simple de l'entraide et soumettre la transmission de données à des tiers à certaines restrictions. Lorsqu'il transmet des éléments relevant du renseignement, le SAP doit ainsi veiller à la sauvegarde des intérêts prépondérants[24] mais aussi à la protection des sources. La protection des sources est toujours garantie dans les rapports avec l'étranger[25] tandis que le besoin de protection des sources internes doit être pondéré dans chaque cas en fonction de la nécessité de l'entraide administrative ou judiciaire. Les transmissions ont donc lieu sous la forme de rapports d'évaluation, et non sous la forme d'informations brutes.

18 Cf. le «rapport donnant suite au postulat CPS», ch. 3.2.5, let. a.
19 Cf. art. 17, al. 1, LMSI; cf. également la collaboration prévue à l'art. 4 LOC; cf. le «rapport donnant suite au postulat CPS», ch. 3.2.5, let. b.
20 Art. 13, al. 1, let. a, LMSI.
21 Art. 13, al. 2, LMSI.
22 Cf. le «rapport donnant suite au postulat CPS», ch. 3.2.5, let. c.
23 Cf. le «rapport donnant suite au postulat CPS», ch. 3.2.5, let. d.
24 Art. 18, al. 5, OMSI.
25 Art. 17, al. 7, LMSI et art. 20*a* OMSI.

Le MPC et la PJF peuvent aussi refuser ou restreindre la transmission d'informations ou encore l'assortir de charges. Ils y sont tenus lorsque les intérêts légitimes d'une personne l'exigent[26] ou lorsque la procédure en cours le commande[27].

Relations avec l'étranger

Le SAP assure les liaisons avec les autorités de sûreté étrangères qui accomplissent des tâches au sens de la LMSI (art. 8 LMSI). Il représente en outre la Suisse dans les instances internationales (art. 6 de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI; RS *120.2*). La lutte contre le terrorisme représente aujourd'hui la majeure partie des échanges internationaux d'informations entre services de renseignements.

Dans le détail, le SAP coopère sur une base permanente dans le domaine du renseignement et de la police avec environ 90 services partenaires appartenant à des Etats étrangers et/ou à des organisations internationales (par ex. l'ONU ou l'UE)[28]. Le SAP est membre de quatre instances multilatérales informelles: le «Groupe antiterroriste» (un service de chaque Etat de l'UE ainsi que de la Norvège et de la Suisse), le «Club de Berne» (services de renseignements de 22 pays européens), la «Middle European Conference» (services de 17 pays, ainsi que 8 pays ayant le statut d'observateur, principalement du Sud-Est de l'Europe) et le «Police Working Group on Terrorism» (autorités de police antiterroriste de 26 pays). La conclusion d'un accord sur les procédures de sécurité dans les échanges d'informations classifiées est prévue afin de pouvoir continuer à coopérer dans le domaine du renseignement avec le «Centre de situation» du Conseil de l'UE[29]. Dans le cadre du Conseil de partenariat euro-atlantique (CPEA), le SAP assume également, pour la Suisse, des tâches d'«Intelligence Liaison Unit» (ILU) à l'égard de l'OTAN.

En ce qui concerne le cercle des services partenaires étrangers, cette coopération répond aux besoins actuels de la Suisse dans tous les domaines spécifiques de la LMSI.

La coopération des services de renseignements avec des services étrangers est informelle. Elle se fonde sur les principes de la confidentialité, sur la règle dite «du service tiers» et sur la confiance réciproque. A ce titre, les informations sont mises à disposition selon le principe du donnant-donnant, en étant confiant dans le fait qu'un des services partenaires transmettra à son tour les informations pertinentes en termes de sûreté («do ut des», principe du juste retour). Cela ne relève cependant pas d'une obligation.

26 Art. 102quater, al. 2, PPF en relation avec l'art. 27, al. 2, PPF, et l'art. 7, al. 2, de l'ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police.

27 Cf. le «rapport donnant suite au postulat CPS», ch. 3.2.5, let. e.

28 La stratégie de coopération internationale du SAP est définie dans un document classifié confidentiel que le Conseil fédéral a approuvé en juin 2005.

29 L'accord a été approuvé par le Conseil de l'UE le 24 juin 2005 et par le Conseil fédéral le 29 juin 2005. Les détails techniques sont actuellement réglés avec l'UE.

1.1.5 Comparaison sous forme de tableau

Soupçon	
de menace pour la sûreté de la Suisse liée à des actes relevant du terrorisme, de l'extrémisme violent, du service de renseignements prohibé, de la prolifération	**d'infraction concrète ou d'acte préparatoire concret selon le droit pénal fédéral ou cantonal**
Prévention	*Répression*
Compétences	
Service d'analyse et de prévention, services de renseignements cantonaux	Ministère public de la Confédération, Police judiciaire fédérale, autorités de poursuite pénale cantonales
Activités	
Recherches relevant des services de renseignements et recherche d'informations Activité d'analyse dans le domaine de la sûreté intérieure	Enquêtes judiciaire en cas de soupçon concret d'infraction (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 suffisants pour donner lieu à l'ouverture d'une procédure pénale
But	
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 Mise en œuvre des mesures nécessaires Stratégique (activité durable d'observation)	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, 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 informel avec les services de renseignements et de sécurité étrangers	Echange 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

1.1.6 Situation de la Suisse en matière de sécurité

Terrorisme

Situation en matière de sécurité

Depuis les attentats terroristes de Madrid (en 2004 contre des trains de banlieue) et de Londres (en 2005 dans le métro et des bus), l'Europe occidentale est passée du statut de base arrière à celui de terrain d'action du terrorisme islamiste. De manière générale, les menaces terroristes visent les intérêts occidentaux, dont font partie – du point de vue des islamistes – les Nations Unies et le CICR, qui ont leur siège en Suisse. 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, notamment au moyen de techniques liées à Internet. 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. Des informations provenant de procédures pénales menées en Suisse et dans les pays voisins montrent que notre pays est mis à profit par des personnes soutenant Al-Qaïda.

Les services de sécurité européens sont déjà parvenus à plusieurs reprises à reconnaître des actes préparatoires et empêcher la commission d'attentats, notamment lorsqu'ils ont déjoué un attentat au marché de Noël de Strasbourg (2000) ainsi que des attentats-suicides qui auraient été commis avec de l'explosif liquide à bord de vols transatlantiques en Angleterre (2006) ou lorsqu'ils ont mis au jour précocement les préparatifs d'attentats à l'explosif qu'un groupe djihadiste entendait commettre contre des institutions danoises (2006).

Suite à l'évolution de la situation internationale décrite ci-dessus, la sécurité de la Suisse s'est peu à peu et durablement dégradée au cours de ces dernières années. La probabilité que des actes terroristes islamistes soient commis aussi en Europe occidentale a augmenté. Notre pays a certes été épargné par des attentats terroristes, mais la situation peut changer à tout moment. La situation actuelle en Suisse peut être comparée à celle de certains pays étrangers dans lesquels des attentats ont été commis ou ont failli être commis. Ainsi, la Suisse fait partie de la zone de danger d'Europe occidentale. Les djihadistes la considèrent comme faisant partie des Etats croisés, raison qui suffit pour légitimer un attentat. Par ailleurs, elle abrite des structures islamistes actives, enclines à la violence et en partie liées entre elles. Les conditions pour commettre un attentat terroriste sont ainsi réunies. Les moyens de recherche actuels, fondés en grande partie sur des sources publiques, ne permettent guère de prévoir si les menaces existantes se concrétiseront et, si oui, à quel moment. Il s'est avéré aussi qu'il y avait en Suisse des islamistes désireux de participer au djihad en Irak en tant que combattants volontaires. La ville de Genève leur servait de zone de transit et leur permettait de recruter des volontaires en provenance de Suisse romande et de France voisine.

Selon l'appréciation actuelle, la Suisse ne constitue toujours 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.

On constate que la Suisse tire actuellement profit, dans ses appréciations de la situation, des informations et des compétences – bien plus étendues – des services de sécurité étrangers chargés de faire des recherches. Une collaboration insuffisante en raison de bases légales incomplètes peut rapidement pousser les partenaires étrangers à se montrer beaucoup plus restrictifs lorsqu'il s'agit de fournir des informations à la Suisse. Or des informations lacunaires peuvent conduire à de fausses interprétations et, partant, avoir des conséquences négatives quant aux mesures à appliquer.

Lacunes dans le dispositif préventif

Si les autorités 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.

Selon le droit en vigueur, la correspondance par poste et télécommunication ne peut pas non plus faire l'objet de recherches menées en vertu de la LMSI en vue d'évaluer la menace, avec pour conséquences des lacunes dans la détection précoce et la collaboration internationale.

Ainsi, après avoir surveillé la correspondance par télécommunication de milieux islamistes milanais, les autorités italiennes sont arrivées à la conclusion que ceux-ci organisaient et finançaient la formation d'extrémistes en Afghanistan par l'intermédiaire de personnes résidant en Suisse. Les conditions nécessaires à l'ouverture d'une procédure pénale contre les personnes vivant en Suisse n'étaient pas réunies. Les services de renseignements italiens ont par contre contacté le SAP et lui ont demandé d'effectuer des recherches sur l'entourage des personnes suspectées. Le SAP n'a pu mener les recherches, habituelles au niveau international, relatives à la sphère privée de ces personnes et à leur entourage. En effet, il ne peut ni procéder à des observations dans le domaine privé (p. ex. par l'utilisation de moyens techniques de surveillance), ni avoir accès aux données transmises par télécommunication ou aux informations soumises au secret postal. Eu égard à l'opération italienne, il n'a pas été question d'intervenir directement, c'est pourquoi ces personnes sont restées en Suisse sans être inquiétées. Conclusion: les enquêtes sur les réseaux terroristes ou extrémistes peuvent s'arrêter à la frontière suisse.

L'arrestation de trois ressortissants turcs au Liechtenstein en décembre 2005 constitue un autre exemple. Ces personnes ont été accusées d'apporter un soutien financier et logistique à un groupe extrémiste turc, responsable d'attentats-suicides à Istanbul. Les enquêtes ont révélé que de nombreux voyages avaient été effectués en Suisse, et qu'une certaine mosquée avait été fréquentée à plusieurs reprises. Des détails relatifs au réseau de relations en Suisse auraient été de la plus grande utilité dans le but de reconnaître les liens existant avec les groupes terroristes locaux ou leurs sympathisants.

Des services de renseignements européens ont estimé que la proportion d'informations utiles recueillies par la surveillance préventive de la correspondance par télécommunication visant à lutter contre le terrorisme allait actuellement jusqu'à 80 %.

Les autorités de protection de l'Etat doivent malgré tout tenter d'entrer secrètement en contact avec les groupes et les personnes concernés, raison pour laquelle elles ont besoin de recourir à des identités d'emprunt qui font défaut aujourd'hui.

Une autre lacune grave touche le domaine d'Internet. Les personnes et les groupes qui menacent la sûreté intérieure de la Suisse utilisent depuis longtemps des infrastructures informatiques modernes, en particulier Internet, pour diffuser leur idéologie et leur propagande et échanger des informations.

Si l'accès aux domaines protégés par des mots de passe, où de la propagande djihadiste est par exemple diffusée, est techniquement possible, il n'en reste pas moins problématique que, ces domaines étant assimilés à la sphère privée, il est interdit par la loi (art. 143bis CP, accès indu à un système informatique). Il en va de même lorsque l'on peut raisonnablement admettre qu'un système ou un réseau de données est utilisé dans le but d'enregistrer, pour soi-même ou pour des tiers, des données susceptibles de nuire concrètement à la sûreté intérieure de la Suisse et que les systèmes se trouvent à l'étranger. Il est pratiquement impossible de faire des recherches relatives à des soupçons si l'on n'a pas accès au texte brut des courriers électroniques envoyés ou reçus de manière codée, ou aux lieux de contact virtuels d'extrémistes accessibles par le biais de sites djihadistes.

L'exclusion générale de la recherche d'informations à titre préventif dans un média aujourd'hui devenu central revient à accepter un vide de connaissance qui peut s'avérer dangereux.

Le manque de moyens rend la Suisse dépendante des informations étrangères. A titre d'exemple, les informations relatives à la radicalisation par certaines branches de l'islam radical de certaines parties de la diaspora bosniaque/slave en Suisse se fondent principalement sur des informations des services partenaires étrangers. De même, sans demande d'entraide judiciaire émanant d'Etats étrangers, la Suisse ne serait pas au courant de la structure locale de soutien à une organisation terroriste algérienne. Une telle dépendance de la Suisse des informations étrangères pourrait s'avérer fatale.

Service de renseignements prohibé

Situation en matière de sécurité

Les services de renseignements étrangers s'intéressent 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 et moins de structures d'espionnage et de cas liés au service de renseignements prohibé ont été mis au jour. Ceci a fait naître la fausse impression que la Suisse n'était plus ou presque plus touchée par l'espionnage. Or certains pays ont posté en Suisse des officiers de leurs services de renseignements, ce qui témoigne implicitement d'activités d'espionnage. Certaines représentations étrangères en

Suisse emploient des collaborateurs formés aux tâches relevant des services de renseignements. Les «agents» font partie du personnel de l'ambassade et bénéficient ainsi de l'immunité diplomatique. Ils sont formés pour collecter également des informations pour les services de renseignements, tout en conservant leur couverture. Au départ, le soupçon ne repose généralement que sur une appréciation de la menace effectuée par les services de renseignements (p. ex. en raison d'un indice fourni par un service de renseignements partenaire ou parce que la personne visée a succédé à une personne identifiée comme faisant partie d'un service de renseignements «ennemi»). A cela s'ajoutent les recherches d'informations effectuées par des bureaux d'investigation et des détectives privés internationaux, qui agissent parfois (sous couverture) sur mandat d'un Etat.

Lacunes dans le dispositif préventif

Selon le droit en vigueur, les lieux qui ne sont pas librement accessibles (p. ex. chambres d'hôtel) échappent en règle générale aux recherches menées en vertu de la LMSI en vue d'évaluer la menace. Il en résulte que les recherches relatives à la sûreté intérieure de la Suisse s'achèvent en principe sur le seuil qui sépare la sphère publique de la sphère privée. Ainsi d'importantes lacunes peuvent se créer dans le dispositif préventif.

Les recherches menées par les services de renseignements (p. ex. lors de rencontres effectuées en toute discrétion) étant soumises à des mesures de protection particulières et ayant généralement lieu dans des locaux privés, l'autorité suisse chargée du contre-espionnage a toutes les raisons de penser qu'une menace existe. Mais n'ayant accès qu'aux lieux publics, elle ne peut pas confirmer la nature des activités suspectées et ne peut donc pas réunir les informations qui lui permettraient de formuler un soupçon pertinent sur le plan pénal. La présomption de culpabilité ne suffit cependant pas encore pour ouvrir des enquêtes pénales. Les questions centrales restent donc sans réponse: quel type de contacts la personne cible entretient-elle? Qui est son interlocuteur en Suisse? Qu'espionne-t-elle et dans quel but? Quelles méthodes utilise-t-elle? Est-il possible de prendre des contre-mesures?

S'agissant du service de renseignements prohibé, l'autorité chargée du contre-espionnage ne peut confirmer des soupçons sans avoir accès aux lieux privés, ce d'autant que les personnes cibles sont spécialement entraînées pour tirer profit des faiblesses de la législation en vigueur et pour dissimuler leurs activités de manière professionnelle. Sans identité d'emprunt, les contre-opérations ne sont réalisables que dans des cas exceptionnels. Si la Suisse ne peut mettre en œuvre des contre-mesures, elle risque de passer à côté d'informations importantes sur le plan de la sécurité.

Les recherches visant les communautés étrangères en Suisse ont montré avec le temps que les personnes concernées se taisaient, de peur des préjudices qu'elles et leurs proches pourraient subir. Pour briser le silence, les recherches des services de renseignements menées dans des locaux privés sont indispensables. En l'absence de soupçons suffisants, les autorités pénales n'ont, dans un tel cas, pratiquement aucune possibilité d'action.

Extrémisme violent

Situation en matière de sécurité

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 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. On compte environ 1200 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.

Lacunes dans le dispositif préventif

Le Conseil fédéral estime que la situation juridique actuelle suffit en soi à contenir la menace dans ce domaine. Sont réservés les agissements de certaines personnes ou de certains groupes susceptibles de menacer la sûreté intérieure de la Suisse, auxquels il s'agit de mettre fin. On peut citer ici les collectes de fonds effectuées par des organisations extrémistes violentes en Suisse. Ces dernières transfèrent ensuite les fonds à l'étranger, sans laisser de traces et sans aucune certitude quant à leur utilisation finale, si bien qu'on ne peut exclure qu'ils servent à financer des actes de violence.

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

Situation en matière de sécurité

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

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.

Dans le domaine du commerce illicite d'armes et de substances radioactives, des réseaux extrêmement complexes sont régulièrement actifs, souvent à l'échelon international, si bien qu'un pays n'abritera souvent qu'une partie du puzzle. Les discussions et les processus importants ont lieu 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 les personnes concernées 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 mise au jour du réseau spécialisé dans le transfert de technologie nucléaire du «père» de la bombe atomique du Pakistan, Abdul Qadeer Khan, met non seulement en lumière les structures complexes et professionnelles de tels réseaux, mais prouve aussi que la Suisse peut être et est impliquée dans de tels agissements et que ses infrastructures peuvent être utilisées de manière ciblée pour mener des activités de recherches. A noter que des Etats sensibles en matière de prolifération montrent un

certain intérêt pour la qualité suisse en général et pour certaines entreprises actives dans le segment de la haute technologie en particulier.

Les efforts déployés par l'Iran pour enrichir l'uranium ou le programme nucléaire de la Corée du Nord en sont d'autres exemples. S'agissant de la menace constituée par les bombes sales (bombes composées d'un explosif conventionnel enrobé d'un matériau non conventionnel, p. ex. radioactif), les trafiquants redoublent d'efforts dans ce domaine, tout particulièrement en Europe, si bien que la quantité de matériel confisqué par les autorités entre 2003 et 2006 correspondait à elle seule à celle des sept années précédentes.

Le SAP est régulièrement informé par des tiers de l'éventuelle implication d'entreprises suisses dans des activités de prolifération. En raison du manque de possibilités en matière de recherches d'informations, les indices existants ne peuvent cependant pas être étayés en un soupçon concret, nécessaire à l'ouverture d'une procédure pénale. Le SAP peut donc supposer l'existence d'une infraction, mais sa marge de manœuvre est très limitée.

Lacunes dans le dispositif préventif

Comme dans le cas du terrorisme et du service de renseignements prohibé, il n'est généralement pas possible pour le service de renseignements de mener des recherches concluantes relatives à des soupçons dans le domaine de la prolifération sans la possibilité de surveiller la sphère privée.

Normalement, la vente ou l'achat d'une machine-outil par exemple ne constitue pas un danger pour la sûreté intérieure ou extérieure. Toutefois, il peut arriver qu'une machine-outil soit achetée dans le but de développer des armes de destruction massive (biens à double usage). Là aussi, en raison de l'impossibilité d'accéder à des locaux privés, des recherches plus approfondies ne sont pas possibles lorsque des indications relatives à ce type d'activités (p. ex. sur la base d'informations émanant de services de renseignements étrangers) certes existent, mais lorsqu'on ne dispose pas d'un soupçon relatif à un acte répréhensible et pertinent sur le plan pénal. C'est par exemple le cas lorsque des services de renseignements étrangers informent la Suisse de l'entrée sur son territoire d'un homme d'affaires auquel on attribue des liens avec un programme nucléaire étranger indésirable. Dans ce cas, il serait particulièrement intéressant d'avoir des informations quant à ses interlocuteurs et à ses partenaires d'affaires en Suisse ainsi qu'au but réel du voyage. La situation juridique actuelle ne permet pas d'étayer des soupçons de façon approfondie.

Crime organisé

Situation en matière de sécurité

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 orga-

nisé pourraient entretenir 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.

Dispositif préventif existant

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.

1.1.7 Collaboration entre le service de renseignements et les autorités de poursuite pénale

Les procédures prévues par la LMSI et par le CP sont différentes

Les soupçons concrets conduisent tant à des investigations relevant du renseignement (prévention, du latin praevenire «venir devant, prévenir») qu'à des enquêtes pénales (répression, du latin reprimere ou primere «réprimer, contenir»). Pour le travail des services de renseignements, le soupçon porte sur une menace significative pour la sécurité, alors que pour le travail des organes de poursuite pénale, il concerne une infraction concrète.

Les recherches fixées dans la LMSI visent à vérifier le soupçon lié à une possible menace pesant sur la sûreté intérieure de la Suisse ou sur la sécurité de ses habitants par le terrorisme, l'extrémisme violent, le service de renseignements prohibé ou la prolifération. Les investigations peuvent être induites tant par un comportement en fin de compte non punissable que par un comportement répréhensible. Les résultats des investigations sont transmis soit aux décideurs politiques, c'est-à-dire aux organes exécutifs de la Confédération et des cantons, afin qu'ils puissent intervenir à temps dans la mesure du droit applicable, soit aux autorités de poursuite pénale lorsqu'un soupçon d'infraction est confirmé.

Il en va différemment de la poursuite pénale (répression). La recherche d'informations vise à vérifier un soupçon d'infraction ou la faute individuelle. Elle se limite à chacun des éléments constitutifs d'infraction. Les résultats des enquêtes sont ensuite intégrés dans des procédures judiciaires et non présentés à des instances politiques.

La clarification de situations de la menace prévues par la LMSI est différente de la clarification d'actes relevant du droit pénal prévue par le CP. Les investigations se différencient par l'élément qui les motive (pour l'un un soupçon de menace contre la sûreté intérieure de la Suisse ou contre la sécurité de ses habitants, pour l'autre un soupçon concernant la commission d'une infraction concrète), par l'objet des investigations (pour l'un la mise au jour de structures et de réseaux relevant des domaines d'action prévus par la LMSI, pour l'autre la preuve d'un comportement répondant à des éléments constitutifs d'infraction au sens du CP) ainsi que par le but visé (pour l'un la base de décision permettant aux pouvoirs exécutifs de prendre des mesures, pour l'autre la vérification d'un soupçon d'infraction ou de la faute individuelle).

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 soupçonnée d'une infraction ou l'infraction présumée sont également l'objet de recherches préventives. En d'autres termes, la même personne ou le même acte peuvent faire, simultanément, 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 menées dans le cadre d'une appréciation de la menace pesant sur la sûreté intérieure de la Suisse. Les deux procédures peuvent donc se compléter partiellement, mais ne peuvent pas se remplacer.

Pour clarifier les différents points de vue, il convient de s'appuyer sur l'exemple d'une organisation terroriste étrangère, laquelle est réputée avoir collecté des fonds auprès de ses compatriotes vivant en Suisse au moyen de méthodes peu délicates. On constate aussi que des personnes proches de cette organisation se sont régulièrement rendues à l'étranger munies d'importantes sommes d'argent liquide. Du point de vue pénal, il n'est pas possible de prouver avec certitude que l'argent transporté à l'étranger a une origine criminelle ou est utilisé à des fins criminelles. La poursuite pénale ne disposant pas d'éléments constitutifs d'infraction, nécessaires à la preuve, toute condamnation est exclue. Du point de vue des services de renseignements, il est en revanche concevable que l'argent en question provienne de «collectes» et serve à financer d'une manière ou d'une autre des attentats terroristes ou la guerre contre le pays d'origine. La Suisse ne tolérant pas la promotion d'actes terroristes, ce comportement est indésirable. Sur la base des informations des services de renseignements, il appartient au pouvoir exécutif de décider de la suite à adopter, notamment de prendre les mesures préventives qui s'imposent (p. ex. interdiction des collectes de fonds pour certains groupements ou ressortissants).

Actes punissables et non punissables menaçant la sûreté intérieure de la Suisse

Les recherches menées en vertu de la LMSI sont déclenchées par des indications révélant des comportements ou une évolution de la situation susceptibles de menacer la sécurité intérieure de la Suisse par le terrorisme, l'extrémisme violent, le service de renseignements prohibé ou la prolifération.

La sécurité intérieure de la Suisse peut être menacée tant par des actes non punissables que par des actes répréhensibles. Par exemple, le régime irakien en place sous Saddam Hussein menaçait, si la guerre venait à éclater, de faire commettre des attentats terroristes dans le monde entier, par le biais des missions diplomatiques de l'Irak, jouissant en tant que telles d'un statut protégé. La Suisse ne disposait pas d'indices concrets laissant penser à la préparation d'actes punissables qui auraient pu faire l'objet d'investigations dans le cadre d'une procédure pénale. Malgré cela, il incombait au gouvernement suisse d'évaluer la situation et de prendre des mesures visant à minimiser le risque d'attentats en Suisse ou commis depuis son territoire. Des informations relevant des services de renseignements s'avéraient donc et sont encore nécessaires.

Cela dit, lorsqu'il s'agit d'évaluer une situation de menace du point de vue de la politique de sécurité, ni l'impunité, ni la punissabilité présumée d'un certain comportement ne constituent les seuls critères décisifs.

Le manque de moyens de renseignement empêche de mieux soutenir les autorités de poursuite pénale

La présence d'un soupçon initial constitue la condition préalable de toute action des autorités de poursuite pénale. Au niveau fédéral par exemple, il faut que des soupçons «suffisants» existent pour qu'une enquête soit ouverte (cf. art. 101, al. 1, PPF; également art. 194, al. 1, ch. 2 P-CPP).

Dans la pratique, les renseignements relatifs à des situations de menace contre la sûreté intérieure contiennent souvent des indices relatifs à la présence ou à la planification d'éventuelles infractions, sans qu'il existe pour autant déjà un soupçon suffisant sur le plan pénal quant aux auteurs ou au degré de concrétisation.

Il en résulte, d'une part, que le service de renseignements suppute l'existence d'une infraction, mais ne dispose pas des instruments nécessaires qui lui permettraient de confirmer ses soupçons et, d'autre part, que les autorités de poursuite pénale disposeraient certes des instruments suffisants mais ne sont, en raison de soupçons insuffisamment fondés, pas autorisées à les utiliser face à de telles constellations.

Si l'on ne souhaite pas accepter de telles lacunes et que la poursuite pénale ne doit pas être ouverte sans soupçon suffisant, alors des possibilités plus développées de recherche doivent être mises en place aux fins de détection précoce par les services de renseignements.

1.1.8 Appréciation des risques

Un certain risque pour la sécurité

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 à la protection des données dans le domaine des services de renseignements. Le législateur renonce largement 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. 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. La Confédération accepte par là de prendre un certain risque (…).» (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'accroissement de la menace a entraîné une augmentation du risque que l'on était prêt à accepter. Les besoins en matière d'informations, nécessaires à la détection précoce, ne sont plus satisfaits depuis longtemps. Dans 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, le Conseil fédéral relevait déjà les points faibles de la lutte contre la menace terroriste.

Lacunes reconnues dans le dispositif préventif

Les recherches prévues par la LMSI visent à déceler précocement les menaces contre la sûreté intérieure et extérieure de la Suisse ou contre ses habitants afin, si possible, de les prévenir. La détection précoce ne dispose pas d'instruments qui lui

permettraient, dans des cas fondés, de mener des recherches approfondies dans la sphère privée également.

L'absence de reconnaissance des situations dangereuses, ou une reconnaissance tardive, implique que les mesures de prévention sont prises trop tard, voire ne sont même plus possibles.

De trop grandes disparités entre les instruments de sécurité de chaque pays impliquent que, lorsque différents pays collaborent, les normes ne sont pas les mêmes. Lorsque ces écarts sont trop grands, la crédibilité du pays est alors remise en question. Dans son rapport sur le terrorisme («Country Reports on Terrorism 2006»), le Département d'Etat des Etats-Unis est notamment parvenu, en ce qui concerne la Suisse, à la conclusion suivante: «… however, law and practice continued to limit the scope of intelligence sharing and joint investigations …» (p. 75). Le risque existe de voir même des services partenaires opérer sur le territoire suisse dans le but de sauvegarder leurs intérêts, ce qui s'est d'ailleurs déjà passé à plusieurs reprises.

Pas de possibilité de surveillance stratégique

Les menaces pour la protection de l'Etat relevant du terrorisme se fondent en général sur des motivations politiques et idéologiques. Les convictions extrémistes et fondamentalistes ne sont généralement pas susceptibles de s'amenuiser, car elles sont hermétiques à toute argumentation et s'inscrivent dans la durée.

Comme l'expérience l'a montré, de telles situations de menace peuvent à tout moment donner lieu à des actes susceptibles de menacer la sûreté de la Suisse. Souvent, les facteurs déclencheurs sont impondérables; dans de nombreux cas, des convictions extrémistes ont évolué vers l'extrémisme violent et, quelques fois, ont même conduit à des attentats terroristes. On ne peut exclure qu'un tel attentat se produise en Suisse également. Le potentiel est présent et de telles intentions ont été formulées.

Ainsi, des substances chimiques ont été saisies chez un ressortissant suisse adepte de l'idéologie terroriste, qui auraient permis de fabriquer plusieurs kilos d'explosifs. Après que la poursuite pénale a dû être suspendue faute de preuves juridiquement tangibles, plusieurs indications ont permis de conclure que la radicalisation se poursuivait. La limite séparant le soupçon de l'acte préparatoire punissable n'a pas été franchie, raison pour laquelle aucune poursuite pénale ne peut être engagée.

Un laisser-faire vis-à-vis de ces personnes ou groupes constitue un risque que la Suisse ne peut prendre à la légère. La question se pose également pour la surveillance à long terme des personnes qui, par exemple, ont été condamnées pour des actes terroristes mais qui ont purgé leur peine et ont retrouvé la liberté ou de celles qui ont été acquittées faute de preuves mais qui semblent ne pas avoir abandonné pour autant leur idéologie empreinte de violence et n'excluent pas les actes de violence.

C'est pourquoi il est nécessaire de créer des base juridiques permettant aux services de renseignements en Suisse d'effectuer une surveillance stratégique qui devra être ciblée mais viser le long terme, se limiter à l'essentiel et être soumise à un contrôle juridique et politique.

Interdiction d'activités constituant une menace pour la sécurité

Afin de protéger la sûreté intérieure, certaines activités doivent pouvoir être interdites, notamment l'encouragement d'agissements terroristes ou extrémistes violents lorsqu'ils sont susceptibles de nuire concrètement à la sûreté intérieure ou extérieure de la Suisse (p. ex. collectes de fonds en Suisse servant à financer une guerre ou un parti menant la guerre à l'étranger).

Selon le droit en vigueur, de telles interdictions sont déjà soumises à des conditions restrictives et peuvent déjà être appliquées lors de situations de menace extraordinaires. Elles se fondent sur les art. 184, al. 3, et 185, al. 3, Cst. Ces interdictions doivent cependant être limitées dans le temps. Or elles ne peuvent être prolongées plusieurs fois ni pour une durée indéterminée car on risquerait de contredire la règle constitutionnelle. Dès lors, une base légale doit être créée et la compétence de décider d'une interdiction dans les cas d'application fixés par la LMSI doit être déléguée au DFJP. Les voies de droit seront renforcées en conséquence.

Une énumération exhaustive des activités devant être soumises à une interdiction n'est pas indiquée, car les détails d'une interdiction, qui doivent être adaptés au cas particulier, ne pourraient pas être fixés avec précision. Par ailleurs, cela reviendrait en quelque sorte à créer une norme de droit pénal et le gouvernement ne pourrait assumer sa responsabilité quant au maintien de la sûreté intérieure que de façon insatisfaisante. Il est impératif qu'après la prononciation d'une interdiction la personne ou l'organisation concernée connaisse les obligations auxquelles elle doit se soumettre et puisse exercer ses droits. Pour ce faire, il faut que les obligations soient adaptés dans chacun des cas particuliers à l'état de fait à évaluer. La procédure proposée ici permet de tenir compte au mieux de cette exigence.

Cette procédure permet d'améliorer la prévention des menaces, en créant la possibilité sur le plan juridique de réagir rapidement et directement face au comportement de certaines personnes ou certains groupes.

1.2 Solutions examinées

1.2.1 Utiliser systématiquement toutes les possibilités du droit pénal et de la protection préventive de l'Etat

Les compétences légales actuelles, pour autant qu'il soit possible d'influer sur elles au plan politique, sont déjà largement exploitées. Il n'est toutefois pas possible d'obtenir les informations nécessaires pour combler les lacunes en matière de sécurité au niveau politique et exécutif, même en interprétant et en appliquant le droit actuel de manière extensive. Il convient par ailleurs d'écarter toute instrumentalisation politique du droit pénal à des fins de prévention. Les procédures pénales ne doivent pas être employées pour satisfaire les besoins des responsables politiques en matière d'information ni pour obtenir des informations relevant du renseignement, par exemple en réduisant les exigences liées à l'ouverture de ces procédures ou en les ouvrant sur ordre des organes responsables de la politique de sécurité. L'indépendance des poursuites pénales doit demeurer garantie, quand bien même celles-ci peuvent fournir ponctuellement des informations importantes pour le maintien de la sûreté intérieure. Mais les lacunes existantes en matière de détection précoce et d'évaluation de la situation ne sauraient être comblées par ces informations.

1.2.2 Améliorer les flux d'information et mieux coordonner entre elles la répression et la prévention

Le Conseil fédéral a déjà examiné de manière approfondie la coopération entre les autorités de poursuite pénale de la Confédération et le service de renseignements intérieur[30]. Il a estimé à cette occasion qu'il n'y avait pas lieu de légiférer en la matière.

1.2.3 Etendre le droit pénal sur le plan formel et matériel

Dans le cadre de son rapport donnant suite au postulat CPS, le Conseil fédéral a également examiné dans quelle mesure il convenait de légiférer afin de combattre plus efficacement le terrorisme et le crime organisé. Il en a conclu qu'il était prématuré d'édicter de nouvelles réglementations en la matière à l'heure actuelle. Au contraire, il est préférable selon lui d'attendre de pouvoir tirer les enseignements de jugements en cours ou à venir ainsi que de connaître les résultats du traitement du projet de révision LMSI par les Chambres fédérales.

1.2.4 Développer la protection préventive de l'Etat

Les lacunes constatées grèvent l'identification précoce et la prévention des menaces et, par conséquent, en premier lieu la protection préventive de l'Etat. Les tâches et les moyens de celle-ci étant régis par LMSI, il convient aussi d'apporter des améliorations à ce texte de loi. Là aussi, il est possible de s'appuyer sur un système qui a fait ses preuves avec les structures existantes.

En outre, les éléments suivants militent pour un renforcement de la LMSI:

- La prévention est un instrument de la politique de sécurité. Ce sont les responsables politiques, ou l'exécutif, qui définissent leurs besoins en matière de renseignement dans le cadre de la loi et qui attribuent les mandats correspondants. C'est à eux qu'il faut donner les moyens d'identifier suffisamment tôt les menaces pour la sécurité du pays et de les intégrer dans l'appréciation de la situation politique. Enfin, ce sont eux qui prennent des décisions en matière de politique de sécurité, en se fondant notamment sur les informations fournies par les instances fédérales et cantonales de sûreté, et qui en assument la responsabilité. Il convient par conséquent de corriger les lacunes constatées dans le dispositif de prévention dans le cadre de la LMSI, qui est appliquée sous le contrôle et la surveillance des autorités politiques.
- Le droit actuel n'autorise une reconnaissance précoce des dangers et une évaluation de la situation que dans une mesure limitée car les instruments existants ne permettent pas de réunir suffisamment d'informations sur les événements dans le pays ni d'effectuer une observation stratégique efficace des foyers de tensions identifiés.
- Tous les moyens conformes au droit doivent pouvoir être mis en œuvre pour lutter contre le terrorisme et les dangers analogues, c'est-à-dire aussi bien les

30 Cf. «rapport donnant suite au postulat CPS».

outils de répression que de prévention. L'identification précoce et la prévention des dangers, autrement dit des attentats terroristes ou autres, relèvent avant tout des services de renseignements.

- Les mesures de lutte contre les agissements terroristes doivent pouvoir être mises en œuvre suffisamment tôt pour identifier ceux-ci et les déjouer au stade de la planification et de la préparation. Il s'agit notamment d'observer efficacement les individus et les organisations dangereux et de coopérer de manière optimale sur le plan international. Mais, comme on a pu le constater à l'étranger, même lorsqu'un acte terroriste a déjà été commis, les informations fournies par les services de renseignements sont souvent d'une importance décisive pour l'identification rapide des auteurs.
- L'existence de grandes différences entre les instruments nationaux de sécurité débouche sur l'existence de standards différents. En faisant coïncider certaines attributions de nos services de renseignements avec ce qui a cours dans la plupart des pays voisins, on évitera de faire de la Suisse un espace de moindre sécurité.
- Le renforcement de la LMSI consolidera durablement la coopération internationale.
- Le renforcement de la LMSI n'irait pas à l'encontre des principes de la procédure pénale selon lesquels, d'une part, une enquête pénale ne peut être déclenchée que sur la base de soupçons d'infraction suffisamment solides et, d'autre part, les comportements répréhensibles doivent être décrits précisément.
- Le renforcement de la prévention permet également d'obtenir régulièrement des renseignements approfondis sur des groupes présentant un danger pour la sécurité et menant également des activités criminelles graves. Ces renseignements («intelligence») peuvent être d'une grande aide pour les autorités de poursuite pénale et permettre à celles-ci d'employer efficacement leurs ressources.
- Grâce aux enquêtes ciblées des services de renseignements et aux mesures préventives prises sur cette base, des infractions graves peuvent être évitées, ce qui permet également de renoncer à des procédures pénales de grande ampleur et de décharger en conséquence les autorités judiciaires.

1.2.5 Autres projets législatifs

La législation en matière de police et de poursuite pénale connaît un régime permanent d'adaptation et de modernisation. De nombreuses conventions internationales, lois et ordonnances sont actuellement en cours de création ou de révision. Il n'y a pas de rapport direct notable entre ces travaux législatifs et le présent projet.

Citons, dans ce contexte, la révision permanente du droit fédéral de la police (cf. 06.3285, Interpellation Banga, Sécurité intérieure. Réglementation constitutionnelle et répartition des compétences entre la Confédération et les cantons) ainsi que l'élaboration en cours de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP) et de la loi sur l'usage de la contrainte dans le cadre du droit des étrangers et des transports de personnes ordonnés par une autorité fédérale (loi

sur l'usage de la contrainte, LUsC) ou encore la création d'une disposition constitutionnelle relative au hooliganisme.

La présente révision vise en premier lieu à améliorer la collecte préventive d'informations destinées à l'évaluation de la situation en matière de politique de sécurité et les mesures prises sur cette base dans l'intérêt de la sûreté intérieure et extérieure du pays.

L'adaptation des bases légales relatives au service de renseignements stratégique rattaché au DDPS est examinée séparément. Le service de renseignements extérieur étant soumis à des exigences légales passablement différentes de celles régissant le service de renseignements intérieur, lequel effectue un travail de police, seul un volet particulièrement important touchant les deux services (l'exploration radio stratégique) est traité par la présente révision.

1.3 Les nouvelles dispositions proposées

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'inttention 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, les activités de renseignements politiques ou militaires prohibées et le transfert illégal de biens de technologie (prolifération d'armes de destruction massive), de fournir des informations exhaustives. Les transporteurs commerciaux seront aussi tenus de fournir des renseignements aux mêmes conditions, dans la mesure où les données qu'ils auront déjà récoltées seront nécessaires. Par ailleurs, il sera possible d'utiliser des moyens spéciaux de recherche d'informations sous certaines conditions strictes. En cas de soupçons fondés de menace pour la sécurité intérieure, 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 de systèmes de surveillance techniques – et de perquisitionner secrètement des systèmes informatiques, là aussi uniquement dans le cadre de la lutte contre le terrorisme, contre les activités de renseignements politiques ou militaires prohibées et contre la prolifération.

L'utilisation de moyens spéciaux de recherche d'informations sera soumise à un double contrôle: à la demande de l'Office fédéral de la police, le Tribunal administratif fédéral examinera si les mesures sont conformes au droit (procédure d'autorisation). Dans le cadre de la décision rendue par le Tribunal administratif fédéral, le chef du DFJP et le chef du DDPS examineront ensuite la demande sous l'angle politique et décideront d'un commun accord des mesures (procédure de décision). En cas de décision négative du Tribunal administratif fédéral, la procédure de décision sera annulée.

La personne visée devra être informée ultérieurement qu'elle a fait l'objet d'une surveillance spéciale, sauf dans des cas précis où des intérêts publics prépondérants l'exigent et où la protection de tiers serait compromise. Le Tribunal administratif fédéral ou les chefs du DFJP et du DDPS déterminent les exceptions à l'obligation de communiquer dans le cadre d'une procédure analogue à celle applicable lors de l'emploi de moyens spéciaux de recherche d'informations (procédure d'approbation ou procédure de décision).

Le chef du DFJP doit recevoir la compétence d'interdire certaines activités à une personne, une organisation ou un groupement (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. Jusqu'ici, seul le Conseil fédéral était habilité à faire cela pour une période déterminée, dans le cadre des compétences spéciales qui lui sont conférées par la Constitution. En contrepartie, les personnes concernées obtiennent un droit de recours qu'elles ne pourraient en principe exercer contre les décisions et les ordonnances du Conseil fédéral fondées directement sur la Constitution.

La possibilité de recourir à des informateurs et le statut de leurs indemnisations (non soumises à l'AVS ni à l'impôt) doivent être inscrits formellement dans une loi; 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. Cette possibilité, existant déjà pour le service de renseignements stratégique, doit être étendue au service de renseignements intérieur. 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.

1.4 Développement et évaluation des solutions proposées

La situation de la Suisse en matière de sécurité et de menaces s'est peu à peu dégradée au cours des dernières années, essentiellement à cause de l'évolution sur le plan international. La probabilité accrue que des attentats terroristes islamistes soient commis a rendu la situation, lentement mais sûrement, de plus en plus imprévisible. Les moyens laissés aujourd'hui aux services de renseignements pour recueillir des informations ne permettent plus d'identifier les dangers de manière précoce, comme l'exigerait l'évolution de la situation. Il existe un vide de connaissance dangereux. L'absence de reconnaissance des situations dangereuses, ou une reconnaissance trop tardive, fait que l'on prend des mesures de prévention trop tard (pour autant que cela soit encore possible après un attentat terroriste) et que l'on met ainsi la population en danger.

Une meilleure collecte d'informations est nécessaire pour que l'on puisse prendre des mesures de prévention à temps, et cela exige parfois certaines atteintes à la sphère privée. De telles atteintes aux droits fondamentaux doivent être possibles sur la base d'indices concrets d'une grave mise en danger de la sûreté intérieure de la Suisse et doivent se dérouler sous contrôle judiciaire et sous la responsabilité

politique du chef du DFJP. En d'autres termes, le régime actuel d'interdiction générale de violer la sphère privée, mis en place dans un contexte différent de celui d'aujourd'hui, doit être remplacé par un régime d'interdiction assorti d'autorisations. Cela ne concernerait qu'un petit nombre de cas par années, mais ces cas sont potentiellement graves.

Tous les moyens disponibles doivent être mis en œuvre pour lutter contre le terrorisme et les dangers analogues, aussi bien les instruments de répression que ceux de prévention. Identifier de manière précoce les menaces, autrement dit les risques d'attentats terroristes ou d'autres menaces analogues, et les empêcher de se concrétiser sont des tâches qui relèvent avant tout de la prévention et incombent par conséquent aux services de renseignements.

1.4.1 Résultats de la procédure de consultation

A l'exception de Berne, tous les cantons approuvent expressément le projet ou le principe, en émettant parfois des réserves. Certains d'entre eux souhaitent que la nécessité de la révision soit motivée de manière plus détaillée.

Le Parti évangélique populaire et le Parti libéral approuvent le projet.

Le Parti démocrate chrétien donne son accord de principe. Le Parti radical démocratique estime que la révision de la loi va dans la bonne direction, mais il réclame certaines modifications. Il estime également que la conduite et la coordination des services de renseignements doivent être clarifiées.

Le projet est rejeté par l'Union démocratique du centre (privilégiant la neutralité par rapport aux mesures de surveillance préventive), par le Parti socialiste (les moyens de poursuite pénale seraient suffisants et pourraient être étendus le cas échéant) et par les Verts (pas d'investigations «préventives» sans soupçons concrets).

Selon le Tribunal fédéral, la proportionnalité des mesures pourra être évaluée dans la pratique des autorités et dans les décisions des tribunaux. On peut en conclure que le Tribunal fédéral a jugé les mesures proposées comme étant applicables dans le respect des droits fondamentaux.

L'Association des communes suisses et l'Union des villes suisses approuvent le projet.

Economiesuisse soutient une adaptation des instruments aux nouvelles menaces tout en réclamant un renforcement de la protection juridique. Swiss Banking exprime sa compréhension pour les mesures proposées. L'Union syndicale suisse rejette le projet (la législation actuelle serait suffisante).

De nombreux avis diamétralement opposés ont été exprimés. Dans le camp du refus, on trouve des organisations comme Amnesty International (le droit pénal serait suffisant), les Juristes démocrates («moins on aura de soupçons, plus on surveillera») ou les Préposés suisses à la protection des données (les garanties de respect des droits fondamentaux seraient insuffisantes). En revanche, les organisations de police comme la Conférence suisse des commandants des polices cantonales, la Fédération suisse des fonctionnaires de police ou la Conférence des directrices et des directeurs de police des villes suisses soutiennent le projet. Les organes de poursuite pénale estiment certes que les structures actuelles pourraient être améliorées mais ils n'en

reconnaissent pas moins la nécessité de méthodes d'investigation adaptées. Ils rappellent en outre l'importance fondamentale de la protection juridique.

La nécessité du projet en tant que tel est au centre des critiques. D'autres critiques de principe visent le manque de définitions légales du terrorisme et de l'extrémisme violent, les procédures d'approbation et de décision relatives à la recherche spéciale d'informations (p. ex. ces procédures ainsi que la notion d'avis du Tribunal administratif fédéral et les implications de celui-ci seraient peu claires) et la protection juridique (p. ex. le manque de pouvoir d'examen du Tribunal administratif fédéral entraverait l'efficacité de la procédure de recours).

D'autres éléments font l'objet de critiques (plutôt ponctuelles), comme la présentation électronique de la situation (p. ex. parce qu'il s'agirait d'une collecte de données conformément à la loi sur la protection des données), la réglementation au niveau fédéral de la consultation des données de la Confédération par les autorités cantonales de contrôle (qui serait incompatible avec l'autonomie organisationnelle des cantons et des communes), le devoir de renseigner s'appliquant aux autorités et aux transporteurs professionnels (la nécessité d'une réglementation non limitée dans le temps ne serait pas claire), la réglementation relative aux informateurs (pas de système d'incitation pour des personnes privées), les identités d'emprunt (seulement en cas de procédure pénale), la protection absolue des sources (pas de protection pour des informateurs encourant une peine ou étant de mauvaise foi), les moyens spéciaux de recherche d'informations (examiner l'extension du champ d'application à l'extrémisme violent et au crime organisé), l'obligation de communiquer ultérieurement (clarifier le rapport entre l'obligation de communiquer ultérieurement et le droit indirect d'être renseigné), la procédure d'urgence (garantir la destruction de données déjà transmises à l'étranger en cas de non-autorisation ultérieure de la mesure), et l'interdiction d'activités (ne pas interdire des activités sans qu'il soit commis d'actes pouvant être sanctionnés pénalement).

1.4.2 Modification de l'avant-projet

Le Conseil fédéral a pris connaissance le 4 avril 2007 des résultats de la procédure de consultation et a chargé le DFJP de rédiger un message; il a approuvé le même jour les principes applicables à la suite des travaux.

La rédaction du message s'est fondée sur le projet mis en consultation. Il a largement été tenu compte des principales objections, remarques et propositions issues de la consultation.

Les principales modifications par rapport au texte mis en consultation sont les suivantes:

- le réexamen et l'approfondissement de l'argumentation visant la nécessité du projet ainsi que des termes et des procédures jugés peu clairs, en particulier la procédure du Tribunal administratif fédéral et la procédure de décision par l'exécutif;
- le renforcement effectif de la protection juridique par l'extension du pouvoir d'examen du Tribunal administratif fédéral;
- le renoncement à une réglementation fédérale de la consultation des données de la Confédération par les autorités cantonales de contrôle;

– le renoncement à une protection étendue des sources;
– l'organisation de la présentation électronique de la situation comme un fichier au sens de la loi sur la protection des données;
– la désignation de la forme écrite pour la garantie donnée par l'Etat demandeur dans les procédures de clearing.

Pour l'heure, il convient de renoncer encore à l'harmonisation de la protection des sources entre le SAP et le SRS. Des craintes ont été exprimées à ce propos lors de la procédure de consultation. En effet, le passage de la protection relative à la protection absolue des sources pourrait avoir comme effet que des délateurs de mauvaise foi discréditent, par des propos fallacieux, des citoyens honnêtes. Les réflexions du législateur au moment de l'élaboration de la LMSI allaient d'ailleurs aussi dans ce sens. Le législateur était d'avis de renoncer à une telle disposition, notamment dans le cas des agents infiltrés, car ceux-ci peuvent s'être rendus eux-mêmes coupables d'une infraction. La réglementation actuellement en vigueur pour le SAP permet cependant déjà d'adapter la protection des sources aux besoins du cas et évite des incohérences dans le domaine de la surveillance.

L'opportunité de définir légalement les notions de «terrorisme» et d'«extrémisme violent», ainsi que le réclamaient différents participants à la procédure de consultation, a été examinée de manière approfondie avant d'être rejetée, essentiellement pour deux raisons: premièrement, l'ordonnance d'application (OMSI) indique ce que l'on entend par «activités terroristes» et «extrémisme violent» (respectivement «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» et «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»); les activités visées sont donc déjà décrites de manière précise et il ne s'agit donc pas de notions floues. Deuxièmement, il n'existe pas à ce jour de définition uniforme et valable sur le plan international de la notion de terrorisme. L'élaboration d'une telle définition reviendrait en outre à anticiper l'évolution du droit international et, partant, à réduire la flexibilité de la législation nationale par rapport au droit international. Une réglementation au niveau de l'ordonnance permet quant à elle de prendre en considération l'évolution du droit international plus rapidement et plus simplement. A cela s'ajoute le fait que la frontière entre combattants de la liberté et terrorisme d'Etat n'est pas encore suffisamment claire. La décision-cadre adoptée par l'Union européenne (décision-cadre 2002/475/JAI) définit les actes terroristes et les sanctions que les Etats membres doivent prévoir dans leur législation nationale. Le but visé consiste à harmoniser les différentes définitions des actes terroristes. Cette harmonisation n'a cependant une influence qu'au niveau de la poursuite pénale (répression) et non au niveau du renseignement (prévention).

Par ailleurs, le texte de loi a été revu dans sa structure et il a été tenu compte pour ce faire de la révision de la LMSI relative à la violence lors de manifestations sportives et à la propagande incitant à la violence, entrée en vigueur entre-temps.

1.5 Harmonisation des tâches et du financement

La sécurité entraîne des coûts (rapport USIS II, thèse stratégique 10). Cependant, les coûts d'une prévention efficace sont toujours beaucoup moins élevés que ceux qu'entraîne la concrétisation d'un risque (p. ex. un attentat terroriste): victimes, blessés, dégâts matériels, insécurité, conséquences économiques, etc. Même avec une augmentation de 40 postes (le SAP est actuellement fort de quelque 140 postes, dont 90 affectés à la tâche centrale de la protection préventive de l'Etat au sens de la LMSI), la protection préventive de l'Etat restera, en comparaison européenne, nettement moins bien dotée que dans certains pays comparables (p. ex. Autriche, Belgique, Pays-Bas, Danemark) et ce, aussi bien en valeur absolue (nombre total de postes) qu'en pourcentage (nombre de postes par habitant). De par son ancrage dans les services de police, elle profite toujours de synergies étendues avec le système policier fédéraliste suisse.

Dans tous les cas, les coûts liés à la mise en œuvre de la révision de la loi se justifient compte tenu des intérêts et des valeurs en jeu.

1.6 Comparaison et liens avec le droit européen

1.6.1 Généralités

Les législations étrangères existantes et celles adoptées ou renforcées après le 11 septembre 2001 ne peuvent être appliquées telles quelles à la Suisse en raison des différences dans les situations de la menace, les systèmes politiques 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 intérieurs 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 intérieurs 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 organisationnelles et la marge de manœuvre politique et 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 schématiquement les mesures adoptées sur le plan légal et les compétences existant dans certains pays, ainsi que la protection juridique et le système de contrôle existant dans ces pays. On trouvera des explications détaillées à l'annexe 1. L'absence de réglementation légale expresse ne signifie pas forcément que la mesure en question n'est pas appliquée dans le pays concerné, mais que l'on considère, le cas échéant, qu'elle ne nécessite pas de réglementation ou qu'elle est comprise dans d'autres réglementations.

1.6.2 Comparaison juridique avec d'autres pays

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

1.6.3 Protection juridique et contrôles institutionnels à l'étranger

Pays	Contrôle ordinaire	Contrôle spécifique
Allemagne	*De manière générale:* 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 d'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.

Pays	Contrôle ordinaire	Contrôle spécifique
Autriche	Possibilité de recours auprès de la commission pour la protection des données, du tribunal administratif ou de la cour constitutionnelle.	*De manière générale:* 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	Demande de consultation à la Commission nationale de l'informatique et des libertés (CNIL)	*Surveillance de la correspondance par poste et télécommunication:* 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. Le préposé à la protection des données (Garante per la protezione dei dati personali) 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

1.6.4 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 en résulte 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 dispose pas de moyens nécessaires à l'identification précoce des dangers dans notre pays et à la coopération internationale, elle risque de se nuire à elle-même, car les autres Etats pourraient devenir réticents à lui 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 sont 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, on a souvent utilisé des moyens de recherche d'informations 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 en 2003.

La Suisse doit disposer du standard minimal des autres Etats européens. Il n'est pas nécessaire pour l'heure d'adopter des mesures plus poussées.

1.7 Mise en œuvre

La mise en œuvre peut être fondée presque entièrement sur des structures fédérales (Tribunal administratif fédéral, SAP, Service des tâches spéciales du DETEC) et cantonales (polices cantonales et autorités cantonales de sûreté) existantes.

1.8 Liquidation des interventions parlementaires

La motion Burkhalter[31] exige que les adaptations législatives nécessaires afin de rendre plus efficaces les mesures de prévention du terrorisme soient proposées à l'Assemblée fédérale. Il n'est pas possible, à l'heure actuelle, d'estimer dans quelle mesure le présent message répond à cette demande, car la motion est combattue et n'a, pour l'instant, pas encore été traitée par les Chambres fédérales.

31 04.3216 Motion Burkhalter. Lutte contre le terrorisme. Mesures préventives.

2 Commentaire des différentes dispositions

Structure générale

L'actuelle révision de la LMSI nécessite une modification de la structure générale de la loi. Les moyens de recherche d'informations actuels et «ordinaires», qui subsisteront, doivent être clairement distingués des moyens «spéciaux» de recherche d'informations et des conditions exigées pour les ordonner. C'est pourquoi la loi est complétée par le chapitre «Recherche spéciale d'informations», qui comprend deux sections: «Dispositions générales» et «Moyens spéciaux de recherche d'informations». La première section du nouveau chapitre définit les conditions générales permettant d'ordonner les moyens spéciaux de recherche d'informations; la deuxième section décrit chacun des différents moyens, à savoir la surveillance de la correspondance par poste et télécommunication, la surveillance de lieux qui ne sont pas librement accessibles (aussi au moyen d'appareils de surveillance techniques) et la perquisition secrète de systèmes informatiques. Le nouvel art. 13*a* introduit par le ch. I de la LF du 24 mars 2006 (en vigueur depuis le 1er janvier 2007) doit être déplacé en raison de la nouvelle subdivision de la LMSI (cf. ci-après le commentaire de l'art. 18*o*).

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 chap. 3*a*, et de celle des interdictions d'activités (let. b^{ter}), réglées dans le chap. 3*b*.

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 de la police peut prendre la direction des opérations. Cette compétence doit être complétée de manière à permettre à l'Office fédéral de la police 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 de la police garantit donc une coordination dans l'échange des informations entre les unités administratives (cantonales), qui conservent leur primauté. La notion de coordination indique que la mesure revêt essentiellement un caractère de coopération. Par ailleurs, le critère de l'importance significative énonce que l'échange réciproque d'informations doit présenter de nets avantages. Autrement dit, il faut que la coordination assurée par l'Office fédéral de la police 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, pour l'Office fédéral de la police, de se charger de la coordination.

Intérêt public et proportionnalité

Cette extension du rôle de l'Office fédéral de la police 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 processus et de réseaux complexes dépassant le cadre des frontières nationales. Par ailleurs, de nombreux échanges d'informations avec des partenaires étrangers sont décisifs dans ce contexte. 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. 5*a* 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).

Chapitre 3 Recherche et traitement généraux d'informations

En raison de la nouvelle structure de la loi, l'actuelle section 3 («Traitement des informations») devient le chap. 3: «Recherche et traitement généraux d'informations».

Le titre du chap. 3 nouvellement introduit permet de mieux délimiter la notion de recherche générale d'informations de celle de recherche spéciale d'informations. Le titre «Recherche et traitement généraux d'informations» correspond à la notion de recherche qui a été pratiquée jusqu'ici. Fondé sur des règles d'entraide administrative entre autorités, ce type de recherche ne porte pratiquement pas atteinte aux droits fondamentaux et correspond à la conception qu'avait le législateur en 1997 du rôle de la police préventive.

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

Art. 10a Présentation de la situation

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[32], art. 15, al. 3, LMSI et art. 4, al. 2, let. k, de l'ordonnance du 30 novembre 2001 sur le système de traitement des données relatives à la protection de l'Etat[33]).

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. événements majeurs). Il exploite un système d'information électronique, nécessaire à l'accomplissement de ses tâches. Le système de traitement des données relatives à la protection de l'Etat (ISIS) et le système d'information sur la situation ne sont techniquement pas reliés. Le système peut également contenir des données sensibles,

32 RS **172.213.1**
33 RS **120.3**

pour autant que celles-ci soient nécessaires à la présentation de la situation (cf. art. 3 de la loi fédérale du 19 juin 1992 sur la protection des données[LPD][34]).

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

L'introduction de l'art. 13*a* 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

La modification du titre de l'art. 13, en particulier le qualificatif «général», met en évidence le fait que le devoir de renseigner est applicable à tous les domaines d'application de la LMSI.

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 (cf. art. 13*a* ci-après), la délégation au Conseil fédéral doit être réduite, dans l'art. 13, aux seuls domaines restants, à savoir l'extrémisme violent et le service prohibé de renseignements économiques.

Al. 4

Cette disposition est maintenue et transférée dans un article autonome (cf. art. 13*b*)

Art. 13a Devoir spécifique de renseigner incombant aux autorités

En raison de la nouvelle structure de la loi, l'actuel art. 13*a* LMSI (Saisie, séquestre et confiscation de matériel de propagande) devient l'art. 18*o*; ce déplacement n'implique pas de changement matériel dans cette disposition (cf. commentaire de l'art. 18*o*).

L'art. 13*a* 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, et plus large, puisqu'elle vise toutes les autorités de la Confédération et des cantons ainsi que les organisations accomplissant des tâches de service public. Les banques cantonales ne tombent par exemple pas sous le coup de cette disposition, car elles n'exercent pas de fonctions souveraines en la matière.

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 la Suisse en s'attaquant à ses institutions parlementaires, judiciaires ou gouvernementales, et à miner son système démocratique en entravant l'exercice des droits populaires et en intimidant la population. Constituent de telles menaces le terrorisme, le

34 RS **235.1**

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. La liste des organes concernés se fonde sur l'art. 13, al. 3, LMSI ainsi que sur l'actuelle 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 sûreté intérieure et extérieure (RS *120.1*). Cette disposition prévoit que, lorsqu'une menace concrète relevant des champs d'application limités de cette disposition (terrorisme, service de renseignements politiques ou militaires prohibé, commerce illicite d'armes et de substances radioactives, transfert illégal de technologie) vise la sécurité de la Suisse, l'ensemble des pouvoirs publics (Confédération, cantons, communes) doit participer à la lutte contre ladite menace. A titre d'exemple, le Bureau de communication en matière de blanchiment d'argent (MROS) ou les autorités chargées des documents d'identité font aussi partie des unités administratives de la Confédération. Par unités administratives des cantons, on entend aussi celles des communes; elles sont comprises dans le terme «cantons». 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 à la situation, 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 (cf. al. 3).

L'expression «dans des cas particuliers» exprime l'idée que les autorités tenues de renseigner sont obligées en tout temps de fournir des renseignements, mais seulement dans des cas concrets et sur la base d'une demande précise que leur adressent l'Office fédéral de la police ou les organes de sûreté cantonaux agissant pour son compte. Le fait qu'il s'agisse de cas particuliers liés à une menace concrète justifie que les organes tenus de fournir des renseignements ne soient pas énumérés dans le détail.

Le destinataire des renseignements obtenus auprès des différentes autorités et organisations est l'Office fédéral de la police. Conformément au système adopté pour l'ensemble de la loi (cf. art. 7, al. 1, art. 13, al. 1, art. 14, al. 1, LMSI), les autorités désignées par les cantons pour accomplir les tâches de sûreté 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 de la police. S'il surgit un différend au sujet d'une obligation de renseigner, celui-ci opposera l'autorité ou l'organisation refusant les renseignements à l'Office fédéral de la police et non à l'autorité cantonale qui aura tenté de recueillir le renseignement pour le compte de la Confédération.

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 en particulier des éventuelles clauses de confidentialité, des codes de conduite et des procédures d'opération

permanentes («Standing operating Procedures»). Les circonstances liées à chaque cas sont déterminantes.

Al. 2

L'art. 13*a* règle la libération du secret de fonction. A ce titre, les autorités chargées des assurances sociales et les autorités fiscales ont fait valoir que, dans leur domaine, il ne s'agissait pas seulement de la libération d'un secret de fonction mais de la libération d'un secret de fonction qualifié, ce qui nécessitait une réglementation spéciale.

Dans le domaine des assurances sociales, la transmission des données est réglée en détail dans les lois spéciales qui s'y réfèrent. Elle constitue en soi un ordre fermé, global et exhaustif. De ce fait, le secret de fonction est levé à l'égard des organes de sûreté de la Confédération et des cantons dans chacune des lois spéciales lorsque les conditions prévues à l'art. 13*a* sont remplies. Dans ces lois spéciales, on trouve des réglementations analogues s'appliquant aux autorités chargées de l'aide sociale, aux tribunaux civils, aux tribunaux pénaux, aux autorités d'instruction pénale, aux offices des poursuites et aux autorités fiscales.

La situation se présente de façon moins homogène dans le domaine fiscal. Certaines dispositions fixent certes des prescriptions relatives à l'obligation de garder le secret, mais il n'existe, pour la transmission des données, aucun système comparable à celui appliqué dans le domaine des assurances sociales. De même, la notion de secret fiscal n'est définie à aucun endroit de manière explicite; on trouve quelques définitions dans la littérature, p. ex.: «Steuergeheimnis ist jede einer mit steuerlichen Aufgaben betrauten Person in Ausübung ihrer hoheitlichen Tätigkeit anvertraute oder ihr sonst wie zur Kenntnis gelangte persönliche Tatsache eines Steuerpflichtigen, die Steuerakten sowie die Verhandlungen innerhalb der Steuerbehörden[35]». Le secret fiscal va plus loin que le secret de fonction général en ce sens qu'il protège aussi les intérêts privés (protection de la personnalité). Considérant cela, il apparaît que le secret fiscal doit être traité dans une disposition spéciale. Il convient tout d'abord de stipuler que les autorités fiscales sont aussi tenues de fournir des renseignements. L'interlocuteur pour la communication des renseignements est l'autorité fédérale ou cantonale compétente pour l'impôt en question. Si l'office fédéral et l'autorité compétente s'entendent sur le devoir de renseigner, les informations peuvent être communiquées sans autres formalités. En cas de désaccord, la procédure prévue à l'art. 13*b* (Différends relatifs au devoir de renseigner) est applicable: la décision finale concernant le devoir de renseigner revient alors au Conseil fédéral pour les impôts fédéraux et au Tribunal administratif fédéral pour les impôts cantonaux et communaux. Cette procédure permet également d'appliquer de manière uniforme le droit de renseigner prévu à l'art. 13*a*, al. 4, du présent projet.

Al. 3

Les organes de sûreté ne déterminent pas eux-mêmes quelles organisations sont tenues à un devoir de renseigner. Il incombe par conséquent au Conseil fédéral de désigner par voie d'ordonnance chacune des organisations tenues de renseigner.

35 Weber, M.: Berufsgeheimnis im Steuerrecht und Steuergeheimnis, Zurich 1982, p. 139.

Al. 4

Les services mentionnés à l'al. 1, qui comprennent les services visés à l'al. 3, sont aussi autorisés à communiquer spontanément aux autorités de la Confédération et des cantons chargées d'accomplir des tâches au sens de la LMSI 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, ou au transfert illégal de technologie. Les services mentionnés aux al. 1 et 3 sont ainsi libérés de toute accusation de violation du secret de fonction. Cela dit, il n'existe aucun devoir de fournir systématiquement des renseignements.

Intérêt public et proportionnalité

Le nouvel art. 13*a* entend transposer définitivement dans la loi la règle de l'art. 13, al. 3, LMSI, 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, LMSI. 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).

L'art. 13, al. 3, LMSI, sur lequel se fonde ladite ordonnance, exige que les actes législatifs correspondants du Conseil fédéral soient limités dans le temps. Ainsi l'ordonnance qui se base sur cette disposition ne peut pas être prorogée indéfiniment. Le délai fixé par le législateur vise à inscrire les normes dans le droit ordinaire lorsque leurs dispositions doivent rester en vigueur durant une longue période. Il s'agit d'introduire la législation nécessaire dès que les règles qu'elle contient s'avèrent indispensables à long terme. Ces conditions sont remplies pour les raisons suivantes:

Après les attentats de Madrid en 2004, la menace que le terrorisme islamiste fait peser sur l'Europe a atteint une nouvelle dimension en juillet 2005[36]. 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 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. A ce titre, une enquête a été menée auprès des corps de police des cantons ainsi que des villes de Berne et de Zurich. Son objectif principal n'était pas de juger du nombre de renseignements fournis, mais d'évaluer le contenu des communications en termes de qualité, cette dernière étant plus importante que la quantité.

36 Rapport sur la sécurité intérieure de la Suisse 2005, p. 27.

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 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 prorogation de l'ordonnance.

D'une manière générale, le nombre de communications est plutôt faible, mais la qualité de leurs contenus s'est largement améliorée.

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, son maintien et 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.

Art. 13b Différends relatifs au devoir de renseigner

L'art. 13*b* s'applique lorsque l'Office fédéral de la police ou un organe cantonal de sûreté accomplissant des tâches sur son mandat demande la communication de renseignements sur la base des art. 13 ou 13*a* 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 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration [OLOGA][37]), il appartient à l'autorité commune de surveillance, c'est-à-dire au chef du département requérant ou au Conseil fédéral, de le trancher (cf. art. 9, al. 3, de la loi fédérale sur la procédure administrative [PA][38]). 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 DFJP.

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 de la police peut, s'il ne parvient pas à un accord avec cette autorité, déférer le différend au Tribunal administratif fédéral 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. la modification

37 RS **172.010.1**
38 RS **172.021**

demandée concernant l'art. 35, let. d, de la loi du 17 juin 2005 sur le Tribunal administratif fédéral[39]). La voie de l'action est ouverte à l'Office fédéral de la police 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 la Confédération. 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 de la police.

L'action au Tribunal administratif fédéral se substitue à la voie de la plainte au Tribunal pénal fédéral (cf. art. 13, al. 4, LMSI); les autres litiges en matière d'application de la LMSI relèveront également de la compétence du Tribunal administratif fédéral (cf. le nouvel art. 29*a*).

Les différends peuvent impliquer des autorités fédérales ou cantonales, des organisations accomplissant des tâches de service public ou des organes de l'administration fédérale décentralisée, tels que le Ministère public de la Confédération (art. 8 OLOGA).

Art. 13c Devoir de renseigner incombant aux transporteurs commerciaux

Cette disposition introduit un devoir de renseigner, comparable à celui prévu à l'art. 13*a*, mais s'adresse aux transporteurs commerciaux. Pour des raisons de proportionnalité, le cercle des organes visés par cette disposition a été limité aux transporteurs commerciaux, comme les entreprises de taxi, les compagnies aériennes, les entreprises de location de véhicules, les entreprises de chemins de fer, les transporteurs routiers, etc. Comme celui de l'art. 13*a*, ce nouveau devoir de renseigner incombant aux transporteurs commerciaux ne porte que sur certains types de menaces (terrorisme, service de renseignements politiques ou militaires prohibé, commerce illicite d'armes et de substances radioactives, transfert illégal de technologie).

Les actions de personnes reconnues comme dangereuses (p. ex. espions, terroristes, ingénieurs actifs dans le domaine de la prolifération, etc.) ne peuvent souvent être découvertes après coup que grâce à des renseignements relatifs à leurs déplacements (p. ex. documents relatifs à la location de véhicules, etc.). Il en va de même pour les transports de biens soupçonnés être liés à la prolifération ou pour les transferts de technologies qui sont sur le point d'être effectués ou qui l'ont déjà été.

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, l'art. 13*c* 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; le renseignement est fourni à titre gratuit.

Enfin l'expression «dans des cas particuliers» 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 de la police ou les organes de sûreté cantonaux agissant pour son compte.

39 RS **173.32**

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 parfois 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, car ce secteur est particulièrement important pour les organes de sûreté. 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, les informations détenues par les transporteurs privés peuvent revêtir 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 (p. ex. les collaborateurs d'entreprises secrètes étrangères) ou de certains biens (p. ex. le transport de biens soupçonnés être liés à la prolifération) et l'observation de la fréquence de tels 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 de la police.

La proportionnalité de la mesure dépend des circonstances concrètes du cas particulier. Comme il a déjà été mentionné, pour que les transporteurs commerciaux soient soumis au devoir de renseigner, il faut que le renseignement soit, dans le cas particulier, nécessaire pour déceler et prévenir une menace concrète visant la sûreté intérieure ou extérieure de la Suisse et que ladite menace relève de l'un des domaines d'application de la LMSI mentionnés plus haut. Dans ce cadre bien délimité, il convient de relever que le transporteur est seulement tenu de fournir des renseignements sur des informations dont il a déjà connaissance, et qu'il n'est donc pas tenu de rechercher activement des informations. L'atteinte à sa sphère professionnelle n'est donc pas disproportionnée. Par ailleurs, le renseignement ne concerne pas un domaine protégé par le secret professionnel ou protégé par une relation de confiance particulière. En règle générale, il s'agit davantage de renseignements relatifs à des événements qui se sont déroulés dans des lieux librement accessibles (p. ex. rues, chemins de fer, etc). Il n'est donc pas question ici d'atteinte disproportionnée à la sphère privée. Cela dit, dans la pratique, comme c'est le cas pour toute atteinte aux droits fondamentaux, l'intérêt public et l'intérêt privé (en particulier la protection de la sphère privée), méritant tous les deux une protection, doivent être confrontés avec attention et sur tous les plans dans chaque cas particulier. Il en résulte que les transporteurs commerciaux doivent être soumis au devoir de renseigner uniquement pour détecter et prévenir des menaces importantes.

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[40]; art. 35 LPD) 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.

La présente révision n'affecte en rien le secret professionnel, ce qui, compte tenu de son importance, est précisé de façon explicite à l'art. 13*d*. Ainsi, un médecin cantonal est certes tenu de fournir des renseignements généraux dans le cadre de ses fonctions conformément à l'art. 13*a*, mais n'est pas obligé de divulguer, dans le but de renseigner, les connaissances dont il dispose et qui relèvent du secret médical.

Art. 14, al. 3

L'art. 14 LMSI énumère exhaustivement les moyens de recherche d'informations actuellement autorisés auxquels peuvent 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 pour la recherche d'informations et doivent rester les instruments ordinaires des organes de sûreté, le recours aux moyens spéciaux de recherche d'informations du chap. 3*a* étant réservé à des circonstances particulières et n'intervenant qu'à titre subsidiaire.

Al. 3

Dans le droit actuel, cette disposition est importante car c'est elle qui pose l'interdiction générale, pour les organes de sûreté, de recourir à titre préventif à des mesures de contrainte prévues par la procédure pénale et à l'observation de faits dans des locaux privés. Or la présente révision vise désormais l'usage préventif de telles mesures, à savoir les moyens spéciaux de recherche d'informations, de façon exceptionnelle et à certaines conditions strictes. On passe donc d'un système d'interdiction générale à un système de «dérogations» soumises à 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. Cela dit, les nouveaux moyens spéciaux de recherche d'informations prévus sont formulés de manière restrictive et sont soumis à des contrôles sévères par les pouvoirs judiciaire et exécutif (cf. les commentaires relatifs au chap. 3*a*).

Art. 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 considérée comme comprise 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).

40 RS **311.0**

Par exploration radio contre des cibles à l'étranger, on entend d'une manière générale le fait de répertorier des rayonnements électromagnétiques émis à l'étranger ou par des satellites et pouvant être reçus en Suisse. Actuellement, cette opération peut être effectuée au moyen du système ONYX pour les communications par satellites ou au moyen d'une installation de réception en ondes courtes pour ce spectre de fréquences. Les développements techniques détermineront à l'avenir quels moyens et systèmes devront être utilisés pour les mandats d'exploration radio. En employant la notion générale d'exploration radio, le législateur entend laisser la marge de manœuvre nécessaire afin de pouvoir continuer à faire face aux évolutions techniques.

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 aussi répertoriés et transmis par les prestataires de télécommunications dans le cadre de leurs activités commerciales. 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. 9*a* OMSI. Cette disposition doit être transférée dans la loi dans le cadre de la présente révision. Ce transfert permettra de répondre à une demande de la Délégation des commissions de gestion, qui réclame une base légale expresse pour l'utilisation d'ONYX. La loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM)[41] est parallèlement modifiée pour permettre aux services de renseignements du DDPS d'utiliser l'exploration radio (cf. modification du droit en vigueur, ch. 3, art. 99, al. 1 et 1bis et art. 99*a*, LAAM). Ainsi les deux services de renseignements disposent, chacun pour leur domaine de compétence, d'une base légale formelle pour l'utilisation de l'exploration radio.

Le nouvel art. 14*a* correspond largement à la réglementation actuelle de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI)[42]. 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. 18*d* et 18*e*.

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 analyser les informations recueillies et il définit, d'autre part, ce qu'il faut entendre par «exploration radio». La définition inclut tous les 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.

L'utilisation d'ONYX se fonde ainsi sur une base légale formelle. Le SAP est détenteur de la compétence exclusive de collecter les données dans le cadre du mandat légal qui lui est attribué, mais charge le DDPS de le faire dans la pratique (cf. commentaire de l'al. 3).

41 RS **510.10**
42 RS **120.2**

Al. 3

Cette disposition, qui autorise l'Office fédéral de la police à collaborer avec d'autres instances fédérales ou cantonales pour procéder à l'exploration de signaux, consacre la pratique actuelle en matière de coopération technique entre les organes fédéraux. 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. Un raccordement à un système étranger de surveillance de signaux (p. ex. à «ECHELON») reste interdit.

Al. 4

L'al. 4 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. 99*a*). Afin d'éviter les disparités au profit des services de renseignements du DDPS qui pratiquent l'exploration radio, 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. 18*d* et 18*e* (cf. ci-après) doit toutefois être appliquée, dans la mesure où la mesure ou l'exploration radio 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 en principe accessibles au public. Les informations peuvent être reçues par toute personne disposant de l'équipement adapté. En ce sens, elle ne porte guère atteinte à la sphère privée et ne viole pas le secret des télécommunications. Si, en revanche, l'exploration radio 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. 18*k*. Nous renvoyons donc au commentaire relatif à cet article.

Art. 14b Informateurs

Pour accomplir leurs tâches, les organes de sûreté dépendent des communications et des renseignements de personnes qui ont accès aux informations pertinentes. 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, LMSI, à savoir les demandes de renseignements et la réception de communications). Il s'agit donc de combler cette lacune.

Al. 1

Cet alinéa autorise expressément l'Office fédéral de la police à recourir à des informateurs. L'informateur est une personne qui décide 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)[43] ou du droit du personnel de la Confédération. Le fait

[43] RS **220**

qu'un informateur puisse occasionnellement être indemnisé de ses frais ou percevoir une prime (cf. al. 2) ne suffit en soi pas à transformer ce rapport en un rapport de travail. Il faudrait réunir, pour un rapport de travail au sens de l'art. 310 CO, 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 de la police sous l'angle personnel, organisationnel et temporel. Or il n'y a en aucun cas intégration dans l'organisation de travail d'un tiers.

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 imposables au sens de la législation sur l'AVS. Il s'agit des frais découlant des activités menées par les informateurs, notamment des frais de voyage ou de télécommunication.

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 subissent pas une pression liée aux résultats. De modestes 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 du fait 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 sont les organes de contrôle ordinaires 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, si et 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; la charge administrative découlant de la saisie et de la perception des charges dépasserait largement les montants attendus.

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 travaillent avec des services de renseignements étrangers parce que ceux-ci peuvent, contrairement à la Suisse, 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 violents), soit d'Etats étrangers (p. ex. les informateurs qui se sont engagés auprès d'un service de renseignements étrangers 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.

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 pourraient certes être 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 concrètes, 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 infractions.

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, mais n'impliquerait pas une protection contre la poursuite pénale en Suisse.

Al. 1

Cet alinéa pose le principe de l'octroi d'une protection aux informateurs et fixe le type de mesures que l'Office fédéral de la police est tenu de prendre pour protéger la vie ou l'intégrité corporelle de l'informateur, c'est-à-dire des mesures de protection de personnes ou de changement du lieu de séjour. Par mesures de protection, on entend l'engagement de gardes du corps, de véhicules ou d'appareils de protection ou des mesures de construction; par changement du lieu de séjour, on entend un

déplacement en des lieux plus sûrs, en Suisse ou à l'étranger, après accord de la personne concernée. 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 de la police 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 seront nécessaires et que peu d'entre elles 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, en de tels cas, d'avoir recours à des autorités étrangères, ce qui permettrait aussi de prévoir les coûts. Des formes de protection partielle pourraient 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 de la police 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 fédéral de la police pour prendre les mesures adaptées au 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 fédéral de la police 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 de sa collaboration avec l'Office fédéral de la police, celui-ci est autorisé à lui constituer une identité d'emprunt durable pour le protéger et, par conséquent, l'informateur est en droit de l'utiliser aux conditions que l'Office fédéral de la police fixe. L'octroi d'une identité d'emprunt est soumise à l'approbation du Tribunal administratif fédéral et à 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 et les procédures fixées à cet effet pour la recherche spéciale d'informations sont respectées (voir ci-après, sur cette autre hypothèse, le commentaire de l'art. 14*d*).

Conformément à l'art. 27, al. 1bis, du présent projet, le département doit rendre compte régulièrement au Conseil fédéral et aux organes de contrôle parlementaires du nombre d'identités d'emprunt constituées, de leur utilisation 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 car elle doit être adaptée au cas d'espèce. A titre exceptionnel, le chef du département peut

renoncer à une telle limitation, si les risques encourus sont particulièrement graves et qu'il y a tout lieu de les tenir pour permanents.

Art. 14d Identités d'emprunt

Les services de renseignements et les autorités chargées de tâches de police préventive 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 (cf. commentaire de l'al. 1).

Depuis 1998, le Service de renseignement stratégique a la possibilité de constituer des identités d'emprunt pour ses agents, 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). Le contrôle relatif à ces identités d'emprunt est effectué par le chef du DDPS et par la Délégation du Conseil fédéral pour la sécurité.

Le chef du DFJP peut autoriser l'Office fédéral de la police à constituer des identités d'emprunt dans le cas d'espèce. Auparavant, le Tribunal administratif fédéral (art. 18*d*, procédure d'approbation) 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.

Il convient de relever que, dans le domaine du renseignement, les identités d'emprunt sont exclusivement liées à deux buts: la sécurité des collaborateurs et la recherche d'informations. Leur utilisation n'est autorisée dans aucun autre cas. Les possibilités de surveillance prévues par la législation en matière de procédure pénale ne peuvent pas non plus être utilisées, car les recherches effectuées par les services de renseignement conformément à la LMSI diffèrent de celles mises en place dans le cadre d'enquêtes pénales. En effet, elles se distinguent considérablement par l'élément qui les motive, l'objet des recherches et le but visé.

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. 18*a* ss est applicable. 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 en tant que collaborateurs 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 informateurs doivent aussi pouvoir être dotés d'une identité d'emprunt si cela est indispensable pour la recherche de renseignements. Pensons notamment aux personnes pour lesquelles l'identité d'emprunt est le seul moyen de s'infiltrer 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 d'accomplir des actes juridiques, notamment 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

Une identité d'emprunt doit en principe pouvoir être conservée tant qu'elle est nécessaire aux opérations. Son utilisation cesse une fois que les objectifs visés ont été atteints.

Afin de mieux pouvoir contrôler les risques liés à l'usage d'une identité d'emprunt, il est recommandé de limiter la durée de cet usage. Cette mesure est particulièrement indiquée en ce qui concerne les identités d'emprunt octroyées à des informateurs, lesquels, n'étant pas des employés de l'Office fédéral de la police, échappent à son pouvoir disciplinaire. L'identité d'emprunt doit par conséquent pouvoir être prolongée aussi longtemps que nécessaire tout en étant limitée dans le temps. Si une identité d'emprunt est toujours nécessaire après l'expiration de son délai ou de sa prolongation, une nouvelle demande doit être déposée.

Al. 3

L'al. 3 garantit que les identités d'emprunt ne sont utilisées qu'aux fins visées par la LMSI. Rappelons encore que, conformément à l'art. 27, al. 1bis, 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, dans le cadre duquel le département doit renseigner annuellement le Conseil fédéral et la Délégation des commissions de gestion à ce sujet.

Art. 15, al. 6

La disposition date de l'ancienne police fédérale, époque à laquelle la répression et la prévention étaient unies. La mise en œuvre de la séparation des aspects répressif et préventif a rendu 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.

Art. 17, al. 3, let. e

Al. 3, let. e

Les clearings font partie des activités effectuées depuis longtemps par le 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). Tel que souhaité par de nombreux participants à la consultation, l'Etat étranger requérant doit désormais assurer par écrit au SAP qu'il a obtenu l'accord de la personne concernée pour 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 mesure 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. 365 ss CP pour que l'Office fédéral de la police ait accès à VOSTRA aux fins du clearing. La présente modification de la LMSI constitue donc la 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.

Chapitre 3*a* Recherche spéciale d'informations

Le chap. 3*a* 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 spéciaux de recherche d'informations, dénommés ici «moyens spéciaux».

Le titre du chapitre 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 chap. 3 et qui se pratique avec les moyens ordinaires qui y sont énumérés. La recherche spéciale d'informations recourt à des moyens spéciaux, qui ne peuvent pas être employés dans tous les cas et ne peuvent l'être que pendant une durée limitée.

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

Art. 18a Principe

Al. 1

La recherche spéciale d'informations vise à déceler ou prévenir une menace concrète contre la sûreté intérieure ou extérieure de la Suisse. Conformément à l'art. 18*b* du présent projet, il faut que les organes de sûreté puissent, avant même d'utiliser des moyens spéciaux de recherche d'informations pour chercher à déceler ou à prévenir une menace, 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 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 ou de substances radioactives ainsi que le transfert illégal de technologie. Demandée par différents participants à la consultation, l'extension du champ d'application à l'extrémisme violent, au service de renseignements économiques et à la criminalité organisée a été écartée. S'agissant de la lutte contre la criminalité organisée, le Conseil fédéral estime qu'il faut d'abord attendre les résultats du projet d'efficacité.

Al. 2

L'al. 2 énumère de façon exhaustive les moyens spéciaux de recherche d'informations; aucun autre moyen ne peut donc être utilisé.

Art. 18b Conditions

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

Les quatre premières conditions sont de nature matérielle et répondent aux exigences de l'art. 36 Cst. Elles ont pour objet de définir l'intérêt public et les circonstances qui, en l'espèce, peuvent seuls 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 et extérieure de la Suisse et de la protection de la sécurité de collaborateurs de l'Office fédéral de la police contre les personnes, organisations et groupements qui représentent une menace pour la sûreté intérieure ou extérieure (ci-après dénommés «perturbateurs présumés»; cf. let. a).

La question de la protection en particulier ne doit pas être sous-estimée. En effet, les collaborateurs de l'Office fédéral de la police (ainsi que les sources humaines) peuvent, notamment dans le cadre de la recherche d'informations menée sur le plan opérationnel, être exposés à de graves menaces. En cas de nécessité fondée, des précautions doivent donc pouvoir être prises afin de les protéger. Généralement, il s'agit d'accompagner les personnes concernées lors de leur engagement et de pouvoir les mettre à l'abri à temps en cas de danger (p. ex. lorsqu'elles sont démasquées).

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) visée à la let. d in initio, selon laquelle le moyen doit être propre à atteindre le but d'intérêt public; la nécessité (Erforderlichkeit) aux let. c et d in fine, si les moyens non spé-

ciaux sont inefficaces; 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.

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

Al. 1

Cette disposition vise le cas d'une implication indirecte. Il arrive que le perturbateur présumé qui fait l'objet d'une recherche impliquant des moyens spéciaux de recherche d'informations utilise des choses ou des lieux qui appartiennent à un tiers, par exemple une ligne téléphonique ou un système d'informations local privé. L'utilisation se fera parfois même à l'insu de ce tiers. Ces moyens de communication et ces lieux qui ont un lien avec le perturbateur doivent toutefois pouvoir être surveillés.

Le texte précise bien que ce n'est pas le tiers qui est surveillé pour lui-même, tant qu'il n'est pas 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 et se soucie de la meilleure protection possible 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)[44]. Conformément à la jurisprudence de la Cour européenne des droits de l'homme (arrêt Kopp c. Suisse, du 25 mars 1998), le tri des résultats de la surveillance doit être opéré sous la surveillance d'une autorité judiciaire. Cet arrêt se rapportant à une procédure pénale peut être appliqué au domaine de la prévention. 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).

Les détenteurs du secret de fonction visés à l'art 321 CP sont les ecclésiastiques, avocats, défenseurs en justice, notaires, contrôleurs astreints au secret professionnel en vertu du code des obligations, médecins, dentistes, pharmaciens, sages-femmes, ainsi que leurs auxiliaires, à qui des faits ont été confiés en vertu de leur profession ou dont ils ont eu connaissance dans l'exercice de celle-ci. A titre d'exemple, les détenteurs de secrets décrits à l'art. 47 de la loi du 8 novembre 1934 sur les banques (LB)[45] ne tombent pas sous le coup de l'art. 321 CP. Une protection particulière ne se justifie pas dans ce cas – ni dans le droit de la procédure pénale – car l'utilisation de moyens spéciaux de recherche d'informations doit être autorisée tant par le Tribunal administratif fédéral que par les chefs respectifs du DFJP et du DDPS. Ces derniers peuvent, tout au plus, prendre en compte des intérêts de protection justifiés. Par ailleurs, la banque n'est pas tenue de fournir activement des renseignements (elle garantit ainsi le secret bancaire). Il s'agit ici uniquement de savoir si un juge du Tribunal administratif fédéral surveille ou non le tri des données recueillies

44 RS **780.1**
45 RS **952.0**

lors d'une surveillance. Par ailleurs, en vertu de l'art. 47 LB, tous les organes et employés d'une banque notamment sont tenus au secret; au vu du nombre concerné, un règlement d'exception n'aurait aucun sens.

Art. 18d Procédure d'approbation

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 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)[46] 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, 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 et de façon échelonnée. 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 du Tribunal administratif fédéral (contrôle a posteriori). Ce système de communication et de recours est prévu, dans le projet de loi, aux art. 18*i* (Obligation de communiquer) et 29*a* (Voies de droit).

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, la loi permet, à certaines conditions, de renoncer provisoirement, voire durablement, à la communication (cf. art. 18*i*, al. 2, du projet de loi). 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 et qui soit aussi strict que celui qui serait exercé dans le cadre d'une procédure de recours.

En procédure répressive, le contrôle est normalement prescrit par la loi et assumé par une autorité judiciaire dès que la mesure a été ordonnée. Quand les moyens spéciaux sont employés à des fins de prévention, il n'y a aucune raison de faire l'économie du contrôle judiciaire car les atteintes aux droits fondamentaux sont similaires. 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 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 et le Tribunal fédéral ont donné deux réponses qui ne convergent pas: s'agissant de la pratique courante, la Cour estime qu'un organe quasi judiciaire suffit. Le Tribunal fédéral paraît préférer l'intervention d'une autorité judiciaire formelle.

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

46 RS **0.101**

une commission du Bundestag et statuant en pleine indépendance, satisfaisait aux exigences de l'art. 8, al. 2, CEDH en tant que cette loi 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 l'arrêt Klass, § 21, 53 et 60) et que son but est justifié compte tenu 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 Telefonüberwachung als geheim durchgeführte Massnahme … bedarf einer richterlichen Prüfung» (ATF *122* I 182, 190, T., du 2 mai 1996). Dans le second cas, il s'est agi toutefois d'examiner le recours aux mesures de surveillance lors de procédures pénales formelles.

Ce qui, toutefois, n'est pas tout à fait clair, c'est de savoir 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 d'une instance judiciaire, considérée comme «souhaitable» par la Cour européenne dans le cadre de la CEDH, est «obligatoire» dans le système constitutionnel suisse ou non.

Devant cette incertitude, le Conseil fédéral a retenu, dans le cadre du présent projet de loi, l'autorisation octroyée par une instance judiciaire.

Le domaine préventif étant une activité dont la conduite, le contrôle et la responsabilité incombent, dans le cadre de la loi, aux autorités politiques, le projet de loi prévoit une double procédure de contrôle, ajoutant ainsi une composante politique. L'Office fédéral de la police dépose une demande écrite dûment motivée, sur la base de laquelle le Tribunal administratif fédéral vérifie les mesures demandées (procédure d'approbation). C'est seulement une fois que le Tribunal administratif fédéral a approuvé la mesure que le chef du DFJP examine la demande, consulte le chef du DDPS et, en cas d'accord réciproque, décide de façon définitive d'ordonner l'exécution de la mesure (procédure de décision). La demande est donc soumise à un examen judiciaire, et à un examen (double lui aussi) portant sur différents points relevant de la politique de l'Etat (effectué par le pouvoir exécutif). L'utilisation de

moyens spéciaux de recherche d'informations n'est autorisée que si et dans la mesure où toutes les instances donnent leur accord.

Cette procédure, qui a été consolidée par rapport à celle soumise à la consultation, tient compte de l'avis de nombreux participants à la consultation, lesquels ont certes approuvé la double procédure de contrôle mais ont estimé que la procédure proposée en consultation manquait de clarté.

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 les juges compétents tiendront compte de manière appropriée des exigences liées au maintien du secret lors du traitement des cas; pour cette raison, l'alinéa qui s'y référait dans le projet mis en consultation a été supprimé.

Al. 4

Le Tribunal administratif fédéral a pour tâche de juger du caractère conforme au droit de la constitution d'identités d'emprunt (cf. art. 14*c*, al. 3 et 4, et art. 14*d*). 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. 14*c*, al. 3, et à l'art 14*d*, 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, la décision du Tribunal administratif fédéral a un caractère impératif (cf. art. 14*c*, al. 3, et art. 14*d*, al. 1). Dans ce domaine, les décisions du Tribunal administratif fédéral sont définitives.

Art. 18e Procédure de décision

Al. 1

La procédure de décision fixée à l'art. 18*e* se conforme à la procédure d'approbation prévue à l'art. 18*d*. L'Office fédéral de la police ne peut demander au chef de département l'utilisation de moyens spéciaux de recherche d'informations qu'une fois que le Tribunal administratif fédéral a approuvé la mesure. A la demande de nombreux participants à la consultation, la disposition précise en même temps explicitement que la décision doit toujours être prise dans les limites prévues par le Tribunal administratif fédéral («dans les limites de la décision du Tribunal administratif fédéral»); la décision correspondante doit donc être jointe à la demande.

La dernière phrase de l'al. 1 dispose que l'Office fédéral de la police informe le département des demandes refusées par le Tribunal administratif fédéral. Cette procédure permet à la direction du département d'avoir une vue d'ensemble sur toutes les demandes déposées par l'Office fédéral de la police, et pas seulement sur les demandes qui ont été approuvées par le Tribunal administratif fédéral.

Al. 2 et 3

Le chef du DFJP consulte le chef du DDPS et décide ensuite, en cas d'accord réciproque, d'ordonner l'exécution de l'utilisation des moyens spéciaux de recherche d'informations approuvés par le Tribunal administratif fédéral; sa décision est définitive; en outre, aucune délégation de la décision n'est possible. Si le chef du DFJP et celui du DDPS n'arrivent pas à se mettre d'accord sur l'engagement de moyens spéciaux de recherche d'informations demandé, l'utilisation effective desdits moyens ne peut être ordonnée.

Même si le Tribunal administratif fédéral approuve la mesure demandée, le chef du DFJP et le chef du DDPS peuvent renoncer partiellement ou complètement d'un commun accord à l'exécution de la mesure ou ils peuvent assortir l'exécution de restrictions ou de charges supplémentaires (p. ex. l'obligation d'informer régulièrement de l'exécution de la mesure).

Selon les cas, le chef du DFJP peut consulter les chefs d'autres départements pour prendre sa décision (p. ex. le chef du DFAE lorsqu'il s'agit de politique étrangère).

Art. 18f Procédure d'urgence

L'art. 18*f* prévoit une procédure spéciale pour les cas où il y a péril en la demeure. Il faut pouvoir agir rapidement dans les cas où le fait d'attendre la décision du Tribunal administratif fédéral ou des chefs du DFJP et du DDPS compromet l'efficacité des 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 une surveillance des télécommunications doit aussi être mise en place.

Al. 1

Dans les cas d'urgence, le directeur de l'Office fédéral de la police ordonne directement les moyens spéciaux de recherche d'informations afin qu'ils puissent être immédiatement mis en œuvre. Même dans de tels cas d'urgence, toutes les conditions matérielles liées à l'emploi d'un moyen spécial (art. 18*b* du projet de loi) doivent être entièrement remplies. Il appartient au directeur de l'Office fédéral de la police de s'en assurer. Le chef du département doit être informé dans le même temps.

Al. 2

Le directeur de l'Office fédéral de la police est tenu de soumettre la demande habituelle au Tribunal administratif fédéral dans les 24 heures, en motivant l'urgence de la mesure. La procédure suit ensuite son cours ordinaire. Comme dans la procédure «ordinaire», le Tribunal administratif fédéral doit communiquer sa décision dans les 72 heures à l'Office fédéral de la police.

Al. 3

La demande de l'Office fédéral de la police visant à ordonner a posteriori l'utilisation de moyens spéciaux de recherche d'informations et à poursuivre l'exécution est déposée dans le cadre de la décision du Tribunal administratif fédéral concernant la conformité au droit. La demande doit être soumise immédiatement. Ici aussi, il faut l'accord réciproque du chef du DFJP et du chef du DDPS pour que l'utilisation des mesures puisse être ordonnée.

Al. 4

Si le Tribunal administratif fédéral refuse la demande ou si le chef du DFJP, après avoir consulté le chef du DDPS, n'ordonne pas la poursuite de l'exécution dans les 48 heures, l'Office fédéral de la police doit suspendre la mesure et détruire immédiatement toutes les données collectées jusqu'alors dans le cadre de cette recherche d'informations (cf. la disposition analogue de l'art. 7, al. 4, LSCPT).

Si l'Office fédéral de la police a déjà transmis à d'autres organes ou autorités des informations issues d'une mesure refusée, il doit leur demander de procéder à leur destruction.

Lors de la procédure de consultation, il a été question de savoir comment, en cas de décision négative, garantir que les données qui auraient éventuellement été transmises à l'étranger seront détruites.

A cet égard, on peut préciser ce qui suit. Lors de procédures d'urgence, il faut généralement s'attendre à ce que l'éventuelle transmission d'informations aux services partenaires étrangers (p. ex. informations concernant les projets de voyages d'une personne cible) doive se faire rapidement (en l'espace de quelques heures); il n'y a donc pas le temps pour des procédures judiciaires préalables (p. ex. décisions superprovisionnelles). Selon le droit en vigueur, les services partenaires étrangers ne doivent utiliser les informations reçues que dans le but dans lequel elles ont été transmises. Le SAP peut exiger des renseignements quant à leur utilisation, et informer les autorités étrangères concernées à propos de la rectification ou de l'effacement de données. Il est certes exclu pour les organes suisses de s'assurer auprès de services de renseignements étrangers ou d'autorités de sécurité étrangères de la destruction effective ou de l'utilisation de données. Toutefois, il faut s'attendre à ce que, en cas de rejet de la demande, les données déjà parvenues à l'étranger soient détruites si le SAP le demande. En effet, d'une part, ni les services de renseignements suisses ni les services de renseignements étrangers n'ont intérêt à détenir des données déclarées comme «fausses» ou non autorisées. D'autre part, la transmission d'informations à des pays étrangers se fonde généralement sur le principe selon lequel l'information transmise ne doit pas être transmise plus loin sans l'accord explicite du SAP (règle dite «du service tiers»). Il va de soi qu'en pareil cas, le SAP ne donnerait pas son accord à la transmission à des services tiers et que les données perdraient de ce fait leur valeur aux yeux du service étranger concerné. Enfin, il convient de relever que l'échange d'informations avec des services étrangers se déroule, contrairement aux cas d'entraide judiciaire, sur une base volontaire. Si un service partenaire étranger ne se tient pas aux règles, la Suisse peut suspendre ou limiter la collaboration en tout temps.

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, que le chef du DFJP, après consultation du chef du DDPS, l'a refusée ou ne l'a pas ordonnée dans les 48 heures (let. d et e), l'Office fédéral de la police l'interrompt immédiatement. Le principe de proportionnalité doit permettre dans ce cas, non seulement de suspendre l'emploi des moyens spéciaux dans leur totalité, mais aussi, si la recherche spéciale d'informations continue à durer, de suspendre l'emploi de certains des moyens appliqués.

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

Al. 1

Cette disposition précise le régime général de la conservation des données visées 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.

En raison de considérations pratiques et juridiques, il n'est pas possible de donner suite aux remarques faites à quelques reprises lors de la consultation, selon lesquelles le tri des informations ne doit pas être effectué par l'Office fédéral de la police ou doit au moins être contrôlé par le Tribunal administratif fédéral. Le tri des informations nécessaire présuppose d'une part une connaissance approfondie des cas que des personnes externes ne peuvent que difficilement assimiler en si peu de temps et avec des moyens raisonnables. D'autre part, le travail de l'Office fédéral de la police est déjà contrôlé de manière approfondie par différentes instances (inspectorat interne au département, surveillance parlementaire, etc.), ce qui exclut la nécessité de créer un instrument de contrôle supplémentaire.

Art. 18i Obligation de communiquer

Cette règle est l'un des éléments déterminants du projet de loi: elle est primordiale pour le contrôle juridique a posteriori. C'est seulement en étant informées que les personnes concernées pourront faire valoir leur droit de recours fixé à l'art. 29*a* auprès des tribunaux.

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. En vertu de l'arrêt du Tribunal fédéral *109* Ia 273, 298–299, cela vaut pour l'observation à titre préventif et répressif, à l'égard de prévenus, de suspects et de tiers. Il y a donc en principe obligation de faire savoir aux personnes concernées qu'elles ont fait l'objet de mesures d'observation.

Si, après usage de moyens spéciaux, l'Office fédéral de la police n'informe pas la personne concernée que des informations la concernant ont été récoltées grâce à de tels moyens, celle-ci ne pourra en général pas l'attaquer, à moins qu'elle n'en ait eu connaissance par une autre voie. C'est pourquoi, dans de tels cas, une procédure judiciaire supplémentaire doit garantir la conformité au droit, comme lors de procédures pénales.

Al. 1

Fondé sur cette jurisprudence, le présent projet de loi consacre le principe du droit d'être renseigné ultérieurement. Lorsqu'une opération est terminée, l'Office fédéral de la police doit, en principe, communiquer à la personne concernée dans un délai d'un mois qu'elle a fait l'objet de recherches (sur la notion d'opération, voir l'art. 14 OMSI)[47].

Il n'est ni justifié ni possible d'étendre l'obligation de communiquer à la recherche générale d'informations ou à toutes les personnes visées par la surveillance, comme

47 RS **120.2**

l'avaient souhaité quelques participants à la consultation. D'une part, la recherche générale d'informations ne porte atteinte que de façon marginale aux droits fondamentaux. D'autre part, il en résulterait de lourdes charges administratives. Il ne s'agirait pas seulement de communiquer l'exécution de milliers de recherches par an (même si celles-ci n'ont mené à aucun résultat), mais aussi d'identifier une multitude de personnes supplémentaires (pas seulement les personnes concernées, mais aussi les personnes présentes par hasard). De même, il n'y a pas lieu d'informer les tiers concernés par hasard de la surveillance ou de procédures pendantes visant les personnes cibles.

Al. 2 et 3

Dans l'arrêt Klass précité (§ 57 à 59, voir le commentaire de l'art. 18*d*), la Cour européenne des droits de l'homme a reconnu que 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 les mêmes 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 relativisés par les nécessités de la procédure pénale. 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[48] et à l'art. 22, al. 2, LFIS[49]. La liste mentionnée aux let. a à d est exhaustive.

Une personne est par exemple aussi considérée comme ne pouvant pas être atteinte (let. d) lorsque la localisation de son lieu de séjour implique le déploiement de moyens disproportionnés ou lorsque son lieu de séjour est connu mais que la prise de contact exigerait des moyens disproportionnés (notamment à l'étranger).

Par ailleurs, la renonciation temporaire ou durable à la communication n'est pas de la compétence de l'Office fédéral de la police. 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 de la police dépose une demande dûment motivée indiquant pourquoi il conviendrait de renoncer à la communication. Le Tribunal administratif fédéral procède ensuite à un contrôle judiciaire de cette demande. S'il décide que la renonciation à communiquer est conforme au droit, le chef du DFJP consulte le chef du DDPS, comme le prévoit l'art. 18*e*, et prend la décision. En d'autres termes, la procédure appliquée ici est donc la même que lorsque des moyens spéciaux de recherche d'informations sont ordonnés.

48 RS **780.1**
49 RS **312.8**

Le droit d'accès au sens des art. 8 à 10 LPD, qui est réglé par l'art. 18 LMSI (appelé «droit d'accès indirect»), doit être différencié de l'obligation de communiquer ultérieurement. Selon cette disposition, toute personne peut demander au Préposé fédéral à la protection des données et à la transparence qu'il vérifie si des données la concernant sont traitées conformément au droit dans le système d'information de l'Office fédéral de la police. Le Préposé fédéral à la protection des données et à la transparence communique au requérant une réponse au libellé toujours identique selon laquelle aucune donnée le concernant n'a été traitée illégalement ou que, dans le cas d'une éventuelle erreur dans le traitement des données, il a adressé à l'office fédéral la recommandation d'y remédier.

A la différence de la communication ultérieure, qui présuppose qu'un moyen spécial de recherche d'informations a été utilisé, le droit d'accès indirect peut être exercé sans conditions. Toute personne peut donc faire vérifier en tout temps par le Préposé fédéral à la protection des données et à la transparence si ses données sont traitées en toute conformité. La personne concernée peut demander que le président de la cour du Tribunal administratif fédéral qui est compétente en matière de protection des données examine la communication du Préposé fédéral à la protection des données ou l'exécution de la recommandation qu'il a émise.

Cette possibilité de faire vérifier en tout temps le traitement des données effectué par le SAP fixe un niveau de contrôle élevé, mais elle se justifie par le fait que la personne concernée n'a, en règle générale, pas le droit de consulter le dossier la concernant. Cette solution permet d'une part de garantir que les intérêts de la personne concernée soient pris en considération correctement dans leur totalité, d'autre part elle permet d'éviter qu'une personne peut-être dangereuse puisse prendre connaissance des recherches pendantes ou effectuées la concernant.

Il faut noter qu'il est possible de déroger au droit d'accès indirect à certaines conditions. A titre exceptionnel, en vertu des dispositions de la LPD, le Préposé fédéral à la protection des données peut fournir de manière appropriée des renseignements aux personnes qui en font la demande, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et qu'il n'existe pas d'autre moyen pour empêcher que ces personnes soient lésées gravement et de manière irréparable.

Dans ce contexte, différents participants à la consultation se sont référés à une décision prise le 15 février 2006 par la Commission fédérale de la protection des données et de la transparence, alors compétente en la matière. Cette décision est en cours d'analyse, comme le reste de la jurisprudence (p. ex. relative à la CEDH). L'examen porte notamment sur la possibilité d'harmoniser les réglementations de la LMSI, de la LAAM et de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP). La LSIP est déjà en délibération au Parlement. Dans la mesure du nécessaire, le département abordera cette problématique lors des délibérations aux Chambres sur la présente révision et proposera des solutions.

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 procèdent, à la demande de la Confédération, à une observation dans des lieux qui ne sont pas librement accessibles ou y installent des dispositifs de surveillance, c'est le régime

des art. 18*a* à 18*i* du présent projet qui s'appliquera et non d'éventuelles dispositions du droit cantonal.

Les conséquences du nouvel arsenal juridique sur les cantons dépendent largement du type et de l'aménagement des nouvelles mesures, mais surtout de la nécessité de leur utilisation, laquelle découle des circonstances. Dans la mesure où ils sont concernés, les cantons devront donc éventuellement engager des ressources en personnel supplémentaires pour les organes cantonaux d'exécution de la LMSI (cf. art. 6 LMSI), pour lesquelles la Confédération leur accordera une indemnité équitable (art. 28 LMSI).

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 et sur quoi elles peuvent porter, et définir les principales modalités spécifiques des opérations autorisées.

Par ailleurs, il a déjà été mentionné que la finalité préventive de la recherche d'informations ne s'oppose pas à une transmission à des autorités de poursuite pénale suisses et étrangères (l'art. 17, al. 1, LMSI, précise même qu'il s'agit, à l'égard des autorités de poursuite pénale nationales, d'une obligation de transmettre les informations importantes pour la poursuite pénale). Des informations provenant des services de renseignements («Intelligence») peuvent être intégrées de différentes manières dans une procédure pénale, par exemple dans le cadre d'activités d'analyse ou par le biais de rapports officiels, et donc permettre entre autres l'utilisation ciblée des ressources de la poursuite pénale.

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. En revanche, 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 pour la sécurité 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 par des dispositions particulières dans la LMSI.

La LMSI ne doit toutefois mettre en place des règles spéciales que 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 de définir d'autres procédures et exigences techniques pour les surveillances menées à titre préventif.

Le libellé de l'art. 18*i*, al. 1, du présent projet indique clairement que les autres autorités impliquées dans la procédure, comme le Service des tâches spéciales (STS) du DETEC, ne sont ni tenues ni autorisées à fournir des renseignements sur l'exécution de mesures de surveillance fondées sur la LMSI.

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, tout comme la loi sur les télécommunications et la LSCPT, à mentionner les différents moyens techniques afin de ménager la marge de manœuvre nécessaire dans un domaine où l'évolution technique est particulièrement rapide. Sur le plan matériel, il faut que des indices concrets permettent de supposer que le perturbateur présumé utilise lesdits moyens pour échanger des informations 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 ces indices soient suffisamment concrets et actuels pour justifier une surveillance à un moment donné. Des informations générales collectées par le passé relatives à d'éventuelles menaces ne suffisent pas.

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 des contacts bien précis.

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, devait être autorisée expressément pour chaque raccordement, 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 par poste et télécommunication 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 de l'intérêt public, nous relèverons que, comme tous les autres moyens spéciaux de recherche d'informations, la surveillance de la correspondance ne peut intervenir que dans les trois domaines susceptibles de compromettre les fondements mêmes de notre société (cf. commentaire relatif à l'art 13*a*, al. 1). Cette mesure est donc évidente 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 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 quant à la menace et quant au fait que la personne soupçonnée utilise précisément des moyens déterminés de communication à distance dans ses menées.

Quant au caractère nécessaire, il est évident que, pour connaître suffisamment le réseau de contacts ou le contenu des communications à distance d'une personne dangereuse, il n'y a pas d'autre moyen à disposition que l'interception de ces communications. Le seul recours à un moyen ordinaire (art. 14, al. 2) ne permet guère 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. La description étroite des tâches prévues par la LMSI limite déjà beaucoup le domaine d'utilisation sur le plan légal. Une limitation plus stricte allant dans le sens d'un catalogue des délits tel que c'est le cas dans le droit de la procédure pénale serait inappropriée, car aucun lien ne doit exister avec les soupçons relevant de la justice pénale et que l'activité de prévention, par essence, ne peut viser des éléments constitutifs d'infractions précis. 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, de façon indépendante et selon des critères légaux, entre les besoins des professionnels de la sûreté, d'une part, et l'intérêt légitime du particulier à communiquer et entretenir des contacts sans ingérence étatique d'autre part.

Dans les limites décrites ci-dessus, nous pouvons donc admettre que la surveillance préventive de la correspondance par poste et télécommunication constitue, compte tenu des garde-fous que pose le projet de loi, une mesure proportionnée au but d'intérêt public qui la justifie. Son application est conforme aux exigences de la Constitution et des conventions internationales relatives aux droits de l'homme.

Art. 18l Surveillance de lieux qui ne sont pas librement accessibles, notamment 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. 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 à 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). Il est également interdit d'observer ou d'enregistrer un fait relevant du domaine secret ou privé d'une personne avec un appareil de prises de vue (cf. art. 179^{quater} CP), quand bien même ce fait se déroulerait dans un lieu librement accessible mais aurait été volontairement dissimulé au public. En revanche, la surveillance de comportements à caractère privé qui ont lieu dans un lieu public n'est pas soumise à des règles particulières.

Al. 1

Cet alinéa a pour but de décrire les modalités et les conditions de l'observation. Il faut que des indices concrets et actuels permettent de penser que la personne concernée 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.

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[50]. 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 observer et enregistrer 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. 13*a* et 18*k*.

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 tout l'environnement privé 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 considérée comme 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 vraisemblance suffisante, la mesure peut être tenue pour adéquate.

Quant à son caractère nécessaire, il est évident qu'aucun moyen ordinaire au sens de l'art. 14, al. 2. LMSI ne se prête à l'identification de faits se déroulant en des lieux privés, hormis le recours à un informateur bénéficiant d'un accès à ces lieux. Mais ce recours n'est pas toujours possible.

Enfin, quant à la proportionnalité au sens étroit, c'est-à-dire quant à savoir si l'intérêt public en jeu mérite de l'emporter sur l'atteinte que subit la personne concernée, elle ne peut, comme nous l'avons déjà dit, qu'être appréciée dans le cas d'espèce par les organes compétents. Il appartiendra au Tribunal administratif fédéral de procéder à cette pesée des intérêts 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 en soi, une moda-

50 RS **312.0**

lité 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 mêmes raisons 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 s'agira de déterminer si l'intérêt public en jeu est prépondérant.

Art. 18m Perquisition secrète d'un système informatique

Dans la société actuelle, les moyens informatiques modernes occupent une place toujours plus importante. 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 de plus en plus leurs messages sensibles 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).

L'art. 18*m* 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 protégées spécialement 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 un système déterminé 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. Pensons à ce titre à la recherche d'adresses dans l'ordinateur portable d'un perturbateur présumé ou au décodage d'un courriel chiffré, qui aurait pu être constaté, mais pas être mis en évidence, lors d'une surveillance autorisée de la correspondance.

Le traitement de la propagande de nature djihadiste s'impose comme un champ d'application concret. Même si ce type de propagande ne vise pas directement la Suisse, il recèle un potentiel de menace élevé et revêt donc un caractère important en termes de sûreté. On observe depuis peu une radicalisation par le biais des sites Internet de propagande djihadiste et des contacts virtuels. Le SAP peut certes consulter les sites Internet librement accessibles et participer à des forums de discussions non protégés, mais la législation actuelle ne lui confère pas le droit de perquisitionner des domaines sécurisés par des mots de passe ou par d'autres moyens. Or c'est justement là que les contacts décisifs ont lieu (p. ex. dans la rubrique privée des forums de discussion publics). Le SAP ne peut donc pas accéder aux domaines déterminants, ce qui doit changer dans l'intérêt de la sûreté de notre pays.

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 de ce moyen spécial par un intérêt public, nous renvoyons au commentaire des art. 13*a* et 18*l*. 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 traiter ou 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 aux données indispensables pour apprécier la menace. 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. Seuls des systèmes informatiques doivent pouvoir être perquisitionnés, et non pas, par exemple, des locaux ou des véhicules. Pour ces derniers, d'autres instruments de la recherche d'informations doivent être employés (comme l'observation physique ou des dispositifs techniques de surveillance). Comme on le voit, le choix réduit 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 guère appréciable de manière abstraite. Il appartiendra au Tribunal administratif fédéral de procéder à cette pesée des intérêts dans le cas concret et d'admettre ou de nier le caractère prépondérant de l'intérêt public qui sera en jeu.

Chapitre 3*b*
Interdiction d'activités et lutte contre la propagande incitant à la violence

Un nouveau type de mesure, à savoir l'interdiction de certaines activités, est introduit. 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, a constitué un premier pas dans ce sens. Plusieurs règles telles que l'interdiction de périmètre, l'interdiction de se rendre dans un pays donné, l'obligation de se présenter à la police et la garde à vue prescrivent des obligations de comportement pour le particulier et entendent ainsi empêcher que des actes de violence soient commis lors de manifestation sportives. La présente révision suit aussi cette direction: la prévention des menaces doit avoir un effet sur le comportement des particuliers.

Art. 18n Interdiction d'activités

Cette disposition octroie au chef du DFJP la compétence de prononcer des interdictions de droit administratif contre certaines activités, pour autant qu'elles représentent une menace concrète pour la sûreté intérieure ou extérieure de la Suisse.

De telles interdictions ne peuvent actuellement être prononcées que sur la base de la Constitution et à des conditions très strictes. La Constitution habilite en effet le Conseil fédéral à édicter des ordonnances et à prendre des décisions pour sauvegarder les intérêts du pays dans ses relations internationales (art. 184, al. 3, Cst.) ou pour parer à des troubles imminents menaçant gravement la sûreté intérieure de la Suisse (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 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 de la Suisse.

La nouvelle règle ne change 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. 18*e* in fine et 29*a*, al. 1).

En ce qui concerne les voies de droit, les interdictions et mesures prononcées par le Conseil fédéral en vertu de la Constitution et les interdictions prononcées par le 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[51]. En dehors de ces cas, les décisions du Conseil fédéral sont définitives. En revanche, les décisions fondées sur la LMSI constituent des actes parfaitement justiciables et pourront, de ce fait, être portées devant le Tribunal administratif fédéral puis le Tribunal fédéral.

La nouvelle réglementation proposée entraîne un net renforcement de la protection juridique des personnes concernées, indépendant du droit international public (les recours peuvent être portés, via le Tribunal administratif fédéral, au Tribunal fédéral). Ce point a été critiqué par quelques participants à la consultation qui estimaient que les voies de recours prévues conduisaient à un renversement de la situation concernant l'apport des preuves. Or ce n'est ni ce qui figure dans le projet de loi ni ce qui est souhaité. Au contraire: le corrélat de nouvelles compétences attribuées doit impérativement être une forte protection juridique.

S'agissant des demandes de création d'une base légale visant à confisquer les insignes des organisations radicales – qui ont été formulées au sujet du présent article lors de la procédure de consultation – nous nous référons aux travaux législatifs spécifiques relatifs à la loi fédérale instituant des mesures contre le racisme.

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

51 Voir l'ATF **125** II 417 ss; cette jurisprudence est également consacrée à l'art. 83, let. a, de la loi fédérale du 17 juin 2005 sur le Tribunal fédéral, RS **173.110**, et à l'art. 32, al. 1, let. a, de la loi du 17 juin 2005 sur le Tribunal administratif fédéral, RS **173.32**.

taisent par crainte pour elles-mêmes ou pour leurs proches, amis et connaissances dans leur pays d'origine. Il est certes possible de retracer le transfert des fonds à l'étranger, mais la trace de l'argent se perd ensuite 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 à grand recours de corruption; mais les raisons de la perte de la trace des fonds peuvent aussi être d'une toute autre nature. Il est exclu de se renseigner directement dans le pays-cible sur ce qu'il est advenu des fonds, car les personnes impliquées pourraient s'en trouver menacées. A cela s'ajoute le fait que les organisations mises à profit pour la collecte des fonds changent souvent de nom et d'apparence et ont elles-mêmes souvent recours à des tiers séjournant à l'étranger pour collecter les fonds.

Le chef du département doit décrire aussi précisément que possible l'étendue et le contenu de l'interdiction. La demande de certains participants à la consultation d'établir dans la loi une liste des activités interdites a été examinée et rejetée pour deux raisons: premièrement, car l'existence même d'une telle liste inviterait directement à la contourner et deuxièmement, car il ne serait pas possible d'interdire dans de brefs délais des menaces nouvelles ou ne figurant pas dans la liste. Si notre objectif est de couvrir une palette la plus large possible de comportements indésirables, il est alors difficile d'établir des critères plus précis.

Contrairement aux craintes exprimées par certains milieux consultés, l'interdiction d'activités n'est pas un instrument visant à lutter contre les mouvements d'opposition. Elle est plutôt dirigée contre toutes les personnes qui soutiennent des agissements terroristes ou relevant de l'extrémisme violent, et qui, de surcroît, menacent ainsi concrètement la sûreté intérieure ou extérieure de la Suisse. Cette interdiction de droit administratif ne vise donc pas en priorité à empêcher la commission d'infractions, mais plutôt à endiguer les menaces touchant la sûreté intérieure (qui ne sont pas, a priori, forcément punissables).

La décision d'interdiction doit faire référence à la menace de la peine telle que citée à l'art. 292 CP, dans la mesure où l'insoumission à une décision de l'autorité doit être sanctionnée. Il n'est pas nécessaire de mentionner cette norme pénale dans la loi, car cette mention n'aurait qu'un caractère déclaratoire.

Al. 2

Les interdictions prévues à l'al. 1 peuvent empêcher les personnes concernées de jouir de leurs droits fondamentaux, raison pour laquelle il est important de limiter ces interdictions dans le temps. Au terme de la durée de validité d'une interdiction, les autorités seront ainsi obligées d'examiner si les conditions requises pour l'interdiction sont toujours remplies ou si elles sont caduques.

Si les conditions sont toujours remplies, l'interdiction pourra être prolongée autant de fois qu'il est nécessaire. Corollaire de cette limitation dans le temps, le projet de loi prévoit aussi expressément l'obligation pour le département de s'assurer régulièrement que ces conditions sont encore remplies; si ce n'est plus le cas, le département doit lever immédiatement l'interdiction. Le département doit donc se montrer actif 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 Cst.), à la liberté d'opinion et d'information (art.16 Cst.), à la liberté de réunion (art. 22 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 être 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.

Art. 18o Saisie, séquestre et confiscation de matériel de propagande

Le nouvel art. 13*a* introduit par le ch. I de la LF du 24 mars 2006 (en vigueur depuis le 1er janvier 2007) doit être déplacé en raison de la nouvelle subdivision de la LMSI et devient l'art. 18*o*. Sa formulation et son contenu demeurent inchangés.

Art. 27, al. 1bis

En vertu de l'art. 27 LMSI, le Conseil fédéral est tenu de renseigner, annuellement ou selon les besoins, les Chambres fédérales, les cantons et le public sur son appréciation de la menace et sur les activités des organes de sûreté de la Confédération. De la même manière, le département doit fournir des renseignements, annuellement ou selon les besoins, sur l'utilisation des moyens introduits par la présente révision (p. ex. dans le cadre du rapport sur la sécurité intérieure de la Suisse). Au vu 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 porte sur le recours à des identités d'emprunt, sur les moyens spéciaux de recherche d'informations et sur l'interdiction d'activités. Notons par ailleurs que bien qu'aucune loi ne le prévoie expressément, des rapports complets sont aujourd'hui déjà soumis au département et à la Délégation des commissions de gestion.

Chapitre 6*a* Procédure et voies de droit

Art. 29a

Avec l'introduction des moyens spéciaux de recherche d'informations, la question des voies de droit doit être adaptée aux exigences de la Constitution et de la CEDH, et notamment à l'art. 29*a* Cst., qui garantit l'accès au juge, et à l'art. 13 CEDH, qui garantit le droit à un recours effectif.

Lors de la procédure de consultation, la limitation des voies de recours à la seule violation du droit fédéral, telle que prévue dans l'ancien al. 2 de la disposition, a été largement critiquée. Cette critique a été prise en considération et les recours portent désormais également sur la constatation inexacte ou incomplète des faits pertinents

(cf. commentaire de l'al. 3), ce qui garantit des voies de droit efficaces en corrélation avec les compétences élargies des services de renseignements.

Al. 1

Cette disposition inscrit le droit de recours contre les décisions prises par des organes fédéraux sur la base de la LMSI. Ainsi, l'art. 29*a*, al. 1, précise l'art. 32, al. 1, let. a, de la loi sur le Tribunal administratif fédéral, en tant qu'il dispose que les décisions fondées 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. 18*n*).

Al. 3

Le recourant peut invoquer la violation du droit fédéral, y compris l'excès ou l'abus du pouvoir d'appréciation ainsi que la constatation inexacte ou incomplète des faits pertinents.

Annexe: modification du droit en vigueur

1. Loi du 17 juin 2005 sur le Tribunal administratif fédéral[52]

L'introduction de l'art. 13*b* LMSI, qui consacre la compétence du Tribunal administratif fédéral de trancher les différends entre l'Office fédéral de la police, d'une part, et les autorités, les 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 l'art. 35, let. d, de la loi sur le Tribunal administratif fédéral (voir aussi le commentaire de l'art. 13*b*).

2. Code pénal suisse[53]

Art. 179^{octies}

La violation du domaine secret au moyen d'appareils de surveillance techniques tels qu'enregistreurs de sons ou d'images constitue une infraction 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 nouvelles mesures de surveillance autorisées en vertu de la LMSI.

Art. 317bis

Les faux dans les titres constituent des infractions (cf. art. 251, 252, 255 et 317 CP). L'actuel art. 317bis réserve toutefois le cas où de tels faux sont constitués et utilisés pour constituer ou assurer une identité d'emprunt dans le cadre d'une investigation

52 RS **173.32**
53 RS **311.0**

secrète autorisée par le juge. Il convient dès lors d'adapter cette disposition pénale afin de réserver aussi l'utilisation d'identités d'emprunt conformément à la LMSI.

3. Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire[54]

Art. 99, al. 1, 2e phrase, al. 1bis et 2

Al. 1, 2e 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 no 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 projet de loi emploie la notion générale d'exploration radio.

Al. 1bis

Conformément à l'al. 1, 2e phrase, l'exploration radio doit être 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, 2e phrase, a caractère de principe et sachant que toute limitation des droits fondamentaux tels que le 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. 1bis 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 des fréquences utilisées par l'armée en Suisse. Ainsi, l'armée doit, d'une part, pouvoir vérifier si des utilisateurs civils utilisent éventuellement les fréquences qu'elle utilise elle-même. D'autre part, elle doit pouvoir rechercher et surveiller, avec ses propres moyens, toutes les fréquences utilisées à des fins militaires. Si nécessaire, l'armée identifie et filtre les civils qui utilisent ses fréquences. Ce procédé est le seul permettant de garantir une utilisation militaire des fréquences et d'empêcher des abus.

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)[55], 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

54 RS **510.10**
55 RS **748.111.1**

recours à l'exploration radio pour surveiller l'espace aérien d'une manière générale et pour établir la situation aérienne, comme les y oblige l'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)[56].

Art. 99, al. 2

L'actuel al. 2 habilite le Service de renseignements stratégique (SRS) à traiter des données personnelles. Or cette disposition ne correspond pas totalement aux bases générales en matière de protection des données, surtout du point de vue du traitement de données sensibles et de profils de la personnalité. Afin donc de répondre aux normes en matière de protection des données, les principes prévus aux al. 1 et 2 de l'actuel art. 15 de la LMSI doivent, en majeure partie, être introduits dans le présent alinéa.

La deuxième et la troisième phrase de l'al. 2 ont été reprises, sur le fond, de l'art. 15, al. 1, LMSI. Elles portent sur le traitement de toutes les données personnelles et inscrivent les principes généraux relatifs à l'évaluation de l'exactitude des données et à la destruction des informations inexactes ou inutiles (voir les art. 4 et 5 LPD).

De plus, l'actuelle règle a été reprise de l'art. 9, al. 1, let. a, b et c, de l'ordonnance du 3 septembre 2003 sur les services de renseignements au DDPS (Orens)[57]; les conditions relatives au traitement de données sensibles et de profils de la personnalité figurent ainsi directement dans la LAAM. Le Conseil fédéral règle les détails au niveau de l'ordonnance.

Grâce à la proposition d'adaptation de l'art. 99, al. 2, LAAM, le SRS et le SAP traiteront les données personnelles selon les mêmes principes.

Art. 99a

Conformément à l'art. 164, al. 1, Cst., toutes les dispositions importantes qui fixent des règles de droit doivent figurer dans une loi formelle. Les dispositions de l'ordonnance du 15 octobre 2003 sur la conduite de la guerre électronique (OCGE)[58] consacrées à l'exploration radio contiennent certes des normes fixant des règles de droit, mais elles ne disposent pas d'une base formelle expresse dans la LAAM. 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'OCGE.

L'ACI ne contrôle en principe que les mandats d'exploration radio qui ne nécessitent pas d'autorisation (spécifique) particulière au niveau politique, comme cela est le cas pour les mandats d'exploration radio permanente (p. ex. du Service de rensei-

56 RS **321.0**
57 RS **510.291**
58 RS **510.292**

gnement 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.

4. Loi du 30 avril 1997 sur les télécommunications[59]

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 poste et 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 du 20 mars 1981 sur l'entraide pénale internationale[60]. 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.

5 à 11: Assurances sociales

Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[61]

Loi fédérale du 19 juin 1959 sur l'assurance-invalidité (LAI)[62]

Loi fédérale du 25 juin 1982 sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP)[63]

Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal)[64]

Loi fédérale du 20 mars 1981 sur l'assurance-accidents (LAA)[65]

59 RS **784.10**
60 RS **351.1**
61 RS **831.10**
62 RS **831.20**
63 RS **831.40**
64 RS **832.10**
65 RS **832.20**

Loi fédérale du 19 juin 1992 sur l'assurance militaire (LAM)[66]

Loi du 25 juin 1982 sur l'assurance-chômage (LACI)[67]

Dans le domaine des assurances sociales, le législateur a réglé la communication des données dans les différentes lois régissant ce domaine, créant ainsi un régime exhaustif en la matière. Dès lors, la levée du secret de fonction à l'égard des organes de sûreté de la Confédération et des cantons au sens de l'art. 13*a* du présent projet nécessite une adaptation spéciale des lois concernées. Il ne s'agit pas là d'une levée totale du secret de fonction, mais d'une levée partielle limitée au cas où les conditions prévues à l'art. 13*a* sont remplies. Les secrets professionnels prévus par la loi (p. ex. pour les médecins, les avocats, les ecclésiastiques, etc.) ne tombent pas sous le coup de cette adaptation et demeurent inchangés. Notons par ailleurs que la levée du secret de fonction ici proposée est analogue à d'autres règles déjà existantes pour les autorités d'instruction pénale, les autorités compétentes en matière d'aide sociale, les offices de recouvrement, les autorités fiscales, etc.

Il convient enfin de souligner que le devoir de renseigner se limite quant à lui aux domaines du terrorisme, du service de renseignements politiques ou militaires prohibé et de la prolifération. Ainsi, la levée du secret de fonction porte uniquement sur ces menaces précises.

La révision en cours du code civil (Protection de l'adulte, droit des personnes et droit de la filiation; FF *2006* 6635) introduit, dans le domaine des assurances sociales, certaines dispositions identiques à celles de la présente révision de la LMSI. Le département proposera – en temps voulu et en fonction de l'avancement de ces deux projets de révision menés en parallèle – des solutions d'harmonisation.

3 Conséquences

3.1 Conséquences pour la Confédération

3.1.1 Conséquences financières

Les conséquences financières dépendront fortement du type et de l'aménagement des différentes mesures, mais aussi et surtout de la nécessité de leur mise en œuvre (au gré des événements). L'expérience fait défaut en la matière, en particulier en ce qui concerne la pratique de l'approbation par le pouvoir judiciaire et par le pouvoir exécutif (qui est décisive dans bien des domaines). Le manque d'expérience également empêche toute indication concrète quant à d'éventuelles économies (liées p. ex. au remplacement des observations par la surveillance de la correspondance par télécommunication). Selon les estimations, le domaine technique (appareils, équipement) exigerait des investissements uniques de l'ordre d'un million de francs et engendrerait des frais annuels de l'ordre de 100 000 francs, ainsi que des frais annuels de personnel de l'ordre de 6,5 millions de francs (cotisations de l'employeur comprises). Ces montants seront financés par compensation interne au sein du département.

66 RS **833.1**
67 RS **837.0**

3.1.2 Conséquences pour le 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 (autorités de police cantonales). Au total, il faut compter près de 40 postes supplémentaires. Ces postes seront compensés en interne au sein du département.

Les postes supplémentaires sont donc nécessaires dans les domaines suivants:

- 35 postes au sein du SAP pour la recherche et l'évaluation des informations (policiers, interprètes, techniciens, analystes) et pour l'adaptation du traitement des données (saisie des données, garantie de la qualité, correspondance avec l'étranger);
- 5 autres postes pour l'adaptation des services administratifs nécessaires à l'exécution mais n'appartenant pas aux structures du renseignement (p. ex. pour la technique et l'administration au sein du STS DETEC, le Tribunal administratif fédéral et la Direction de fedpol).

Ainsi, les compétences supplémentaires seraient mises en œuvre avec des ressources relativement modestes.

Certains participants à la procédure de consultation se sont demandé si l'ampleur actuelle de la collaboration entre les services impliqués suffisait et ont exigé que les tâches, les processus et les structures soient soumis à réexamen.

A cet égard, il convient de se reporter à l'avis exprimé le 2 décembre 2005 par le Conseil fédéral quant à la motion Schlüer (05.3637: Fusion des services de renseignement du DDPS et du DFJP): «(…) L'Office fédéral de la police (fedpol) a été réorganisé à compter de 2001 pour répondre aux exigences de la CEP DFJP, en ce sens que les fonctions du service de renseignement intérieur et la police judiciaire, selon les principes de l'organisation, ont été séparés en fonction du déroulement des procédures, et répartis sur le plan interne dans plusieurs divisions principales. Ces divisions sont sous la direction du directeur du fedpol, lequel est directement subordonné au chef du DFJP (…)».

Le Conseil fédéral considère cette répartition des tâches et cette organisation au sein du DFJP comme efficace et appropriée.

Par ailleurs, le ch. 3 du rapport «Lutter plus efficacement contre le terrorisme et le crime organisé»[68] s'exprime dans le détail sur la collaboration entre les organes de poursuite pénale et le service de renseignements intérieur. Au vu des circonstances, le Conseil fédéral ne voit aucune nécessité urgente de prendre des mesures législatives ou politiques dans le domaine structurel. Il n'y a nulle raison de revenir sur ces questions, dans la mesure où le Conseil fédéral, lorsqu'il a pris ses décisions relatives à la politique des services de renseignements et à leur collaboration le 24 janvier 2007, n'a pas jugé nécessaire de prendre d'autres mesures en la matière.

3.1.3 Autres conséquences

Il ne devrait pas y avoir d'autres conséquences spécifiques.

68 Cf. «rapport donnant suite au postulat CPS».

3.2 Conséquences pour les cantons et les communes

Le niveau de sécurité dans les cantons et les communes s'améliorera. L'accroissement des obligations de renseigner et de communiquer des unités administratives cantonales et communales prévu aux art. 13 et 13*a* du présent projet sera compensé par certaines diminutions de travail à moyen et long terme (recherches facilitées, les moyens spéciaux de recherche d'informations remplaceront en partie les observations menées par les forces de police cantonales, qui nécessitent 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.

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

La mise en œuvre du projet augmentera la sécurité de la Suisse et permettra notamment de mettre en œuvre des interventions politiques.

3.3.2 Impact du projet sur les différents groupes de la société

Les normes proposées contribueront à renforcer la sûreté intérieure et extérieure 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 et socialement plus stable aura pour effet indirect d'améliorer les conditions économiques générales, ce qui renforcera la place économique suisse.

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 com-

merce 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 Adéquation 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 la politique étrangère

Ce projet, qui vise avant tout à lutter efficacement contre le terrorisme international, pourrait avoir un impact positif durable sur la réputation de la Suisse à l'étranger. Il permettra de détecter plus tôt les activités en Suisse de groupes extrémistes étrangers violents et de mieux les contrôler, comme l'exige depuis longtemps la Délégation du Conseil fédéral pour la sécurité.

3.4.2 Conséquences sur les relations internationales

La révision de loi proposée ne met pas formellement en œuvre un engagement international de la Suisse. Par contre, l'harmonisation des standards aura vraisemblablement pour effet de renforcer considérablement la coopération internationale.

4 Programme de la législature

Le présent projet n'est pas inscrit au programme de la législature 2003 à 2007 (FF *2004* 1035).

Il est néanmoins contenu dans l'objectif n° 19 du Conseil fédéral pour l'année 2007: «Amélioration de la coopération internationale, de la prévention et des structures internes de la justice et de la police».

L'urgence et la nécessité du projet résident dans les dégradations successives de la situation sécuritaire et de la situation de la menace en Suisse au cours des dernières années, en raison notamment des attentats terroristes commis par des individus islamistes. L'Europe occidentale n'est plus seulement une base arrière et la Suisse fait également partie de la zone menacée. La loi actuelle consent à des risques qui ne sont plus conciliables avec la nouvelle situation de la menace. La solidarité internationale (notamment avec les Nations Unies et les Etats européens) est également compromise.

5 Aspects juridiques

5.1 Constitutionnalité

La LMSI se fonde sur la compétence inhérente de la Confédération en matière de maintien de la sûreté intérieure et extérieure de la Suisse et sur les tâches de la Confédération visant à préserver la sûreté intérieure (art. 173 Cst.). 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 actuel 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 que les mesures de recherche spéciale d'informations prévues ne visent ni le renseignement économique prohibé ni le crime organisé.

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 Cst.); peuvent aussi être touchées la liberté de conscience et de croyance (art. 15 Cst., notamment al. 3), la liberté de réunion (art. 22 Cst.), la garantie de la propriété (art. 26 Cst.).

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 doivent être ancrés dans 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 contestée. Quant au caractère proportionné des nouvelles mesures, nous renvoyons aux commentaires relatifs aux différents articles. Il faut aussi rappeler ici que les différentes cautèles qui accompagnent les nouvelles mesures sont autant d'éléments qui mettent en œuvre le principe de la proportionnalité de l'ingérence étatique et qu'il convient d'observer au cas par cas comment elles sont appliquées (comme l'a souligné le Tribunal fédéral dans l'avis qu'il a fourni lors de la procédure de consultation). En outre, il ressort clairement des conditions de l'art. 18*b*, notamment let. c, que les moyens 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 de recherche d'informations ne suffisent pas à élucider un soupçon concret relatif à une menace contre la sûreté intérieure ou extérieure de la Suisse.

Les moyens et mesures prévus dans le projet sont conformes à la Constitution. Les principes de l'Etat de droit sont pleinement préservés.

5.2 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)[69].

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. 18*b* et des conditions particulières fixées aux art. 18*k* à 18*n*, avec suffisamment de précision la catégorie de personnes visées, les circonstances dans lesquelles les mesures peuvent être prises (cf. art. 18*a* et 18*b*), ainsi que les garanties de procédure (art. 18*d*, 18*e*, 18*f* et 18*i*). 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.

5.3 Forme de l'acte à adopter

5.3.1 Loi

Les dispositions importantes qui fixent des règles de droit relatives à la restriction des droits constitutionnels doivent être édictées sous la forme d'une loi fédérale (art. 36, al. 1, art. 163, al. 1, et art. 164, al. 1, Cst.). Ces conditions sont remplies en l'espèce.

5.3.2 Révision partielle

Bien qu'une révision totale soit souhaitable pour des raisons de lisibilité, préférence a été donnée à une révision partielle pour les raisons suivantes:

69 RS **0.103.2**

– 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 de la présente révision prennent certes 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.

5.4 Frein aux dépenses

En vertu de l'art. 159, al. 3, let. b, Cst., le paquet législatif doit être adopté à la majorité des membres de chaque conseil s'il entraîne de nouvelles dépenses périodiques de plus de 2 millions de francs. C'est effectivement le cas, mais les besoins en effectifs et les besoins financiers seront couverts grâce à des compensations internes au sein du département.

5.5 Conformité à la loi sur les subventions

Les cantons ont exigé unanimement dans le cadre de la procédure de consultation que la Confédération indemnise d'éventuelles prestations supplémentaires dans le domaine de la protection de l'Etat.

Les prestations financières allouées aux cantons sont réglées comme suit à l'art. 28, al. 1, LMSI: «La Confédération rembourse aux cantons les prestations qu'ils fournissent sur son mandat, conformément à la section 3. Le Conseil fédéral détermine l'indemnité forfaitaire sur la base du nombre de personnes essentiellement affectées à des tâches fédérales.»

Dans le commentaire de cette disposition légale, il était expliqué que, dans le cadre du traitement des informations, le défaut de prise en charge des coûts pourrait avoir des conséquences fatales, raison pour laquelle était prévue une dérogation au principe selon lequel les cantons devaient prendre en charge seuls les frais d'exécution du droit fédéral. Ce commentaire demeure valable.

5.6 Délégation de compétences législatives

A l'art. 10*a* du présent projet, il est prévu que le Conseil fédéral règle dans le détail les droits d'accès et les principes régissant la conservation et l'effacement des données du système d'information électronique dans lequel sont traitées des données concernant des événements et des mesures policières. Il définit par voie d'ordonnance les organisations qui sont soumises à l'obligation de renseigner en vertu de l'art. 13*a* du projet et règle le détail des activités, de l'organisation et de la procédure liées à l'exploration radio en vertu de l'art. 14*a*. Il règle par ailleurs, en vertu du nouvel art. 99*a* LAAM, la composition de l'autorité de contrôle indépendante, l'indemnisation de ses membres et l'organisation de son secrétariat.

Analyse de droit comparé (Allemagne, Autriche, France, Italie, Luxembourg, Pays-Bas, UE)

1. Allemagne

La République fédérale d'Allemagne est un Etat à la structure fédéraliste. Sa constitution confère aux *Länder* la souveraineté en matière de police sur leur territoire.

Les autorités de défense de la constitution de l'Etat fédéral et des *Länder* ont pour tâche principale de recueillir et d'exploiter des informations sur des velléités de s'opposer à l'ordre constitutionnel démocratique libéral, telles que des activités ou des tentatives représentant une menace pour la sécurité ou relevant des services secrets, dans le domaine d'application de la loi sur la défense de la constitution fédérale[70].

L'Etat fédéral et les *Länder* sont tenus de coopérer dans le domaine de la défense de la constitution. L'Etat fédéral possède un Office fédéral de la défense de la constitution (*Bundesamt für Verfassungsschutz, BfV*) dépendant du ministère de l'intérieur. Le BfV peut traiter et utiliser les informations nécessaires à l'accomplissement de ses tâches, y compris des données personnelles, à moins que les dispositions applicables de la loi fédérale sur la protection des données ou les règles spéciales de la loi sur la défense de la constitution ne l'interdisent. En outre, il peut demander des données et des informations aux autorités chargées de la répression[71]. A l'inverse, le service de renseignement fédéral peut transmettre des informations aux autorités nationales lorsque l'accomplissement de ses tâches l'exige ou que les données sont nécessaires à des fins de sécurité publique[72]. Ces données peuvent être utilisées dans le cadre de poursuites pénales.

Les activités du BfV sont soumises à la surveillance d'un organe de contrôle parlementaire auquel il fait régulièrement rapport sur ses activités en général et sur les actions d'une importance particulière[73]. Cet organe peut exiger que le gouvernement fédéral le laisse consulter les dossiers et les données et entendre des collaborateurs. Le BfV est tenu de renseigner gratuitement les personnes qui le demandent sur les données conservées à leur sujet, si elles se réfèrent à des faits concrets et attestent d'un intérêt particulier à être renseignées[74]. Il doit rectifier les données conservées en cas d'inexactitude, et examiner au plus tard après cinq ans si les données relatives à une personne doivent être rectifiées ou effacées. Les données doivent de toute

70 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungssschutzgesetz; BVerSchG)

71 § 18 BVerfSchG

72 § 9 de la loi du 20 décembre 1990 sur le service de renseignement fédéral (*Gesetz über den Bundesnachrichtendienst, BNDG*).

73 § 2 de la loi sur le contrôle parlementaire de l'activité de renseignement de l'Etat fédéral (*Gesetz über die parlamentarische Kontrollenachrichtendienstlicher Tätigkeit des Bundes*)

74 § 15 BVerfSchG

façon être effacées au plus tard quinze ans après le dernier enregistrement, sauf décision contraire du responsable de service[75].

Pour ce qui est des attributions du BfV, celui-ci peut notamment relever des données provenant du trafic des télécommunications dans des cas d'espèce pour remplir ses tâches[76]. Son président ou son vice-président doit en faire la demande écrite, assortie de motifs. Le ministère désigné par le chancelier approuve ou rejette la demande. Il informe chaque mois des demandes déposées un organe parlementaire spécifique appelé *«G 10-Kommission»*. Les décisions ne sont exécutées qu'une fois celui-ci informé, sauf s'il y a urgence[77]. Le ministère informe au moins tous les six mois le *Parlamentarisches Kontrollgremium* – commission de contrôle parlementaire – des collectes de données effectuées. Par ailleurs, le BfV est habilité à avoir recours à des agents et à des personnes de confiance, à pratiquer l'observation, les enregistrements audio et vidéo, à utiliser des identités d'emprunt ou des signes conventionnels de camouflage[78]. Ces mesures sont ordonnées par des instructions de service approuvées par le ministère de l'intérieur. Ce denier informe la commission de contrôle parlementaire. S'il est question de recueillir des renseignements sur une personne, le but de cette mesure doit être indiqué.

Le BfV est en outre autorisé, à certaines conditions, à recueillir des renseignements auprès des banques[79]. Il peut exiger des fournisseurs de services de poste ou de télécommunication des informations telles que des noms, des adresses ou des indications sur les cases postales, ou bien des indicatifs, des numéros de téléphones et des indications sur le lieu des appels[80]. Enfin, il peut installer des appareils destinés à détecter les numéros d'appareil et de carte des téléphones portables[81]. Les conditions sont les mêmes que pour les écoutes téléphoniques.

Par contre, les autorités allemandes de défense de la constitution ne disposent pas de pouvoirs de police. Notamment, elles ne peuvent pas procéder à des perquisitions ni confisquer des objets.

Suite aux attentats du 11 septembre 2001, la loi (de durée limitée) sur la lutte contre le terrorisme[82] a été révisée le 12 juillet 2006 et mise en œuvre par une loi complémentaire[83]. Les services de renseignement peuvent désormais consulter des données du registre central des véhicules selon une procédure d'appel automatisée. Ils peuvent diffuser le signalement d'un suspect à l'échelle européenne à des fins de surveillance discrète, lorsqu'il s'agit d'écarter un danger grave. Ils sont informés lorsque la personne recherchée est prise dans un contrôle de police. Les demandes de renseignements peuvent aussi s'étendre à des agissements contraires à la constitution. Les règles sensibles relatives au renseignement sont limitées à cinq ans et devront être évaluées dans ce délai.

75 § 12 BVerfSchG
76 § 8, al. 8, BVerfSchG
77 § 8, al. 9, BVerfSchG
78 § 8, al. 2, BVerfSchG
79 § 8, al. 5, BVerfSchG
80 § 8, al. 6, et § 8, al. 8, BVerfSchG
81 § 9, al. 4, BVerfSchG
82 *Terrorismusbekämpfungsgesetz (TBGE)* du 9 janvier 2002 (BGBl I 2002, p. 361, 3142)
83 *Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (TBEG)*, du 5 janvier 2007 (BGBl I 2007, 2)

2. Autriche

L'Etat autrichien est organisé de manière fédéraliste. Son régime juridique établit une différence fondamentale entre le domaine répressif et le domaine préventif. L'Office fédéral de défense de la constitution et de lutte contre le terrorisme (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, BVT*) assume les tâches de renseignement civil[84]. Le BVT assure essentiellement la protection de l'Etat et de ses institutions constitutionnelles. Ses tâches principales sont la lutte contre le terrorisme international, contre les phénomènes extrémistes, contre l'espionnage, contre le trafic d'armes international, contre le trafic de matériaux nucléaires et contre le crime organisé dans ces domaines. Il fait partie de la Direction générale de la sécurité publique au ministère fédéral de l'intérieur.

Chaque *Land* dispose d'un office de défense de la constitution et de lutte contre le terrorisme, qui relève de la Direction de la sécurité. Il incombe au BVT de mettre en place et de coordonner les mesures de protection des personnes et des objets et de les mettre en œuvre via les offices des Länder. Il en va de même pour la protection des représentants d'Etats étrangers ou d'organisations internationales et autres sujets du droit international.

Les autorités de protection de l'Etat ont accès aux données des autorités répressives. Les personnes concernées ont le droit d'être renseignées sur les données collectées à leur sujet, de demander leur rectification ou leur effacement, et de faire recours auprès de la commission de la protection des données. Le droit d'être renseigné peut être refusé si la protection de l'Etat l'exige.

Les autorités chargées de la sécurité qui pratiquent la *erweiterte Gefahrenforschung* ou recherche extensive sur les menaces – une observation des groupements de personnes qui sera exposée plus loin – doivent signaler immédiatement au ministre de l'intérieur les mesures qu'elles prennent. Les enquêtes ne peuvent avoir lieu qu'après avis du délégué à la protection des droits ou au terme d'un délai de trois jours, à moins qu'un grave danger ne commande l'urgence[85].

Si le délégué à la protection des droits constate que les droits des personnes concernées ont été lésés par l'utilisation de données personnelles sans que ces personnes aient eu connaissance de l'utilisation de ces données, il est autorisé à les en informer ou, si cela n'est pas possible, à présenter un recours à la commission de la protection des données.

Le délégué à la protection des droits doit faire au ministre de l'intérieur un rapport annuel sur les activités liées à la recherche extensive sur les menaces[86]. Le ministre de l'intérieur doit présenter ce rapport à la sous-commission permanente du Conseil national, si elle en fait la demande.

Les autorités de protection de l'Etat sont habilitées, à certaines conditions, à exiger des renseignements des fournisseurs de services publics de télécommunication. La surveillance de la poste et des télécommunications n'est cependant permise qu'aux autorités répressives. Les investigations secrètes sont également autorisés, ainsi que

84 Loi fédérale du 31 octobre 1992 sur l'organisation de la sûreté et sur la police de sûreté (*Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei; SPG*)
85 § 62a, al. 7, SPG (modification de 2005)
86 § 21, al. 3, SPG

les enregistrements sonores effectués lors de ces investigations[87]. Il est cependant interdit de faire un enregistrement sonore hors de la présence de l'agent infiltré. Le délégué à la protection des droits assure un contrôle permanent sur les investigations secrètes et sur l'utilisation, dans ce cadre, d'appareils d'enregistrement audio et vidéo[88]. Ces investigations doivent lui être signalées, ainsi que leurs raisons essentielles, si l'identité de la personne concernée est connue. Les autorités de protection de l'Etat peuvent en outre saisir, confisquer et séquestrer des objets[89], pratiquer l'observation[90], pénétrer dans des locaux privés[91] et ordonner ou mener des interrogatoires[92]. Les intermédiaires financiers sont tenus, dans des cas déterminés, de donner des renseignements aux autorités compétentes[93].

L'activité du BTV est soumise au contrôle parlementaire en vertu de l'art. 52*a* de la constitution fédérale autrichienne. Lorsque les voies de recours administratives sont épuisées, un recours peut être déposé auprès de la cour administrative ou constitutionnelle.

Le 11 septembre n'a pas été sans impact en Autriche. Les structures et les dispositions légales ont été renforcées. Les autorités de protection de l'Etat ont reçu de nouvelles compétences.

Une modification de 2002 de la loi sur la police de sûreté a étendu aux membres des groupes suspects la protection des personnes pouvant donner des renseignements sur une attaque dangereuse ou sur une association criminelle. Les bases juridiques du camouflage des mesures d'appui lors d'opérations d'observation ou d'investigations secrètes ont également été modifiées. Face au développement de menées extrémistes, des dispositions sur la recherche étendue sur les menaces ont été intégrées dans la SPG le 1er octobre 2000, accompagnées de règles de protection des droits[94]. Ces dispositions permettent aux autorités du domaine de la sécurité d'observer des groupements de personnes lorsqu'elles soupçonnent que ces groupements pourraient en venir à se livrer à des activités criminelles liées à une menace grave pour la sécurité publique. Les autorités chargées de la sécurité ne pouvaient auparavant observer des groupes extrémistes que s'ils se livraient déjà à des actes criminels.

La loi sur la police de sûreté a été de nouveau modifiée en décembre 2003, instaurant une attestation de conformité en matière de sécurité pour les entreprises et les installations[95].

Le 1er décembre 2002, un Office fédéral de protection de la constitution et de lutte contre le terrorisme a été créé au sein du ministère fédéral de l'intérieur. Il est directement subordonné au directeur général de la sécurité publique[96]. Ses activités sont régies par la loi sur la police de sûreté et, lorsqu'il agit au service des autorités judiciaires pénales, par le code de procédure pénale.

87 § 54 SPG
88 § 62a, al. 7, SPG
89 § 42 SPG
90 § 54, al. 2, SPG
91 § 39 SPG
92 § 28a SPG
93 § 38 de la loi sur les banques (*Bankwesengesetz; BWG*)
94 §§ 21, al. 3, 53, al. 1, ch. 2a, 54, al. 2, et 62*a* SPG
95 § 55 à 55b SPG
96 § 7, al. 1 et 9 de la loi sur les ministères fédéraux (*Bundesministeriengesetz*)

3. France

La France est une démocratie unitaire fortement centralisée dans laquelle les 26 régions disposent d'une autonomie quasi-nulle.

Le premier ministre, soutenu par le Secrétariat général de la défense nationale (SGDN) et par un cabinet militaire, est directement responsable de la sécurité intérieure. Celle-ci incombe à plusieurs services de l'Etat, sans qu'il y ait de séparation entre le domaine de la prévention et celui de la répression.

La France possède deux services de sécurité indépendants: la police et la gendarmerie nationale. La gendarmerie est en charge des régions rurales, la police des zones urbaines. La gendarmerie mobile est responsable du maintien de l'ordre public et de la lutte contre le terrorisme, la criminalité organisée et les sectes. La police nationale est subordonnée au ministère de l'intérieur. Placée sous l'autorité du directeur général de la police nationale (DGPN), elle compte de nombreuses directions, dont la Direction de la surveillance du territoire (DST), la Direction centrale des renseignements généraux (DCRG) et l'Unité de coordination de la lutte antiterroriste.

La DST assume le rôle d'un service de renseignement. Elle a pour mission de lutter contre les activités de nature à menacer la sécurité du pays[97]. Son organisation et son fonctionnement font l'objet d'un arrêté du ministre de l'intérieur du 8 mars 1993, classifié secret-défense. La DST, en tant que service central, recueille et traite toutes les informations que lui transmettent les Renseignements généraux; elle gère leur transmission à d'autres services. Elle participe à la protection de domaines et secrets sensibles de la défense nationale. Elle a accès au fichier informatisé géré par les Renseignements généraux[98].

L'Unité de coordination de la lutte anti-terroriste coordonne les travaux de tous les services mobilisés en France et à l'étranger.

Le SGDN est un organe purement administratif, chargé de la coordination interministérielle. Son domaine couvre notamment la sécurité des systèmes d'information, la prévention du terrorisme, la protection des structures de direction et de communication de l'Etat et la lutte contre la prolifération nucléaire. Il surveille également les exportations de matériel de guerre.

La Direction générale de la sécurité extérieure (DGSE) est un service secret chargé de la sécurité extérieure. Rattachée au premier ministre, elle pratique le renseignement et possède un volet opérationnel.

Les personnes intéressées peuvent exercer leur droit d'accès aux fichiers informatiques des Renseignements généraux de manière indirecte[99]. La demande de consultation doit être adressée à la Commission nationale de l'information et des libertés (CNIL), qui contrôle les informations et informe le demandeur d'éventuelles rectifications. Si la sécurité intérieure n'est pas menacée, celui-ci peut avoir accès aux données. Le responsable du fichier peut l'informer directement si la communication des informations ne compromet pas les buts du fichier informatique.

97 Décret nº 82-1100 du 22 décembre 1982
98 Décrets nº 91-1052 et 91-1051
99 Loi nº 2003-239 du 18 mars 2003 pour la sécurité intérieure

Le gouvernement peut autoriser des écoutes téléphoniques préventives afin de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel économique de la France, ou la prévention du terrorisme, de la criminalité organisée et de la constitution de groupements illégaux[100]. Les écoutes sont autorisées par une décision du premier ministre ou par l'une des deux personnes spécialement déléguées par lui, sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur, du ministre chargé des douanes ou de leurs délégués[101]. Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément est arrêté par le premier ministre, sous la surveillance d'un organe indépendant, la Commission nationale de contrôle des interceptions de sécurité[102]. A la tête de celle-ci se trouve un président nommé pour six ans par le président de la République. Les autorisations d'écoutes sont données pour une durée de quatre mois au maximum, renouvelable pour la même durée. Les enregistrements effectués sont détruits dans les dix jours, sous l'autorité du premier ministre.

Selon la commission, toutes les informations liées aux écoutes préventives sont classifiées secret défense. Cela signifie en particulier que les personnes ayant fait l'objet de ces écoutes ne peuvent en être informées, car il y va de la sauvegarde des intérêts de la défense nationale. La surveillance de la correspondance postale est par contre interdite aux autorités de protection de l'Etat.

Les autorités peuvent également, dans des cas exceptionnels réquisitionner ou geler des biens par arrêté motivé, si la sécurité intérieure l'exige[103]. Elles peuvent mener des auditions. Elles peuvent également procéder à des fouilles corporelles ou à des perquisitions de domicile sans contrôle judiciaire[104]. En cas de crime organisé, les perquisitions sont également autorisées la nuit.

En ce qui concerne les enregistrements sonores et visuels, les papiers et les insignes d'emprunt, de nombreuses compétences ont été fondées sur la loi pour la sécurité intérieure, notamment celle d'accéder directement à des fichiers informatiques ou de recueillir des renseignements auprès de banques ou de particuliers. Dans certaines circonstances, il est possible d'interdire notamment des manifestations armées ou des groupes qui menacent la sécurité nationale[105]. Dans le cadre de la lutte contre la criminalité organisée, l'emploi de personnes de confiance est autorisé. Le procureur de la République doit en être avisé a posteriori. Les informateurs sont indemnisés sur des fonds spéciaux[106].

Une loi du 19 janvier 2006 a étendu les possibilités d'installer notamment une surveillance vidéo dans les bâtiments publics ou les installations sensibles, en cas de menace terroriste potentielle. L'accès aux données électroniques des fournisseurs de services de télécommunication et des compagnies aériennes a été donné à la police

100 Art. 3 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications
101 Art. 4 de la loi relative au secret des correspondances émises par la voie des télécommunications
102 Art. 5 de la loi relative au secret des correspondances émises par la voie des télécommunications
103 Art. 3 de la loi pour la sécurité intérieure et loi n° 2005-750 du 4 juillet 2005
104 Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (ci-après loi du 9 mars 2004)
105 Loi du 10 janvier 1936 sur les groupes de combat et milices privées
106 Loi portant adaptation de la justice aux évolutions de la criminalité

et à la gendarmerie nationale. Un prolongement de la garde à vue a été autorisé et la possibilité de procéder à des contrôles dans les trains internationaux instaurée[107].

Aucun système de contrôle parlementaire n'est actuellement prévu, mais des lois à ce sujet sont en préparation. Le gouvernement est cependant tenu de faire rapport au parlement.

4. Italie

Contrairement à la Suisse, l'Allemagne ou l'Autriche, l'Italie est un Etat unitaire décentralisé.

La sauvegarde de la sécurité intérieure et extérieure est bâtie 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 Direzione Investigativa Antimafia (DIA).

Elle relève du ministère de l'intérieur, auquel est subordonnée la Direzione centrale per la Polizia di Prevenzione[108].

La Polizia di Prevenzione a pour objectif de lutter contre les organisations terroristes à l'intérieur et à l'extérieur du pays et contre les groupements paramilitaires et violents. Selon l'art. 6 de la loi 121, elle peut classifier, analyser et évaluer des données pour assurer la sécurité.

Alors que le SISMI est responsable des activités à l'étranger, le SISDE est chargé de la sécurité intérieure. Il a notamment pour tâches de lutter contre le terrorisme, l'immigration illégale, la criminalité informatique, l'espionnage économique, les nouvelles menaces et la criminalité organisée.

Dans le cadre de ces tâches, le SISDE recueille des données. En principe, les personnes concernées ont le droit de les consulter[109]. Tous les documents et dossiers dont la publication menacerait la sécurité de l'Etat sont cependant couverts par le secret d'Etat[110]. Le délégué à la protection des données (garante per la protezione dei dati personali) contrôle les données recueillies. Les autorités de protection de l'Etat collaborent avec les autorités de la police judiciaire dans le cadre de la sécurité informatique.

Les activités du SISMI et du SISDE sont surveillées par une commission parlementaire. Le gouvernement doit soumettre au parlement des rapports semestriels sur les activités de ces deux services. Les activités des services de renseignements sont aussi soumises à un contrôle judiciaire.

La DIA met en œuvre des mesures contre la criminalité organisée telles que des surveillances, y compris téléphoniques, et elle mène des enquêtes contre la Mafia[111]. Elle peut recueillir des informations concernant la situation financière de personnes soupçonnées d'appartenir à des organisations criminelles. Elle transmet ces informations au SISDE et au SISMI. Elle collabore avec les forces de police.

107 Loi n° 2005-532 du 19 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers
108 Loi n° 121 de 1981 *«Nuovo ordinamento dell'Amministrazione della pubblica sicurezza»*
109 Décret-loi n° 196 du 30 juin 2003
110 Art. 12 de la loi du 24 octobre 1997
111 Loi n° 410 de 1991

En principe, des données ne peuvent être traitées qu'avec le consentement des personnes concernées, sauf si le traitement repose sur un mandat légal[112].

Un décret-loi du 27 juillet 2005 a créé une série de nouvelles compétences et mesures pour les autorités de protection de l'Etat[113]. Celles-ci peuvent désormais surveiller les communications téléphoniques à titre préventif, en cas de soupçon fondé de terrorisme ou de menace contre l'Etat, sur demande approuvée par le premier ministre. Ce dernier peut déléguer cette compétence aux services de renseignement. La mesure est ordonnée par le ministère public, avec l'approbation préalable du juge. S'il y a urgence, il est possible d'engager la surveillance sans cette approbation, mais celle-ci doit être requise dans les 24 heures par la voie ordinaire. Le juge doit alors décider dans les 48 heures. Si ce délai n'est pas respecté, les renseignements recueillis ne sont pas exploitables devant les tribunaux.

En outre, la loi n° 675, limitée à fin 2007, a instauré l'obligation, pour la société de télécommunications et les fournisseurs Internet, de conserver les données téléphoniques et électroniques. Les autorités de protection de l'Etat peuvent maintenant entendre des détenus hors de la présence d'un défenseur (colloquio investigativo), procédure autrefois limitée aux infractions relevant de la Mafia.

Enfin, il est désormais possible d'expulser selon une procédure simplifiée les suspects présentant un danger pour la sécurité publique ou soutenant de quelconque manière une organisation terroriste. L'expulsion est immédiatement exécutoire, mais elle peut faire l'objet d'un recours devant le tribunal administratif. Si la décision d'expulsion se fonde sur des sources relevant des services secrets, les débats judiciaires peuvent être reportés de deux ans. La décision d'expulsion peut être suspendue si la personne en question coopère avec les autorités. Une autorisation d'établissement peut même être accordée si elle coopère de manière déterminante dans une enquête contre le terrorisme.

En cas d'abus, cette autorisation peut être retirée.

Le décret-loi du 27 juillet 2005 donne enfin au ministère de l'intérieur la possibilité d'instituer des unités anti-terroriste inter-forces de police (unità investigative interforze).

5. Luxembourg

Le Luxembourg est une monarchie constitutionnelle dotée d'un régime démocratique parlementaire; il est subdivisé en trois districts, douze cantons et 118 communes.

Trois institutions y sont chargées de la protection préventive de l'Etat: le Service de renseignement de l'Etat (SRDE), chargé de la sécurité intérieure, le Haut Commissariat de la sécurité extérieure (HCSE), service de renseignement civil chargé de la sécurité extérieure, et le Deuxième Bureau de l'armée, service de renseignement militaire.

112 Art. 12, al. 1, de la loi n° 675 du 31 décembre 1996 *«Tutella delle persone e di altri soggetti rispetto al trattamento die dati personali»*

113 Décret-loi n° 144 du 27 juillet 2005 (intégré à la loi du 31 juillet 2005)

Le SRDE, qui relève du ministère de l'intérieur, a pour tâches de lutter contre le terrorisme, l'espionnage, la prolifération des armes non conventionnelles et des technologies afférentes et la criminalité organisée dans ces domaines, mais aussi contre toutes les activités susceptibles de menacer l'intégrité, la souveraineté et l'indépendance du pays, la sécurité de ses institutions, le fonctionnement de l'Etat et la sécurité de la population[114]. Dans les limites de ses compétences, le SRDE coopère d'une part avec les autorités policières, judiciaires et administratives, d'autre part avec le HCSE. La police, les tribunaux et l'administration sont tenus, en retour, de lui transmettre les informations définies à l'art. 2 de la loi du 15 juin 2004.

La loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel régit le traitement des données personnelles par le SRDE. Celui-ci à accès à certaines banques de données, notamment la banque de données générale de la police, la banque de données de la police des étrangers et la banque de données des véhicules routiers[115]. La surveillance est exercée par le procureur général ou un de ses délégués et par deux représentants d'une commission spéciale, désignés par le ministre. Ils ont accès aux données traitées par le SRDE, ordonnent les rectificatifs nécessaires et informent les personnes concernées du fait que des données sont traitées à leur sujet conformément à la loi.

Dans les affaires relevant de la criminalité organisée et de la sécurité extérieure de l'Etat, le premier ministre peut ordonner des écoutes téléphoniques préventives à la demande du SRDE et avec l'accord d'une commission spéciale[116]. La surveillance doit cesser après trois mois, mais elle peut être renouvelée pour trois autres mois. Les renseignements recueillis ne sont pas exploitables devant les tribunaux si les personnes concernées sont dépositaires de secrets au sens de l'art. 458 du code pénal et qu'elles ne sont pas soupçonnées d'avoir commis ou d'avoir l'intention de commettre un acte punissable. Dans un tel cas, le chef du SRDE doit aussitôt détruire les documents. Les décisions de la commission doivent être transmises au directeur du service de télécommunication concerné, qui fait alors exécuter et contrôler les écoutes par un service créé à cet effet. Une fois l'écoute achevée, les personnes concernées reçoivent une copie des informations recueillies, à moins qu'elles ne soient classifiées secrètes. Si aucun résultat n'a été obtenu, tous les documents doivent être détruits. Dans le cas contraire, ils le sont à la fin de la procédure.

L'activité du SRDE est soumise au contrôle de la commission qui se compose des présidents de groupes politiques représentés à la Chambre des députés. Le directeur du service de renseignement l'informe des activités générales de son service. La commission peut consulter les dossiers et interroger les agents qui s'en occupent. Elle adresse au premier ministre, au chef du service de renseignement et aux députés de la commission de contrôle un rapport final confidentiel qui comprend des observations, des conclusions et des recommandations. La commission de contrôle parlementaire est informée tous les six mois des mesures mises en œuvre concernant les écoutes téléphoniques préventives.

Le SRDE ne peut pas effectuer de saisies et de perquisitions, ni interroger de témoins. Le premier ministre peut ordonner la surveillance, à l'aide de moyens techniques appropriés, de toute forme de communication s'il existe un soupçon que

114 Loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat (ci-après loi du 15 juin 2004)
115 Art. 4 de la loi du 15 juin 2004
116 Art. 88-3 du code pénal et loi du 26 novembre 1982

la sécurité de l'Etat soit menacée[117]. Des renseignements recueillis, seuls sont transmis aux services compétents le nom, le prénom et éventuellement l'adresse IP des personnes concernées[118]. Il n'est pas possible d'interdire à des personnes ou à des groupes de déployer des activités déterminées.

Plusieurs projets législatifs sont en préparation, notamment des modifications du code pénal concernant l'observation, l'infiltration et le traitement d'informations de police générale (POLIS)[119].

6. Pays-Bas

Les Pays-Bas sont une monarchie constitutionnelle. La reine est membre du gouvernement et nomme les ministres.

Les renseignements néerlandais comprennent le service de renseignement civil (AIVD)[120], deux services de renseignement militaire – le MIVD[121] et la Maréchaussée royale (BD)[122] – et le Service anti-terrorisme[123]. La coopération entre l'AIVD et la police s'est fortement intensifiée depuis les attentats du 11 septembre 2001.

La lutte contre le terrorisme est une des tâches principales de l'AIVD.

L'AIVD et le MIVD sont chargés des enquêtes, des analyses de sécurité et des mesures à l'encontre des organisations et des personnes soupçonnées de représenter un danger pour la sécurité, l'ordre démocratique ou d'autres intérêts essentiels de l'Etat[124]. Ils travaillent avec les autorités de police et de poursuite pénale, par l'intermédiaire du ministère public, en communiquant des renseignements sous forme de rapport. L'AIVD est habilité à demander aux services de renseignements régionaux (RID) et à la Maréchaussée royale d'agir pour son compte. Une révision du code de procédure criminelle permettra prochainement d'utiliser des informations recueillies par l'AIVD devant les tribunaux[125].

En principe, les personnes concernées peuvent demander à consulter les données relevées en relation avec des mesures prises contre elles; la protection des sources demeure cependant garantie. Les droits de consultation sont limités dans la mesure où la publication des données menace la sécurité intérieure. La commission de surveillance ad hoc, qui surveille l'activité des services et fait rapport au ministre compétent, doit être informée de tout refus du droit de consultation. L'AIVD et le MIVD sont habilités à surveiller les correspondances postales et les télécommunications à titre préventif. La demande du chef de l'AIVD ou du MIVD doit être approuvée au préalable par le ministre de la défense, avec l'accord du ministre de

117 Art. 88-3 du code d'instruction criminelle
118 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
119 Modifications du 17 mars 2006 et du 26 mai 2006
120 *Algemene Inlichtingen- en Veiligheidsdienst* (Service de renseignement et de sécurité général)
121 *Militaire Inlichtingen- en Veiligheidsdienst* (Service de renseignement et de sécurité militaire)
122 *Koninklijke Marechaussee, Bijzondere Dienst en Veiligheid* (Police militaire, Section spéciale de sécurité)
123 *Bijzondere Bijstands Eenheid* (Service spéciale d'assistance anti-terroriste).
124 Loi du 7 février 2002 sur le renseignement et la sécurité
125 *Parliamentary documents* II, 29 743

l'intérieur. S'il y a urgence, il est possible de faire approuver la demande a posteriori, mais cela doit être fait le plus vite possible.

En outre, les deux services peuvent mettre en place des missions d'observation à l'aide de moyens techniques, avec l'accord écrit du ministre compétent. L'observation et la perquisition de domicile doivent être autorisées par le ministre de l'intérieur ou le chef du service concerné. Sont également possibles l'usage d'identités d'emprunt et l'ouverture de lettres de tiers, si le tribunal d'arrondissement de La Haye approuve la demande du chef du service concerné. Les services sont également autorisés à pénétrer dans des systèmes informatiques de tiers si le ministre de l'intérieur ou le chef du service concerné donne son accord. Par contre, la saisie et la confiscation d'objets, ainsi que l'interdiction pour des personnes ou des organisations de déployer certaines activités, ne sont pas réglées expressément.

L'ombudsman national, indépendant vis-à-vis du gouvernement, surveille les activités des services. Son influence sur ces derniers a été limitée par une révision de la législation[126]. Il peut consulter leurs dossiers mais non les copier.

Le ministre compétent informe régulièrement la commission de contrôle parlementaire des activités des services.

7. UE

Le terrorisme est une des préoccupations de l'UE depuis l'institution d'Europol, l'Office européen de police, le 26 juillet 1995. Europol est voué notamment à la prévention et à la répression du terrorisme.

Depuis les attentats du 11 septembre 2001, l'UE mène une politique ciblée de lutte contre le terrorisme. Après les attentats à la bombe de Londres qui ont suivi, les ministres de l'intérieur et de la justice, réunis pour un sommet spécial, se sont prononcés pour un renforcement de la coopération entre les 25 Etats membres dans la lutte anti-terroriste. Ils ont appelé à une meilleure collaboration des polices et des services secrets.

Le 21 septembre 2005, la Commission de l'UE a présenté un ensemble de quatre mesures.

1. Une proposition de directive sur la conservation de données relatives au trafic des communications électroniques.

   Cette proposition prévoit l'harmonisation des obligations qui pèsent sur les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications en matière de traitement et de conservation de données relatives au trafic concernant la téléphonie mobile et la téléphonie fixe, ainsi que des données relatives au trafic concernant l'utilisation d'Internet, la durée de conservation étant d'un an pour les premières et de six mois pour les secondes.

2. Une décision financière en vue de l'allocation de 7 millions d'euros à un projet pilote dans le domaine de la prévention des attaques terroristes ainsi que de la préparation et de la réponse à ces dernières.

126 Loi du 3 février 2005

Cette décision vise en particulier à établir des liens entre services répressifs afin de faciliter le partage de l'information et la gestion des crises et à appuyer le programme européen à venir sur la protection des infrastructures critiques.

3. Une proposition de décision autorisant la signature de la convention n° 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 vise à inciter les 46 Etats membres du Conseil de l'Europe à mettre en place, pour lutter contre le blanchiment d'argent, des normes aussi exigeantes que celles qui sont applicables dans l'UE et à faire front commun dans la lutte contre le financement du terrorisme.

4. 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, comme l'y invite le Plan d'action de La Haye, à une stratégie que le Conseil devait définir sur la question avant la fin de l'année. Elle propose différentes manières de canaliser les efforts en ce sens dans des domaines tels qu'Internet, la coopération entre services répressifs et services secrets des Etats membres et les relations extérieures.

L'UE a pris le 20 septembre 2005 une décision relative à l'échange d'informations et à la coopération concernant les infractions terroristes (2005/671/JAI). Enfin, la Commission de l'UE a défini dix priorités pour les cinq prochaines années dans le cadre du programme de La Haye [COM(2005) 184], dont un programme de lutte contre le terrorisme.