14.xxx

Message concernant la loi sur le renseignement

du 19 février 2014

Messieurs les Présidents,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'une loi sur le renseignement, en vous proposant de l'adopter.

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames, Messieurs, l'assurance de notre haute considération.

19 février 2014

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Didier Burkhalter
La chancelière de la Confédération, Corina Casanova

Condensé

Le présent projet vise à créer une base légale formelle uniforme pour le service de renseignement civil de la Suisse, le Service de renseignement de la Confédération (SRC). Le SRC procède à la recherche d'informations, les analyse, les évalue et les transmet aux décideurs à tous les échelons pour qu'ils puissent accomplir leurs tâches de conduite à temps et de manière adaptée à la situation.

Selon le dernier rapport sur la politique de sécurité, le SRC fait partie des instruments de la politique de sécurité de la Confédération, au même titre que l'armée, la politique étrangère et la police.

Le principal objectif du projet est de régler dans la loi les activités, le mandat et le contrôle du SRC, afin qu'il puisse fournir, à titre préventif, une contribution substantielle pour la sécurité de la Suisse et de sa population.

Contexte

Parallèlement à l'adoption de la loi fédérale du 3 octobre 2008 sur le renseignement civil, le Conseil fédéral a décidé de transférer au Département fédéral de la défense, de la protection de la population et des sports (DDPS) les unités de renseignement du Service d'analyse et de prévention (SAP) à compter du 1er janvier 2009. Dans un deuxième temps, en mars 2009, il a décidé de regrouper au 1er janvier 2010 le SAP et le Service du renseignement stratégique (SRS) en un nouveau service, le Service de renseignement de la Confédération (SRC). Dans un troisième temps, il a chargé le DDPS de lui présenter d'ici fin 2013 un message relatif à une loi globale sur le renseignement (décision du 27 novembre 2009).

Selon le mandat du Conseil fédéral, la nouvelle loi doit établir les bases légales régissant les tâches, les droits, les obligations et les systèmes d'information du renseignement civil. Le but n'est pas de développer les bases légales en vigueur, mais de les codifier dans un nouvel ensemble, en tenant compte autant que faire se peut des critiques et des réserves qu'ont suscité les activités déployées par les services de renseignement dans notre pays (en particulier en ce qui concerne la collecte de données personnelles), ainsi que des nouveaux risques et des nouvelles menaces.

Contenu du projet

Les principales nouveautés qu'apporte le projet sont les suivantes:

- Base légale globale *pour le SRC: la dispersion des normes entre la loi fédérale sur le renseignement civil et la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) disparaît.*
- Nouvelle orientation de la recherche d'informations: *la distinction entre menaces provenant de l'intérieur et menaces provenant de l'étranger n'est plus prépondérante; l'extrémisme violent en lien avec la Suisse est en revanche clairement séparé des autres menaces et tâches.*

– Introduction de nouvelles mesures de recherche d'informations *dans les domaines du terrorisme, de l'espionnage, de la prolifération d'armes nucléaires, chimiques ou biologiques et des attaques contre des infrastructures critiques ou pour la sauvegarde d'autres intérêts essentiels de la Suisse: les moyens spéciaux de recherche d'informations que prévoyait le projet LMSI II et que le Parlement a renvoyés pour examen, tels que la surveillance du trafic par poste et télécommunications, l'engagement d'appareils de surveillance dans la sphère privée, sont présentés sous une forme remaniée et complétée. De l'avis du Conseil fédéral, ces nouvelles mesures de recherche d'informations sont nécessaires car les instruments dont dispose le SRC ne lui permettent plus d'assurer ses tâches de prévention face aux protagonistes de plus en plus agressifs qui menacent la sûreté intérieure ou extérieure de la Suisse et face aux formes de plus en plus complexes que prennent les menaces. Une instance judiciaire et une instance politique décideront de la mise en œuvre de ces mesures cas par cas.*

– Saisie et gestion différenciées des données: *le projet prévoit que les renseignements recherchés ou communiqués au SRC soient enregistrés dans un réseau de systèmes d'informations en fonction de leur thématique, de leur source et de leur sensibilité. Avant que des données personnelles saisies par le SRC soient utilisées dans un produit du SRC (par ex. un rapport d'analyse, une annonce à un service de renseignement étranger, une appréciation de la situation), leur exactitude et leur pertinence doivent être examinées. Les données issues d'une mesure de recherche soumise à autorisation seront traitées séparément: seuls les spécialistes du SRC y auront accès.*

– Régime de contrôle: *les activités du SRC seront soumises à un triple contrôle et surveillance, à savoir par le département auquel il est subordonné, par le Conseil fédéral et par la Délégation des Commissions de gestion du Parlement. L'exploration radio fera l'objet d'un contrôle supplémentaire par un organe de contrôle indépendant. Les nouvelles mesures de recherche soumises à autorisation qui sont proposées et l'exploration du réseau câblé ne seront mises en œuvre que sur autorisation du Tribunal administratif fédéral et avec l'aval du chef du DDPS après consultation de la Délégation du Conseil fédéral pour la sécurité. Ces mécanismes garantiront la légitimité et la proportionnalité des activités du SRC.*

Table des matières

Message

1 Présentation du projet

1.1 Contexte

Le présent projet vise à créer une base légale formelle uniforme pour le Service de renseignement de la Confédération (SRC). Ce service procède à la recherche d'informations, les analyse, les évalue et les transmet aux décideurs à tous les échelons pour qu'ils puissent accomplir leurs tâches de conduite à temps et de manière adaptée à la situation.

Selon le rapport du 23 juin 2010 du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse,[1] (ci-après rapport sur la politique de sécurité), le SRC constitue un des instruments de la politique de sécurité de la Suisse, au même titre que la politique étrangère, l'armée, la protection de la population, la politique économique, l'administration des douanes, la police et le service civil. Il fait partie du dispositif mis en place pour veiller à la sûreté de la Suisse.

Le rapport sur la politique de sécurité définit le rôle du SRC comme suit:

«En matière de sécurité intérieure et de sécurité extérieure, le SRC est le centre de compétence traitant de toutes les questions concernant le renseignement. Il soutient les organes de direction politiques et militaires et d'autres services de la Confédération et des cantons, et contribue, par ses renseignements et ses appréciations, à la prise de décisions largement étayées et ciblées en fonction des menaces. Le SRC engage ses moyens selon les besoins et les attentes de ses partenaires et des bénéficiaires de ses prestations. Il génère ainsi une utilité qui lui est propre en aidant à dresser un tableau global important pour les décideurs à tous les échelons.»

Cette définition délimite également le cadre dans lequel les tâches du SRC peuvent s'inscrire en vertu de la Constitution.

Le principal objectif du projet est de régler dans la loi les activités, le mandat et le contrôle du SRC afin qu'il puisse fournir, à titre préventif, une contribution substantielle pour la sécurité de la Suisse et de sa population.

Historique et mandat du Conseil fédéral

Dans son rapport du 29 février 2008 sur l'initiative parlementaire «Transfert des tâches des services de renseignement civils à un département»[2], la Commission de gestion du Conseil des États s'est prononcée comme suit sur les activités des services de renseignement:

En observant la nature des missions qui leur sont confiées ainsi que la définition légale de leurs domaines de compétences, on constate que les champs d'activité du SRS [Service de renseignement stratégique] et du SAP [Service d'analyse et de prévention] se chevauchent. Il y a deux raisons à cela: d'une part, il n'est pas toujours possible d'opérer une distinction claire entre sécurité extérieure et sécurité intérieure, et d'autre part, l'exécution de certaines missions du SRS peut nécessiter des activités à l'intérieur du pays, tandis que le SAP, pour mener à bien les siennes,

1 FF **2010** 4681
2 FF **2008** 3609

dépend souvent de contacts extérieurs. Il apparaît donc que la collaboration entre ces deux services constitue une condition sine qua non pour leur efficacité ainsi que pour le succès de leurs opérations. …

En juin 2005, le Conseil fédéral a décidé de supprimer le poste de coordinateur des services de renseignement pour mettre l'accent sur l'amélioration de la collaboration directe entre les services de renseignement civils respectifs du DDPS et du DFJP. Il s'agissait en particulier de renforcer la collaboration entre le SAP et le SRS pour pouvoir faire face aux menaces transnationales. À cet effet, le Conseil fédéral a décidé de créer des plates-formes pour l'échange d'informations et l'analyse conjointe dans les domaines du terrorisme, de la criminalité organisée et de la prolifération.

Dans le cadre de sa haute surveillance sur les services de renseignement et la protection de l'État, la Délégation des Commissions de gestion (DélCdG) avait alerté depuis longtemps le Conseil fédéral, de même que les départements concernés, sur les lacunes dans la collaboration entre les deux services. Si la délégation a considéré la mise en place de ces plates-formes en 2005 comme un premier pas pragmatique en direction d'une réforme, elle a toutefois estimé que ces mesures n'amélioraient pas la conduite politique des services de renseignement. La délégation a donc réitéré les positions qu'elle avait exprimées en 2004 et exigé que lesdits services soient subordonnés à un seul et unique département, et placés le plus rapidement possible sous une direction commune. La DélCdG s'est néanmoins déclarée prête, dans un premier temps, à accompagner la mise en œuvre des réformes adoptées par le Conseil fédéral et à patienter jusqu'à fin 2006 pour constater leurs effets. …

La DélCdG a exprimé son désaccord avec les points essentiels des conclusions présentées par le Conseil fédéral, au vu de la persistance des carences qu'elle avait relevées dans ses rapports annuels 2004, 2005 et 2006. Elle avait notamment constaté, à l'occasion de nombreuses auditions et de trois inspections inopinées, que les mesures prises n'avaient pas apporté les améliorations attendues sur le plan de la coopération entre le SAP et le SRS. …

Aussi la DélCdG a-t-elle estimé qu'il était urgent d'agir. Elle exige que la coopération des services de renseignement intérieur et extérieur cesse de dépendre du bon vouloir des deux départements, et demande qu'un seul département soit désormais compétent en la matière. À l'unanimité, la DélCdG a donc décidé de proposer le transfert par voie législative des tâches des deux services de renseignement civils à un seul département.

La loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC)[3], élaborée à la suite de cette initiative parlementaire, est entrée en vigueur le 1er janvier 2010.

Après l'approbation de la LFRC, le Conseil fédéral a décidé dans un premier temps de transférer au DDPS les unités de renseignement du SAP à compter du 1er janvier 2009. Dans un deuxième temps, en mars 2009, il a décidé de regrouper au 1er janvier 2010 le SAP et le SRS en créant le SRC.

Dans un troisième temps, le Conseil fédéral a chargé le DDPS de lui présenter d'ici fin 2013 un message relatif à une loi globale sur le renseignement (décision du 27 novembre 2009):

3 RS **121**

Le Conseil fédéral charge le DDPS

… de présenter d'ici fin 2013 un message relatif à un projet de loi sur le renseignement qui crée les bases légales régissant les tâches, les droits, les obligations et les systèmes d'information des services de renseignement civils de la Suisse. Les parties controversées du message du 15 juin 2007 relatif à la modification de la LMSI[4] *et les dispositions en vigueur seront intégrées au projet de loi sous une nouvelle forme.*

Échelonnement des travaux visant à mettre en œuvre la décision du 27 novembre 2009

Au printemps 2009, le Conseil national et le Conseil des États ont renvoyé au Conseil fédéral le projet LMSI II du 15 juin 2007 (Moyens spéciaux de recherche d'informations)[5] pour l'examen de quelques questions d'ordre constitutionnel soulevées par les mesures de recherche de renseignement qui étaient prévues dans le projet et qui s'inspiraient des mesures de contrainte fondées sur le droit de procédure pénale. Seul le Conseil des États s'est penché sur les différents articles du projet de loi, le Conseil national s'étant arrêté à la question de l'entrée en matière. L'acceptation politique des différents éléments du projet ne peut dès lors être déduite que de manière limitée des débats au Parlement.

Par la suite, le Conseil fédéral a demandé une expertise pour l'examen des questions d'ordre constitutionnel et décidé d'échelonner les travaux législatifs (décision du 27 novembre 2009): le premier projet, à traiter rapidement, devait fixer dans la LMSI les dispositions majoritairement non contestées et prêtes à être mise en œuvre. Cette partie a été réalisée par le message complémentaire du 27 octobre 2010 relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure («LMSI II réduite»)[6], adopté par le Parlement le 23 décembre 2011. La LMSI révisée est entrée en vigueur le 16 juillet 2012.

Le deuxième projet était la présente loi, qui devait régler l'ensemble des activités de renseignement.

Élaboration du projet de loi

Le SRC a institué un groupe de travail interdépartemental chargé de préparer la nouvelle loi. Ce groupe se composait de représentants du DDPS, du Département fédéral des affaires étrangères (DFAE), du Département fédéral de justice et police (DFJP), du Ministère public, des cantons et du SRC. Un collaborateur du Préposé fédéral à la protection des données et à la transparence a collaboré à l'examen des questions relatives à la protection des données.

Le groupe de travail a débuté ses travaux fin octobre 2010 et a élaboré jusqu'en juillet 2011 une stratégie et une esquisse de l'acte normatif. Se Le SRC a ensuite rédigé le présent projet en se fondant sur ces travaux. Les différentes versions du projet ont été soumises au groupe de travail pour avis.

Les normes de la LMSI et de la LFRC qui ont donné de bons résultats et certaines normes issues du projet LMSI II réduite ont été reprises dans le projet de loi. Par

4 Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI), RS **120**

5 Message du 15 juin 2007 relatif à la modification de la loi instituant des mesures visant au maintien de la sûreté intérieure (FF **2007** 4773)

6 FF **2010** 7147

exemple, l'obligation spécifique de fournir et de communiquer des renseignements et l'interdiction d'exercer une activité correspondent globalement aux dispositions contenues dans la LMSI II réduite.

Le but de la nouvelle loi sur le renseignement n'est pas de développer les bases légales en vigueur (ni «LMSI III» ni «LFRC II»), mais de les codifier dans un nouvel ensemble, en tenant compte autant que faire se peut des critiques et des réserves qu'ont suscité les activités déployées par les services de renseignement dans notre pays, ainsi que des nouveaux risques et des nouvelles menaces.

L'introduction de moyens spéciaux pour la recherche d'informations s'est avérée de loin la mesure la plus controversée, aussi bien dans le cadre de la procédure de consultation du projet de 2007 que dans les débats politiques et les médias.

C'est pourquoi le Conseil fédéral a renoncé dans son projet LMSI II réduite à une série de moyens de recherche d'informations soumis à autorisation, notamment:

– la surveillance de la correspondance par poste et télécommunication;
– l'observation de lieux qui ne sont pas librement accessibles au public, y compris au moyen d'appareils techniques de surveillance;
– l'intrusion dans des systèmes informatiques de traitement de données.

Ces moyens de recherche sont repris en substance dans le présent projet de loi.

La 8 mars 2013, le Conseil fédéral a approuvé l'avant-projet de loi sur le renseignement et chargé le DDPS de lancer la procédure de consultation. Cette procédure a été ouverte le 8 mars 2013 et s'est achevée le 30 juin 2013. Le Conseil fédéral a pris connaissance des résultats de la consultation le 23 octobre 2013 et chargé le DDPS de poursuivre les travaux législatifs.

1.2 Dispositif proposé

Principaux éléments du projet

Base légale globale pour le SRC

Nouvelle orientation de la recherche d'informations

Le projet de loi comporte une nouveauté en matière de recherche d'informations, dans la mesure où la distinction entre menaces provenant de l'intérieur du pays et menaces provenant de l'étranger n'est plus prépondérante; l'extrémisme violent en lien avec la Suisse est en revanche séparé des autres menaces et tâches. Cette nouvelle optique a pour conséquence que les mesures de recherche d'informations soumises à autorisation ne peuvent pas être mises en œuvre pour l'extrémisme violent. Les événements survenus au DFJP qui avaient conduit à l'institution d'une commission d'enquête parlementaire (rapport de la Commission d'enquête parlementaire du 22 novembre 1989 sur les événements survenus au DFJP[7]) ne risqueront plus de se produire puisque le terrorisme et l'extrémisme violent seront clairement séparés. À l'instar de la gestion des données, la recherche d'informations dans le domaine de l'extrémisme violent essentiellement lié à la Suisse ou à des acteurs suisses doit être soumise à des conditions plus strictes dès lors qu'elle porte atteinte

7 FF **1990** 593

aux droits fondamentaux. Conformément à l'art. 69, al. 1, let. c, du projet, le Conseil fédéral établira chaque année une liste des groupements entrant dans la catégorie des extrémistes violents.

Introduction de nouvelles mesures de recherche d'informations dans les domaines du terrorisme, de l'espionnage, de la prolifération d'armes nucléaires, chimiques ou biologiques et des attaques contre des infrastructures critiques ou pour la sauvegarde d'intérêts essentiels de la Suisse au sens de l'art. 3.

Les moyens spéciaux de recherche d'informations qui étaient prévus dans le projet LMSI II[8]et que le Parlement a renvoyés pour examen ont été expertisés pour déterminer leur conformité à la Constitution et au droit international (expertise du professeur Giovanni Biaggini de juin 2009[9]). Le catalogue des moyens spéciaux de recherche d'informations contenu dans la LMSI II a été remanié et complété dans le présent projet. Le Conseil fédéral demande que les mesures suivantes soient introduites pour la recherche d'informations soumises à autorisation en Suisse:

- surveillance de la correspondance par poste et télécommunication conformément aux dispositions de la loi fédérale du 6 octobre 2000[10] sur la surveillance de la correspondance par poste et télécommunication, y compris informations sur les raccordements et les communications par poste et télécommunication de personnes surveillées et renseignements sur la position d'antennes auxquelles le téléphone portable d'une personne surveillée est relié;
- engagement d'appareils de localisation pour déterminer la position et les mouvements de personnes ou d'objets;
- engagement d'appareils de surveillance pour mettre sur écoute ou enregistrer des conversations privées et pour observer ou enregistrer des événements qui ne se produisent pas dans des lieux publics;
- introduction dans des systèmes et des réseaux informatiques pour rechercher des informations ou, exceptionnellement, pour perturber, empêcher ou ralentir l'accès à des informations;
- fouilles de locaux, de véhicules ou de conteneurs emportés par des personnes.

Ces mesures ne pourront être mises en œuvre que sur autorisation du Tribunal administratif fédéral et avec l'aval du chef du DDPS après consultation de la Délégation du Conseil fédéral pour la sécurité.

Ces nouvelles mesures de recherche d'informations sont proposées parce que les instruments à la disposition du SRC (art. 14 LMSI) ne lui permettent plus d'assurer ses tâches de prévention dans le domaine de la sûreté intérieure, les menaces prenant des formes de plus en plus agressives et complexes. Pour de plus amples informations, on se référera aux commentaires relatifs aux art. 25 ss (Mesures de recherche soumises à autorisation).

8 Message du 15 juin 2007 relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (FF **2007** 4773).

9 Ce document peut être consulté à l'adresse suivante: www.chf.admin.ch > Documentation > Jurisprudence des autorités administratives de la Confédération (JAAC) > JAAC 2009 > 2009.14 (pp. 238–330).

10 RS **780.1**

Mise à profit des développements techniques pour les mesures de recherche non soumises à autorisation

Les mesures de recherche non soumises à autorisation (art. 13 ss) sont également élargies pour tirer profit des nouvelles possibilités techniques (par ex. l'engagement de moyens d'exploration aériens). Aucune base légale formelle ne permet actuellement l'engagement de tels moyens, de sorte que la situation juridique manquait de clarté.

Traitement différencié des données

Le projet de loi prévoit que les renseignements recherchés ou communiqués au SRC soient enregistrés dans un réseau de systèmes d'informations en fonction de leur thématique, de leur source et de leur sensibilité. Avant que des données personnelles saisies par le SRC soient utilisées dans un produit du SRC (par ex. un rapport d'analyse, une annonce à un service de renseignement étranger, une appréciation de la situation), leur exactitude et leur pertinence doivent être examinées. Les données issues d'une mesure de recherche soumise à autorisation ou de contrôles à la frontière seront traitées séparément: seuls les spécialistes du SRC y auront accès.

Régimes de contrôles

Les activités du SRC seront soumises à un triple contrôle et surveillance, à savoir par le département auquel il est subordonné, par le Conseil fédéral et par la Délégation des Commissions de gestion du Parlement. L'exploration radio continuera de faire l'objet d'un contrôle supplémentaire par un organe de contrôle indépendant.

Possibilités de recours

Le projet prévoit la possibilité de recourir auprès du Tribunal administratif fédéral et, en deuxième instance, auprès du Tribunal fédéral contre les décisions et les mesures de recherche d'informations soumises à autorisation prises par le SRC.

1.3 Appréciation de la solution retenue

Contribution substantielle pour la sûreté de la Suisse

La Suisse est tributaire d'un service de renseignement efficace pour défendre ses intérêts et assurer la protection de ses citoyens. Il faut cependant aussi prendre en compte les libertés fondamentales de la population.

Le SRC et les autorités d'exécution cantonales ont pour tâche de fournir une contribution substantielle pour la préservation des intérêts et le maintien de la sûreté intérieure et extérieure de la Suisse en respectant les libertés constitutionnelles des citoyens. Ils doivent rechercher les informations nécessaires avec des moyens et des méthodes du renseignement (en utilisant des sources d'informations publiques et non publiques et des informateurs), les traiter, les analyser et les transmettre sous une forme appropriée aux décideurs de l'État à tous les échelons (Confédération et cantons). À cet effet, il est indispensable que le SRC puisse procéder à une appréciation globale de la menace. Avec les moyens actuels de recherche d'informations définis par la LMSI dans le domaine de la sûreté intérieure, qui se concentrent principalement sur la recherche d'informations de publiques, les demandes de renseignement et l'observation dans des lieux publics (art. 14 LMSI), le SRC ne peut

que partiellement accomplir son mandat. C'est pourquoi le présent projet complète les mesures de recherche d'informations dans le domaine de la sûreté intérieure par des mesures de recherche soumises à autorisation. Il règle aussi la recherche d'informations par les cantons et les autorités d'exécution cantonales.

De manière générale, le SRC fournit dans les meilleurs délais aux bénéficiaires de ses prestations des informations et des appréciations ciblées qu'ils ne peuvent obtenir par d'autres moyens.

Contexte international

Au XXIe siècle, le renseignement continue de relever essentiellement des États et constitue un instrument de la conduite politique d'un pays. C'est particulièrement vrai la Suisse: en tant qu'État indépendant et neutre, la Suisse ne peut compter que sur elle-même. En effet, la majorité de nos partenaires en Europe sont membres de l'Organisation du traité de l'Atlantique Nord (OTAN) ou de l'Union européenne (UE). La création de nouveaux organismes, tels que le Groupe des vingt (G20), où sont prises d'importantes décisions qui concernent aussi la Suisse mais pour lesquelles notre pays n'est que rarement consulté, viennent renforcer ce constat. Les membres de l'UE et de l'OTAN entretiennent aussi d'étroites relations dans le domaine de l'échange d'informations. Leur statut de membre les fait bénéficier d'une vue d'ensemble de la situation, mise à jour en permanence. Grâce ses contacts avec les services de renseignement étrangers et les informations qu'il obtient, le SRC soutient donc la politique extérieure de la Suisse.

Conséquences de l'affaire Snowden

Les révélations de l'ancien employé des services secrets américains Edward Snowden dont les médias se sont récemment fait l'écho donnent un nouvel aperçu des pratiques de grands services de renseignement internationaux, en particulier dans le domaine de la surveillance des communications. Lorsque des solutions techniques permettent de s'introduire dans des systèmes de communication, ces services internationaux n'épargnent pas des pays en principe amis. La dimension de telles surveillances est totalement nouvelle: pour autant que les moyens financiers et techniques et le personnel soient suffisants, le monde entier ou presque peut être surveillé. Aussi le public a-t-il pris conscience des dangers d'une utilisation quasiment illimitée et non contrôlée des techniques modernes.

La loi sur le renseignement doit fixer à cet égard un cadre juridique clair qui limite étroitement l'utilisation de tels moyens par le service de renseignement suisse, les lie à l'obligation de respecter les principes de proportionnalité et de nécessité et les soumet à des contrôles juridiques, politiques et démocratiques. Renoncer totalement à de tels moyens serait en revanche une erreur: la Suisse laisserait le champ libre aux intérêts étrangers et, faute d'accès aux canaux d'informations pertinents, les organes de contre-espionnage suisses resteraient incapables de détecter et identifier les indices de telles activités.

Le Conseil fédéral est donc d'avis qu'en plus des efforts diplomatiques à l'échelon international, la Suisse doit disposer de moyens efficaces et autonomes de détection et de contre-espionnage pour protéger sa sécurité. Des moyens de recherche d'informations dans des domaines auxquels le service de renseignement suisse n'avait pas accès jusqu'à présent en font aussi partie.

Codification globale

Le présent projet met en œuvre la décision du Conseil fédéral du 27 novembre 2009 et codifie dans un seul et même acte les activités du SRC, alors que les dispositions sur la recherche d'informations en Suisse et sur la recherche d'informations à l'étranger sont actuellement contenues dans deux lois distinctes.

La distinction entre les menaces provenant de l'intérieur de la Suisse et celles provenant de l'étranger n'est plus prépondérante dans le projet de loi; celle-ci sépare en revanche l'extrémisme violent en lien avec la Suisse des autres champs de menaces et tâches. Compte tenu des formes actuelles de menaces (émanant par ex. du terrorisme), il n'est souvent pas possible de fixer une limite claire entre la Suisse et l'étranger.

Le projet de loi règle les tâches principales du SRC et contient les dispositions qui requièrent une base légale formelle en vertu de la Constitution. Le Conseil fédéral précisera en détail les domaines d'activité du SRC, dans le respect du cadre légal, en lui confiant un mandat de base qui se fonde sur les intérêts spécifiques de la Suisse et sur l'appréciation de la menace.

Le projet prend également en compte le fait que les activités de renseignement sont soumises à des conditions particulières tant en Suisse qu'à l'étranger (maintien du secret sur les méthodes utilisées, les informations et les processus et moyens techniques ainsi que sur les sources, les collaborateurs et les informateurs) et règle avec précision les atteintes inévitables aux droits fondamentaux.

Élimination des lacunes et des faiblesses du droit en vigueur

Les faiblesses du droit en vigueur sont principalement dues à la conception de la LMSI. Son contenu a été influencé par les conclusions du rapport de la Commission d'enquête parlementaire du 22 novembre 1989 concernant les événements survenus au DFJP, dont l'impact public et politique se ressent encore.

En fixant des limites très strictes au traitement d'informations avant une poursuite pénale, le législateur a sciemment accepté de prendre un certain risque au niveau de la sécurité. Ce risque devait toutefois être minimisé par un suivi attentif des développements et par une nouvelle appréciation périodique de la situation. La recherche, le traitement et la transmission de données sensibles ont été réglés et limités par des dispositions détaillées. La LMSI répondait ainsi aux exigences strictes de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[11]. Peu après l'entrée en vigueur de la LMSI, les attentats du 11 septembre 2001 ont complètement changé la donne. Plusieurs interventions parlementaires ont alors demandé un renforcement du rôle des organes de protection de l'État et des services de renseignement, une augmentation des moyens et des instruments à leur disposition et la présentation de rapports détaillés sur la situation en matière de sécurité. En novembre 2001, le Conseil fédéral a chargé le DFJP de lui soumettre un rapport et des propositions pour renforcer la sécurité et lutter contre le terrorisme. En juin 2002, le Conseil fédéral a approuvé le rapport «Analyse de la situation et des menaces pour la Suisse à la suite des attentats terroristes du 11 septembre 2001»[12] et pris simultanément connaissance du projet de révision de la LMSI, qui visait notamment à combler les

11 RS **235.1**
12 FF **2003** 1674

lacunes que présentaient les instruments permettant de détecter et d'identifier les menaces.

Le 15 juin 2007, après plusieurs années de travaux, le Conseil fédéral a soumis au Parlement un message relatif à la modification de la LMSI (Moyens spéciaux de recherche d'informations; «LMSI II»). Ce projet présentait la situation en matière de sécurité et les lacunes identifiées dans le dispositif préventif de défense pour tous les domaines pertinents du point de vue des menaces.

Comme mentionné plus avant, le projet LMSI II a été renvoyé au Conseil fédéral par le Parlement au printemps 2009. Les principales lacunes et faiblesses de la LMSI n'ont de ce fait pas été comblées depuis.

Ainsi, selon le droit en vigueur, la correspondance par poste et télécommunication ne peut en principe faire l'objet d'aucune recherche en vertu de la LMSI. Là où cette source d'informations fait défaut, les services de renseignement doivent essayer d'obtenir des informations en prenant contact sous une fausse identité avec les groupes et personnes visés, ce qui implique des efforts beaucoup plus conséquents. Sur un plan purement technique, il est certes possible d'accéder à des ordinateurs et à des réseaux informatiques protégés par des mots de passe où des actions terroristes seraient discutées, mais ces mesures sont interdites car ces domaines sont assimilés à la sphère privée. Il en résulte des lacunes au niveau de la détection précoce et de la collaboration internationale.

Selon le droit en vigueur, les lieux qui ne sont pas librement accessibles (par ex. les chambres d'hôtel) échappent en général à toute possibilité d'exploration en matière d'espionnage. Les espions utilisent cette lacune à dessein; bénéficiant souvent de l'immunité diplomatique, ils sont formés pour collecter secrètement des informations. Les recherches menées par des bureaux d'investigation internationaux, qui agissent parfois (secrètement) sur mandat d'un État, complètent le tableau. La législation actuelle limite donc aussi les activités de contre-espionnage, qui s'arrêtent en principe au seuil de la sphère privée. Le dispositif de défense souffre ainsi d'importantes lacunes.

Le trafic d'armes de destruction massive passe par des réseaux internationaux extrêmement complexes. La Suisse peut recevoir à cet égard des indications de tiers sur l'implication d'entreprises et d'instituts financiers, mais comme dans les domaines du terrorisme et de l'espionnage, le SRC n'est pas en mesure d'étayer des présomptions d'activités de prolifération de telles armes parce qu'il n'a pas le droit d'exercer une surveillance ciblée de la sphère secrète et de la sphère privée.

Les lacunes et les faiblesses du droit en vigueur ont aussi fait l'objet d'une série d'interventions parlementaires:

- La nécessité d'une réglementation a été reconnue en ce qui concerne l'engagement de moyens pour l'exploration électronique (11.3862 – Interpellation Amherd, «Renforcement de la surveillance sur Internet»; 11.3471 – Interpellation Malama «Surveillance de l'espace privé. Associer la protection des données et la sûreté intérieure)».
- Il en va de même pour la lutte contre l'extrémisme (11.4076 – Interpellation Eichenberger-Walther «Réglementation future de l'activité de protection de l'État»; 11.4059 – Interpellation, Geissbühler «Surveillance de l'extrémisme de droite en Suisse)».

– Des mesures ont aussi été demandées pour la protection de la place financière suisse (10.3028 – Interpellation Groupe de l'Union démocratique du centre «Vol de données bancaires. Instaurer des mesures visant au respect de l'État de droit»; 09.4146 – Interpellation Wehrli «Place financière suisse. Stratégie)»

Procédure de consultation

Prises de position dans la procédure de consultation

Le 8 mars 2013, le Conseil fédéral a approuvé l'avant-projet de loi sur le renseignement et chargé le DDPS d'ouvrir une procédure de consultation.

Cette procédure a duré du 8 mars au 30 juin 2013. Sur les 72 destinataires invités à s'exprimer sur le projet, 68 ont adressé une réponse au DDPS (26 cantons, 8 partis, 34 organisations et autres milieux intéressés).

Les cantons, qui sont responsables au premier chef de la sûreté intérieure, ont salué dans l'ensemble le projet. Ils ont souhaité toutefois des précisions concernant la collaboration avec la Confédération, en particulier en ce qui concerne les questions de surveillance. Quelques cantons ont soutenu le projet sous réserve de la création d'une nouvelle base constitutionnelle.

Tous les grands partis politiques (à l'exception des Verts et du Parti Pirate Suisse, qui ont refusé le projet) se sont déclarés globalement favorables au projet, en exprimant parfois quelques réserves et souhaits de modifications.

Les avis des associations faîtières de l'économie allaient de l'acceptation du projet à son refus; les milieux des télécommunications ont essentiellement critiqué les coûts de la surveillance, mais ceux-ci découlent principalement des dispositions inscrites dans la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Cette loi est actuellement en révision et c'est dans ce cadre que la question doit être examinée en priorité.

La gamme des avis exprimés par les autres milieux concernés était assez équilibrée: elle allait de l'acceptation globale du projet à son rejet complet en passant par des avis plutôt positifs ou critiques.

Parallèlement à l'analyse des prises de position, des entretiens ont été menés avec la Conférence des commandants des polices cantonales de Suisse (CCPCS) et des représentants des télécommunications pour clarifier certains points. Ils ont permis de rechercher et de définir des règles plus précises et d'éliminer quelques divergences.

Adaptation du projet de loi mis en consultation

Le 23 octobre 2013, le Conseil fédéral a pris acte du rapport sur les résultats de la procédure de consultation[13] et chargé le DDPS de rédiger un message pour la fin de l'année 2013.

13 www.admin.ch > Droit fédéral > Procédures de consultation terminées > 2013 > Département fédéral de la défense, de la protection de la population et des sports > Loi sur le renseignement

Les principales décisions prises lors de l'analyse des résultats de la consultation sont les suivantes:

- Ne pas créer une base constitutionnelle séparée pour le renseignement (voir ch. 5.1).
- Préciser les règles régissant la collaboration avec les cantons (en commun avec la CCPCS) et élargir les droits de surveillance cantonaux afin d'éviter des lacunes dans les contrôles (voir commentaires relatifs aux articles concernés).
- Maintenir les règles concernant l'exploration du réseau câblé (voir commentaires relatifs aux articles concernés).
- Clarifier les voies de droit.

Notons que de nombreuses remarques ont pu être réglées en complétant ou précisant les commentaires des dispositions.

Appréciation générale

À plusieurs égards, le présent projet de loi a une portée considérable pour la politique nationale. Il traite de questions délicates et cruciales en matière de droits fondamentaux, notamment du droit de la population de bénéficier d'une protection de la liberté individuelle mais également d'être protégée face aux menaces qui dépassent le cadre des cas individuels relevant des autorités de police et de poursuite pénale. Voilà pourquoi l'art. 2 (but) énonce que la présente loi vise à préserver les fondements de la démocratie et de l'état de droit en Suisse ainsi que la sécurité de la population suisse. L'État n'est donc pas protégé pour lui-même, mais pour mettre en œuvre les buts fondamentaux définis dans la Constitution.

Ainsi, la LRens part du principe que les mesures de renseignement doivent être autant que possible étroitement axées sur les menaces effectives et sur leurs auteurs et que la majorité de la population ne doit pas y être soumise. En cas de grandes menaces pour la sûreté intérieure ou extérieure qui impliquent un grand nombre de personnes, des mesures intrusives, mais bien ciblées, sont autorisées afin de pouvoir identifier et évaluer la situation à temps. Des conditions légales strictes, une procédure d'autorisation efficace et des instruments de contrôle et de surveillance sont mis en place pour assurer le respect de ces lignes directrices. De nouvelles voies de recours permettront au surplus aux instances judiciaires de vérifier que les dispositions légales sont bel et bien respectées.

La LRens régit également les mesures de recherche d'informations à l'étranger. Même si les normes applicables diffèrent quelque peu, elles suivent toutes des principes identiques de proportionnalité et de préservation des droits fondamentaux. Certes, la recherche d'informations à l'étranger et au sujet de l'étranger se déroule dans un vaste flou du point de vue du droit international. Tous les États pratiquent le renseignement et, inversement, tous les États le punissent lorsqu'il est dirigé contre eux. La LRens ne peut échapper à ce paradoxe, mais elle énonce clairement que la recherche d'informations doit répondre aux règles de la proportionnalité et que l'essence des droits fondamentaux doit également être garantie à l'étranger. Elle respecte donc à la fois les dispositions de la Constitution et les obligations internationales de la Suisse.

Notons que le Service de renseignement ne constitue ni une police auxiliaire ni une source primaire d'informations pour les autorités de poursuite pénale, mais qu'il accomplit des tâches autonomes en matière de sûreté centrées sur l'identification précoce des menaces sans effectuer aucune tâche pénale. C'est pourquoi ses rapports sont axés sur les dispositions prises pour prévenir les menaces, et non sur la poursuite pénale d'infractions qui ont déjà été commises.

Dans la pesée des intérêts, le Conseil fédéral a opté pour des solutions pondérées et réduites au strict nécessaire. Du reste, les résultats de la procédure de consultation l'ont confirmé en grande partie, et nombre de précisions ont encore été apportées au projet. Ce projet de loi permettra de mener concrètement et de manière fondée le débat sur la relation entre la liberté et la sûreté, mais aussi entre la transparence et la nécessité de maintenir le secret, ainsi que sur les rôles que doivent jouer la Confédération et les cantons.

1.4 Adéquation des moyens requis

Garantir la sécurité fait partie des tâches prioritaires de l'État. Afin de défendre les intérêts et d'assurer la protection de ses citoyens et de pouvoir prendre les mesures nécessaires à cet effet, la Suisse est tributaire d'un service de renseignement performant qui détecte et empêche les activités menaçant la sûreté.

Les développements de la société et des techniques et les dimensions de plus en plus globales que prennent les menaces (par ex. extrémisme, terrorisme, criminalité économique, prolifération d'armes nucléaires ou chimiques) requièrent une détection et une réaction plus efficace et plus précoce. Pour ce faire, le Service de renseignement civil doit aussi pouvoir utiliser des technologies et des méthodes modernes.

Compte tenu de ce qui précède, le Conseil fédéral estime que les coûts liés à la mise en œuvre de la loi se justifient puisque le SRC restera bien en-deçà de la taille des services de renseignement d'États européens comparables à la Suisse, même après la création des postes supplémentaires demandés.

1.5 Comparaison avec le droit étranger, notamment européen

Le tableau ci-après compare divers aspects des systèmes de renseignement de pays européens proches de la Suisse. Ces pays ont été choisis sur la base des critères suivants:

- L'Allemagne et la France sont d'importants pays voisins et ils ont une tradition juridique semblable à celle de la Suisse.
- En Espagne et aux Pays-Bas, le service de renseignement est un organisme qui a fusionné avec d'autres services de renseignement, comme le SRC.
- L'Autriche et la Belgique sont des pays qui ont une taille comparable à celle de la Suisse.

	Allemagne *Bundesamt für Verfassungsschutz (BfV)* *(Office fédéral de protection de la Constitution)* *Bundesnachrichtendienst (BND)* *(Service de renseignement fédéral)*
Position dans l'architecture de la sûreté	*BfV:* Le Service de renseignement interne (de même que les offices des Länder chargés de la protection de la Constitution) est subordonné au **Ministère de l'intérieur**. *BND:* Le Service de renseignement sur l'étranger est directement subordonné au **gouvernement fédéral.** Mis à part ces deux services, seul le *Militärische Abschirmdienst* (service de protection militaire) garde encore le statut de service de renseignement.
Tâches	*BfV:* – Collecter et évaluer des informations, des renseignements et des documents relatifs aux activités menées contre l'ordre constitutionnel libéral et démocratique ou contre la pérennité ou la sécurité de la République fédérale ou de l'un de ses Länder; collecter et évaluer des informations, des renseignements et des documents relatifs aux activités qui, par un usage de la violence ou la préparation de tels actes, constituent une menace pour les affaires étrangères de la République fédérale ou qui visent à mettre en péril l'entente entre les peuples, en particulier la cohabitation pacifique entre les peuples. – Lutter contre l'espionnage; lutter contre la prolifération d'armes nucléaires, chimiques ou biologiques, protéger l'économie; coopérer lors d'enquêtes de sûreté et de contrôles de sécurité relatifs aux personnes menés en vue de protéger des informations secrètes ou de prévenir des actes de sabotage *BND:* – Collecter et évaluer des informations nécessaires à l'acquisition de connaissance importantes pour l'État en matière de politique étrangère et de sûreté. – Fournir des informations politiques, économiques, militaires et de technologiques au sujet de pays étrangers.
Compétences (engagement de moyens de renseignement)	*BfV:* L'engagement de moyens de renseignement est clairement réglé par la loi. Pour accomplir les tâches qui lui sont dévolues, le *BfV* a le droit, sous réserve des conditions fixées par les dispositions légales:

– d'appliquer ou d'engager des méthodes et d'utiliser des objets et des instruments dans le but d'acquérir secrètement des informations (par ex. personnes de confiance, observations, enregistrements d'images et de sons, identités d'emprunt, couvertures);

– de collecter des informations auprès d'établissements financiers, d'entreprises postales, de compagnies aériennes et d'entreprises de télécommunication;

– d'accéder à diverses banques de données gérées par la République d'Allemagne (par ex. au registre central des étrangers de l'Office fédéral des migrations et des réfugiés, aux données en matière d'asile de l'Office fédéral pour la reconnaissance de réfugiés étrangers ou encore au registre des véhicules).

Pour l'observation d'organisations et d'individus, le *BfV* doit disposer d'indices concrets d'activités pouvant constituer une menace pour l'ordre constitutionnel ou la sûreté du pays.

BND:

Les moyens engagés à l'étranger ou pour se renseigner sur l'étranger (avant tout acquisition de connaissances par des informateurs et par l'exploration des télécommunications) ne sont pas régis par la loi: les dispositions légales ne règlent que les activités du *BND* sur le territoire allemand.

En accord avec les dispositions de la loi allemande sur la protection des données, il peut se procurer, traiter et exploiter les informations dont il a besoin, y compris des données concernant des personnes:

– pour la protection de ses collaborateurs, des installations, des objets et des sources contre des activités représentant une menace pour la sûreté ou contre des activités de services secrets;

– pour le contrôle de sécurité relatif aux personnes qui travaillent ou qu'il entend faire travailler pour lui;

– pour le contrôle des accès aux renseignements nécessaires à l'accomplissement des tâches qui lui sont dévolues;

– pour la recherche d'informations relatives à des événements survenus à l'étranger ayant une incidence sur la sûreté de la République fédérale d'Allemagne ou sur ses affaires étrangères, pour autant que ces informations ne puissent être obtenues que de cette manière et qu'aucune autre autorité ne soit compétente pour l'acquisition de ces informations.

Le *BND* peut demander cas par cas des informations sur des données auprès de prestataires de la poste, des télécommunications, de compagnies aériennes et d'établissements financiers, dans la mesure il en a besoin pour accomplir ses tâches. En outre, il peut appliquer ou engager des méthodes et utiliser des objets et des instruments pour acquérir secrètement des informations (par

ex. personnes de confiance ou informateurs, observations, enregistrements d'images et de sons, identités d'emprunt, couvertures).

En matière de surveillance de la poste et des télécommunications, le *BfV* et le *BND* sont assujettis à la loi sur la restriction du secret épistolaire, postal et des télécommunications, qui impose d'obtenir l'aval du contrôle parlementaire ou de la Commission G-10 pour les mesures lourdes de conséquences.

Ces deux services n'ont aucun pouvoir de police et ne sont pas habilités à donner des instructions.

Surveillance

BfV et BND:

– L'organe de **contrôle parlementaire** (*parlamentarisches Kontrollgremium*) a le droit de consulter les dossiers et les fichiers des services de renseignement pour exercer son contrôle. Il est également en droit d'auditionner des collaborateurs de ces services et de faire des visites au sein de ces services. Dans certains cas, il peut faire appel à des experts. Par ailleurs, le gouvernement fédéral est tenu de renseigner cet organe de surveillance sur les activités déployées par les services de renseignement, à moins que les conditions légales permettant de refuser l'information soient remplies, par exemple pour des raisons impératives de protection des sources. L'organe de surveillance participe également à des décisions liées aux mesures dans le domaine de la surveillance stratégique.

– Les **Commissions parlementaires d'enquête** (*parlamentarische Untersuchungsausschüsse*) peuvent être mandatées pour élucider de sérieux incidents ressortissant du domaine du renseignement si au moins un quart des députés du Bundestag soutiennent une telle demande. Même si cet instrument n'est pas destiné à un contrôle permanent, les services publics ont l'obligation de présenter tous leurs dossiers et les représentants du gouvernement ainsi que les collaborateurs des services de renseignement ont l'obligation de témoigner.

– Les services de renseignement sont également contrôlés en vertu de la loi sur la restriction du secret épistolaire, postal et des télécommunications. L'organe de contrôle parlementaire et la **Commission G-10** sont complémentaires pour ce qui est de ce contrôle. En outre, la Commission G-10 décide de la recevabilité et de la nécessité des mesures dans le cadre du contrôle des individus et du contrôle stratégique. Elle informe le ministère responsable du service de renseignement en question des mesures envisagées pour la surveillance stratégique de télécommunications. Elle peut également vérifier la recherche globale, le traitement et l'utilisation des données personnelles obtenues par le biais de la surveillance du trafic postal et des télécommunications. Elle a également le droit de consulter les dossiers et a accès à tous les locaux de service.

– Le **parlamentarische Vertrauensgremium** (délégation des finances du Parlement), est compétent pour le contrôle du budget des services de renseignement.

  La **Cour fédérale des comptes** (*Bundesrechnungshof*) supervise les comptes annuels, les budgets et la gestion économique.

– Le **Préposé fédéral à la protection des données et la liberté d'information** (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) contrôle la stricte observation des dispositions de la loi fédérale sur la protection des données et des autres prescriptions en matière de protection des données, tant pour le renseignement intérieur que pour le renseignement extérieur.

Protection des données

BfV et BND:

La législation en matière renseignement régit l'exploitation des services traitant des données personnelles et les droits des personnes concernées. Les dispositions applicables au *BFV* et au *BND* sont quasiment identiques.

Le *BfV* peut sauvegarder, modifier et exploiter des données personnelles si des indices concrets laissent présumer des activités menaçant l'ordre constitutionnel ou la sûreté; le *BND* peut également le faire pour autant que l'accomplissement de ses tâches l'exige. Lorsque les données sont inexactes, elles doivent être corrigées; lorsqu'elles sont irrecevables ou que le service concerné n'en a plus besoin, elles doivent être détruites. Les données font l'objet à cet égard de vérifications ponctuelles ou régulières (chez le *BfV* au bout de cinq ans, chez le *BND* au bout de dix ans).

Les données personnelles qui lèsent des intérêts dignes de protection des personnes concernées et dont les services de renseignement n'ont plus besoin pour accomplir leurs tâches doivent être bloquées.

Dans la mesure où la personne concernée peut fonder sa demande sur des faits et qu'elle a un intérêt particulier à obtenir l'information, le service concerné la renseigne gratuitement au sujet des données qui la concernent.

Dans certaines circonstances, des données personnelles peuvent être transmises à des autorités étrangères, à des services de forces armées alliées et à des services supranationaux et intergouvernementaux. Le *BND* peut obtenir, à certaines conditions, des données personnelles provenant d'autres d'autorités allemandes.

France

Direction centrale du renseignement intérieur (DCRI)

Direction générale de la sécurité extérieure (DGSE)

Le Livre blanc sur la Défense et la sécurité nationale, publié en 2008, prévoit l'élaboration d'un cadre légal pour les activités déployées par les services de renseignement français. À ce jour, ces activités ne sont cependant pour ainsi dire pas réglées par la loi.

Position dans l'architecture de la sûreté

DCRI:

La Direction centrale du renseignement intérieur est subordonnée au **Ministère de l'Intérieur**.

DGSE:

La Direction générale de la sécurité extérieure est subordonnée au **Ministère de la Défense.**

En France, le renseignement est constitué de plusieurs services complémentaires. Outre la DCRI et la DGSE, il existe six services complémentaires.

Tâches

DCRI:

– Prévenir et poursuivre les activités provoquées, engagées ou soutenues par des puissances et des organisations étrangères et menaçant la sûreté du pays.

– Participer à la prévention et à la poursuite d'actes terroristes ou d'actes menaçant l'autorité de l'État, le secret de la défense nationale ou les intérêts économiques du pays.

– Contribuer à la surveillance de communications électromagnétiques et électroniques menaçant la sûreté de l'État et lutter contre la criminalité dans les technologies de l'information et des communications.

– Participer à la surveillance de personnes, de groupes, d'organisations et de phénomènes de société menaçant la sécurité nationale par leur caractère radical, leurs convictions ou leur mode d'action.

DGSE:

– Rechercher et évaluer des informations qui sont pertinentes pour la sécurité de la France, à l'intention du gouvernement et en collaboration avec d'autres organisations.

– Déceler ou entraver les activités d'espionnage pratiquées hors du territoire national et allant à l'encontre des intérêts de la France (mesure préventive).

– Assurer dans ces cas les liaisons nécessaires avec d'autres services et organisations importants, exécuter toute mission que le gouvernement lui confie dans le cadre de ses compé-

	tences et présenter les renseignements collectés sous forme de synthèses. – Tenir particulièrement compte de la lutte contre le terrorisme et contre la prolifération d'armes de destruction massive, mais aussi du renseignement militaire et stratégique.
Compétences (engagement de moyens de renseignement)	*DCRI:* La DCRI collabore avec les gouvernements des départements et les préfectures de la police nationale. Toutefois, ses compétences ne sont pas encore réglementées par la loi. *DGSE:* La DGSE utilise toutes les méthodes de renseignement pour collecter des informations, à savoir: informateurs, exploration des télécommunications et exploration électronique, informations de sources librement accessibles et moyens opérationnels. Elle collabore avec d'autres services de renseignement français et étrangers. Les opérations secrètes sont exécutées par des agents paramilitaires. Aucune loi ne régit les méthodes et les compétences de la DGSE.
Surveillance	*DCRI et DGSE:* – **La Délégation parlementaire au renseignement** contrôle les activités et les moyens engagés. Elle reçoit des informations sur le budget, les activités générales et l'organisation des services de renseignements, mais pas sur les activités opérationnelles, les instructions du gouvernement, le financement de chaque service et l'échange d'informations avec les services de renseignements étrangers ou les organisations internationales. Les informations qui pourraient menacer l'anonymat, la sécurité ou la vie d'une personne ou qui dévoileraient les méthodes d'opération spécifiques mises en œuvre pour obtenir les informations en question ne sont pas accessibles. Le travail de la délégation parlementaire est soumis au respect du secret de la Défense nationale. Cette délégation parlementaire fait des recommandations et des observations et rédige un rapport annuel. Autres instances de contrôle: – **Commission nationale de contrôle des interceptions de sécurité**, chargée de la surveillance de l'écoute des communications domestiques. – **Commission nationale de l'informatique et des libertés**, chargée du contrôle de la protection des données. – **Commission de vérification des fonds spéciaux**, chargée de vérifier les fonds attribués aux services de renseignements.

Protection des données	*DCRI et DGSE:* La France n'a pas fixé d'exigences spécifiques en matière de protection des données pour les services de renseignement. Ceux-ci sont néanmoins assujettis aux dispositions relatives à la protection des données générales et au contrôle de la Commission nationale de l'informatique et des libertés. Cette commission contrôle le respect de la loi sur l'informatique et la manière dont les services de renseignements gèrent les données personnelles; elle consulte aussi au nom des citoyens qui en font la demande les dossiers qui les concernent (le droit d'accès aux données des services de renseignements français est indirect).

Espagne

Centro Nacional de Inteligencia (CNI)

Position dans l'architecture de la sûreté	Le *CNI* est subordonné au **Ministère de la Défense**. La direction de la communauté espagnole des services de renseignements relève de ses compétences. Le *CNI* est complété par un service de renseignement militaire et d'autres services de renseignements et d'informations de plus modeste envergure.
Tâches	– Collecter, évaluer et traiter les informations en Espagne et à l'étranger pour protéger et promouvoir les intérêts politiques, économiques, industriels, commerciaux et stratégiques. – Empêcher, découvrir et neutraliser les activités des services de renseignements étrangers, de groupes ou de personnes qui menacent ou lèsent l'ordre constitutionnel, les droits ou les libertés des citoyens espagnols, la souveraineté, l'intégrité ou la sûreté de l'État ou encore des actes qui menacent la stabilité des institutions, les intérêts économiques nationaux ou la prospérité de la population ou qui leur font courir un risque. – Promouvoir les relations et la coopération avec les services de renseignements d'autres pays et les organisations internationales. – Collecter, évaluer et interpréter les informations issues de télécommunications et les informations électroniques. – Coordonner l'activité des différents services administratifs qui utilisent des méthodes de chiffrement et veiller à garantir la sécurité des technologies d'informations dans ce domaine. Fournir du matériel de cryptologie et de formation du personnel. – Contrôler le respect des consignes en matière de protection de renseignements secrets.

	– Garantir la sécurité et la protection de ses propres installations, des informations, du matériel et du personnel.
Compétences (engagement de moyens de renseignement)	Les compétences du *CNI* ne sont que partiellement régies par la loi; l'engagement de moyens du renseignement est contrôlé par le pouvoir judiciaire. Le *CNI* accomplit ses tâches en collectant des informations tant en Espagne qu'à l'étranger. Il peut procéder à des enquêtes de sécurité sur des personnes et des entités et peut compter à cet effet sur la coopération de la part d'organismes et d'institutions publics et privés. Les moyens engagés par les services de renseignements ne sont pas clairement réglés, mais découlent néanmoins de l'autorisation de déployer des moyens qui portent atteinte à l'inviolabilité du logement privé ou à la confidentialité de la transmission des données (par ex., surveillance et mise sur écoute téléphonique). À la demande de son directeur au juge compétent de la Cour suprême, le CNI peut être autorisé à déployer de tels moyens s'ils sont nécessaires à l'accomplissement de ses tâches. Cette demande doit se faire formellement par écrit et indiquer les mesures nécessaires, les circonstances qui les justifient ainsi que les objectifs et les raisons desdites mesures. Par ailleurs, cette demande doit mentionner les personnes visées ainsi que le lieu où les mesures seront appliquées. Le juge compétent doit rendre sa décision dans un délai de 72 heures, voire de 24 heures dans les cas urgents. Le *CNI* dispose de moyens pour effectuer des enquêtes secrètes et peut obtenir à cet effet de la part des autorités compétentes les identités, immatriculations et pièces d'identité nécessaires à l'accomplissement de ses missions. Les agents du *CNI* peuvent être armés dans la mesure où le port d'une arme répond à une nécessité et pour autant que les dispositions légales le permettent. Cependant, hormis le personnel de sûreté, le service de renseignement espagnol ne dispose d'aucun pouvoir de police.
Surveillance	Le **Comité parlementaire de surveillance des fonds secrets** est compétent pour le contrôle parlementaire. Il examine les objectifs fixés par le gouvernement et le rapport annuel du directeur du *CNI* sur les activités menées et la situation par rapport aux buts fixés. Ce comité parlementaire n'a accès qu'à des informations qui ne se rapportent pas à des sources et à des ressources du CNI ou qui proviennent de services de renseignements étrangers ou d'organisations internationales. Par ailleurs, il ne peut saisir aucun document ni même en faire des copies. La mise en œuvre des moyens de renseignement est assujettie à un **contrôle judiciaire**.

Protection des données	Les textes légaux qui traitent du *CNI* ne règlent pas la protection des données ni ne renvoient à une loi nationale sur la protection des données à laquelle le service de renseignement espagnol devrait se tenir.

Pays-Bas

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
(Intelligence générale et Service de sûreté)

Position dans l'architecture de la sûreté	L'*AIVD* est subordonné au **Ministère de l'Intérieur**. Il est complété par le Service de renseignement militaire.
Tâches	– Enquêter sur des personnes et des organisations soupçonnées sur la base d'indices concrets de constituer une menace pour l'ordre juridique démocratique, la sûreté nationale ou d'autres intérêts importants des Pays-Bas. – Contrôler les candidats prétendant à des postes impliquant l'obligation de garder le secret. – Soutenir des institutions répondant de la sécurité de l'infrastructure privée et étatique qui sont vitales pour le maintien de la structure de la société néerlandaise. – Enquêter sur des pays, en accord avec les activités pour lesquelles le premier ministre, le ministre de l'Intérieur et le ministre de la Défense l'ont mandaté. – Élaborer pour le système national de sécurité des analyses de risques et de menaces auxquels sont exposés des biens immobiliers, des services et des individus.
Compétences (engagement de moyens de renseignement)	Les compétences de l'*AIVD* sont assez clairement réglées par la loi et l'engagement de moyens de renseignement est soumis à une multitude d'exigences dans la loi sur le service de renseignement et de sûreté. L'*AIVD* dispose des pouvoirs suivants pour collecter des informations: – Contacter toutes les autorités ou personnes semblant aptes à fournir les informations voulues. – Surveiller des personnes et des objets, avec ou sans déploiement de moyens techniques pour enregistrer des images ou des sons, rechercher des traces ou localiser une personne ou un objet. – Déploiement d'investigateurs secrets. – Fouiller des locaux fermés et des objets. – Ouvrir des lettres et d'autres envois de marchandises sans le consentement de l'expéditeur ou du destinataire (ces mesures

nécessitent un mandat octroyé par le Tribunal de district de La Haye).

– S'introduire dans des systèmes informatiques avec ou sans instruments techniques ou faux signes, faux mots de passe ou fausses identités.

– Mettre sur écoute téléphonique, procéder à des enregistrements ou surveiller sous n'importe quelle forme des conversations, des télécommunications ou des transferts de données au moyen d'appareils techniques.

– S'adresser à des exploitants de réseaux de télécommunication publics pour obtenir des renseignements sur un utilisateur.

Ces pouvoirs sont soumis à des exigences légales strictes et requièrent fréquemment une directive du ministre compétent ou du directeur du service de renseignement.

L'*AIVD* n'a aucun pouvoir de police et il lui est interdit de poursuivre des infractions.

Surveillance

– Un **comité de surveillance parlementaire sur les services de renseignement et services de sûreté** vérifie que les services de renseignement civil et militaire respectent les dispositions de la loi sur le service de renseignement et de sûreté.

– Tous les milieux participant au processus de renseignement sont tenus de coopérer avec le comité de surveillance. En outre, celui-ci a accès à tous les renseignements et il est habilité à interroger des témoins et des experts ainsi qu'à mener des enquêtes.

– L'**Ombudsman national** est compétent pour les plaintes déposées par la population concernant le comportement des services de renseignement et de sûreté. Il statue sur les plaintes et motive sa position, dans la mesure où la sécurité de l'État ou d'autres intérêts de l'État ne s'y opposent pas. Il informe ensuite le ministre compétent de sa décision. L'ombudsman peut aussi émettre des recommandations. Le ministre transmet ses recommandations et conclusions au Parlement néerlandais.

– **La Cour générale des comptes** supervise les dépenses de l'*AIVD* pour les opérations secrètes et présente chaque année un rapport au Parlement à cet égard.

– Les ministres responsables des services de renseignement et de sûreté informent une fois par an le Parlement au sujet des activités de l'*AIVD*.

Protection des données

L'*AIVD* ne peut utiliser ou traiter des données personnelles que dans les cas suivants:

– il existe un soupçon sérieux que la personne représente une menace pour l'ordre constitutionnel démocratique, la sécurité ou d'autres intérêts vitaux du pays;

– la personne a donné son accord pour subir un contrôle de sécurité;
– la mesure est nécessaire dans le cadre d'investigations sur d'autres pays;
– les informations ont été obtenues par un autre service de renseignement ou de sûreté;
– les données sont nécessaires au service pour accomplir ses tâches;
– la personne est ou était employée dans le service;
– les données sont nécessaires à l'élaboration d'analyses de risques.

Les données personnelles qui ne sont plus pertinentes pour le but pour lequel elles ont été collectées doivent être supprimées. Les informations qui se révèlent inexactes sont corrigées et celles qui ont été traitées de manière illégale sont supprimées.

Les ministres, d'autres personnes et autorités pertinentes, les services de renseignement et de sûreté pertinents d'autres pays et les organisations pertinentes de sécurité, de télécommunication et de renseignement peuvent prendre connaissance des informations traitées par l'*AIVD*.

Lorsqu'une personne demande à consulter ses données personnelles, le ministre compétent est tenu de l'informer dans les meilleurs délais et de lui communiquer quelles données personnelles ont été traitées ou pour quel service elles l'ont été. La personne concernée a ensuite le droit de consulter ces données.

Autriche

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)
(Office fédéral de la protection de la constitution et de lutte contre le terrorisme)

Heeresnachrichtenamt (HNaA)
(Service de renseignement de l'armée)

Position dans l'architecture de la sûreté

BVT:

Le Service de renseignement intérieur fait partie intégrante de la police de sûreté et est subordonné à ce titre à la Direction générale pour la sécurité publique au sein du **Ministère fédéral de l'Intérieur**.

Le *BVT* est soutenu par neuf services de protection de la constitution et de lutte contre le terrorisme des Länder.

HNaA:

Le Service de renseignement de l'armée est le service de renseignement stratégique sur l'étranger. Il est subordonné au chef de

	l'État-major général au sein du **Ministère fédéral de la Défense et des Sports**. Il n'existe qu'un autre service de renseignement, à savoir le Service de la Défense, qui a pour fonction le renseignement militaire.
Tâches	*BVT:* – Rechercher des informations, investiguer et effectuer des analyses dans les domaines du terrorisme, de l'extrémisme, du contre-espionnage, du trafic d'armes et de la prolifération d'armes nucléaires, chimiques ou biologiques. – Protéger des personnes et des objets pour une personne morale gestionnaire d'installations de droit constitutionnel. – Protéger des représentants d'États étrangers, des organisations internationales et d'autres objets de droit international. – Protéger des infrastructures critiques. – Effectuer des contrôles de sécurité. *HNaA:* Recherche de renseignements: rechercher, traiter, évaluer et présenter des informations sur l'étranger ou sur des organisations internationales ou d'autres organismes internationaux en rapport avec des faits, événements et projets militaires ou liés à ceux-ci
Compétences (engagement de de renseignement)	Le déploiement de moyens de renseignement est clairement réglementé dans la loi pour les deux services. *BVT:* Le *BVT* obtient ses informations en exploitant l'outil informatique OSINT et des sources qui ne sont pas librement accessibles. Dans ce cadre (recherche élargie de menaces), le *BVT* a les pouvoirs suivants: – observer des groupements si le contexte et le développement de la situation font peser une sérieuse menace sur la sécurité publique et font craindre des actes criminels, en particulier des actes de violence fondés sur des motifs religieux ou idéologiques; – utiliser secrètement des appareils d'identification des plaques minéralogiques de véhicules et utiliser sans dissimulation des appareils d'enregistrement d'images et de sons dans les foyers de criminalité; – utiliser secrètement des appareils d'enregistrement d'images et de sons et transmettre des enregistrements d'images et de sons privés à des services de sûreté, à certaines conditions; – procéder à des observations et déployer des investigateurs secrets.

Selon l'ampleur des moyens engagés, le préposé à la protection des droits, rattaché au Ministère fédéral de l'Intérieur, doit être informé ou doit donner son aval.

Le *BVT* est un service de police. Comme il fait partie de la police de sûreté, il détient des pouvoirs de police conformément à la loi autrichienne sur la police de sûreté.

HNaA:

Selon la loi sur les pouvoirs militaires, le *HNaA* a les pouvoirs suivants pour rechercher des renseignements:

– rechercher des informations auprès de personnes, d'organes de collectivités régionales et de collectivités de droit public, auprès de fondations desdites collectivités, auprès d'institutions, établissements et fonds et auprès d'exploitants de services de télécommunication publics;

– rechercher des données par l'observation si ces données sont indispensables à l'accomplissement de ses tâches ou qu'y renoncer entraverait considérablement leur accomplissement;

– procéder à des investigations secrètes, s'il est urgent et nécessaire de mettre en œuvre cette mesure dans l'intérêt de la sécurité nationale, en particulier pour garantir la capacité d'intervention de l'armée autrichienne, et que, sans cette mesure, le service ne pourrait pas accomplir sa mission.

– rechercher des données en utilisant des appareils d'enregistrement d'images et de sons lorsque cette mesure est dans l'intérêt de la sûreté nationale, en particulier pour garantir la capacité d'intervention de l'armée autrichienne, et que, sans cette mesure, le service ne pourrait accomplir qu'une petite partie de sa mission.

Avant de rechercher des données par l'observation, par une investigation secrète ou par le déploiement d'appareils d'enregistrement d'images et de sons, le *HNaA* doit informer le préposé à la protection des droits pour qu'il puisse vérifier la légitimité des mesures et lui indiquer les raisons principales qui justifiant une telle investigation. Le *HNaA* est également tenu d'informer le ministre fédéral de la défense nationale. La recherche ne peut être mise en œuvre qu'avec l'aval du préposé. Si toutefois le moindre délai devait causer un dommage grave et irréparable à la sécurité nationale, en particulier à la capacité d'intervention de l'armée autrichienne ou à la sécurité de personnes, l'investigation peut être mise en œuvre dès que le préposé en a été informé, à moins qu'il ne s'y oppose et fasse suspendre l'intervention.

Surveillance

BVT:

– Contrôle dans le cadre du droit d'interpellation parlementaire.

– Contrôle par la **Sous-commission permanente de la Commission des affaires intérieures chargée d'examiner les me-**

sures de protection des institutions de droit constitutionnel et de leur capacité d'action (*Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Massnahmen zum Schutz der verfassungsmässigen Einrichtungen und ihrer Handlungsfähigkeit)*. Cette sous-commission est compétente pour contrôler que le *BVT* accomplisse ses tâches conformément à la loi. Elle a le droit de demander des informations au ministre fédéral de l'Intérieur et de consulter les dossiers.

– Contrôle essentiellement administratif par la **Cour des comptes** et par le **Collège des médiateurs** (*Volksanwaltschaft*).

– Contrôle par le **préposé à la protection des droits auprès du Ministère fédéral de l'Intérieur**. Dans le cadre des pouvoirs spéciaux conférés au *BVT*, l'implication de ce préposé va, selon l'ampleur de l'intervention, de la simple prise de connaissance à un aval aux mesures envisagées. Par ailleurs, le préposé rédige chaque année un rapport d'activités.

– Contrôle par le **Conseil des droits de l'homme** (*Menschenrechtsbeirat***)**. Chargé de conseiller le ministre fédéral de l'Intérieur pour les questions liées à la sauvegarde des droits de l'homme, ce conseil exerce aussi à ce titre une surveillance sur le *BVT*. Ce dernier est tenu de l'épauler dans ses activités; en outre, le ministre fédéral met à sa disposition les moyens nécessaires à l'accomplissement de ses tâches.

HNaA:

– Contrôle dans le cadre du droit d'interpellation parlementaire.

– Contrôle par la **Sous-commission permanente de la Commission de la défense nationale chargée de superviser les mesures de renseignement pour assurer la défense nationale militaire** *(Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Massnahmen zur Sicherung der militärischen Landesverteidigung).* Cette sous-commission peut demander au *HNaA* toutes les informations et documents pertinentes pour ses activités de surveillance. Pour des raisons de protection des sources, elle n'est cependant pas habilitée à demander la production d'informations ou de documents – en particulier sur les sources – dont la révélation pourrait mettre en danger la sûreté nationale ou la sécurité de personnes.

– Contrôle par le *Préposé à la protection des droits chargé de vérifier la légitimité de mesures d'investigations en matière de renseignement ou de défense* (*Rechtsschutzbeauftragter zur Prüfung der Rechtmässigkeit von Massnahmen der nachrichtendienstlichen Aufklärung oder Abwehr*). Ce préposé est compétent pour autoriser et contrôler le déploiement des moyens de renseignement. Il peut consulter en tout temps l'ensemble des

documents et enregistrements nécessaires; le *HNaA* est tenu de lui fournir toutes les informations qu'il demande. Cependant, le préposé n'a pas accès aux informations et aux documents concernant l'identité de personnes ou de sources dont la révélation pourrait menacer la sûreté nationale ou la sécurité de personnes. Le *HNaA* doit lui permettre d'exécuter en tout temps la surveillance de mesures et de pénétrer dans tous les locaux où sont conservés les enregistrements d'images et de sons ou d'autres résultats de surveillances. Le préposé vérifie en outre que le *HNaA* a bien respecté son obligation de rectifier des données erronées ou de les supprimer en vertu des dispositions de la loi sur la protection des données. Il rédige une fois par année un rapport d'activités.

BVT et HNaA:

Contrôle par la **Commission chargée de la protection des données**. La loi sur la protection des données charge cette commission de la protection juridique de personnes physiques en cas de soupçon d'infraction au droit à la protection des données. Cette commission statue sur plainte en cas de de violation présumée du droit à être informé, de l'obligation de garder le secret et du droit à la rectification ou à la suppression des données.

Protection des données

BVT:

La loi sur la police de sûreté régit le traitement des données personnelles et règle les droits des personnes concernées.

Les services de renseignements peuvent saisir des données personnelles et les exploiter pour autant qu'elles soient indispensables à l'accomplissement de leurs tâches. Ils peuvent également demander ces données aux exploitants de services de télécommunication publics ou à d'autres prestataires de service.

Les données inexactes, les données saisies de manière erronée ou celles dont le service de renseignement n'a plus besoin doivent être rectifiées ou supprimées. Les données personnelles traitées doivent être vérifiées si elles n'ont subi aucune modification depuis six ans.

Toute personne a le droit d'obtenir gratuitement des informations sur les données personnelles qui ont été collectées à son sujet. Néanmoins, le *BVT* n'est pas tenu de lui fournir des informations lorsque la protection de la personne requérant l'information est menacée ou lorsque des intérêts prépondérants du mandant ou d'un tiers ou des intérêts publics prépondérants (par ex., la protection d'institutions de droit constitutionnel) s'y opposent.

HNaA:

La loi sur les pouvoirs militaires ne prévoit aucune disposition particulière en matière de protection des données, mais elle renvoie à la loi sur la protection des données.

Le droit d'accès correspond à celui prévu pour le *BVT*.

	Belgique *Sûreté de l'État (SE)* *Service général du renseignement et de la sécurité des Forces armées (SGRS)* En Belgique, le *SE* est un service de renseignement civil, tandis que le *SGRS* est un service de renseignement militaire. Les deux services sont compétents tant pour la Belgique que pour l'étranger, même si le *SE* se focalise essentiellement sur la Belgique et le SGRS sur l'étranger.
Position dans l'architecture de la sûreté	*SE:* Le service de renseignement civil est subordonné au m**inistre de la Justice**, mais le **ministre de l'Intérieur** est également compétent pour les questions de sûreté publique et de protection des personnes. *SGRS:* Le Service de renseignements militaire est subordonné au **ministre de la Défense**. Le service des douanes et la police s'occupent aussi de collecter des renseignements, mais ils ne constituent pas des services de renseignements proprement dits et ne sont donc pas assujettis aux dispositions légales en la matière. Les services de renseignements coopèrent entre eux et avec des services de renseignements étrangers. Ils peuvent soutenir les autorités judiciaires et administratives.
Tâches	*SE:* – Rechercher, analyser et traiter des informations sur les activités menaçant ou susceptibles de menacer la sûreté intérieure de l'État, la pérennité de l'ordre démocratique ou constitutionnel, la sécurité extérieure, les relations internationales, le potentiel scientifique ou économique ou tout autre intérêt fondamental du pays (espionnage, terrorisme, extrémisme, prolifération d'armes de destruction massive, organisations sectaires nuisibles ou organisations criminelles, ingérence). – Procéder à des contrôles de sécurité – Protéger des personnes – Accomplir d'autres tâches prévues par la loi.
	SGRS: – Rechercher, analyser et traiter des informations sur des activités menaçant ou susceptibles de menacer l'intégrité du territoire national, les plans de défense militaires, l'exécution des

tâches des forces armées, la sécurité des citoyens belges ou d'autres intérêts fondamentaux du pays; informer les ministres compétents.

– Conseiller le gouvernement en matière de politique extérieure et de défense.

– Veiller au maintien de la sécurité militaire du personnel du Ministère de la Défense, des installations militaires, des armes, des plans, des systèmes informatiques, de la communication et d'autres objets militaires.

– Protéger le secret défense

– Procéder à des contrôles de sécurité.

Compétences (engagement de de renseignement)

Des dispositions légales régissent clairement le déploiement de moyens de renseignement par les deux services.

SE/SGRS:

Aux termes des dispositions légales, les services de renseignements peuvent rechercher, collecter, obtenir et traiter des informations personnelles pour autant qu'elles soient nécessaires à l'accomplissement de leurs tâches. Ils peuvent avoir recours à cet égard aux services des autorités judiciaires, aux fonctionnaires et employés du service public et à toute personne ou organisation du secteur privé pour obtenir des informations; les services de renseignement peuvent également pénétrer dans des lieux et des locaux accessibles au public, faire des descentes dans des hôtels et autres logement et utiliser des informateurs.

Si ces méthodes habituelles ne suffisent pas, les services de renseignements peuvent utiliser des méthodes dites spécifiques ou exceptionnelles pour rechercher des informations.

Méthodes spécifiques:

– Procéder à des observations avec des moyens techniques dans les espaces et locaux publics ou privés accessibles au public ou procéder à des observations, avec ou sans moyens techniques, d'espaces privés non accessibles au public.

– Contrôler des espaces et locaux publics ou privés accessibles au public et contrôler par des moyens techniques les objets qui y sont enfermés.

– Identifier l'expéditeur ou le destinataire d'un envoi postal ou le détenteur d'une case postale.

– Identifier l'abonné ou l'utilisateur usuel d'un service de communication électronique ou du moyen de communication électronique utilisé.

– Localiser les données d'appel de moyens de communication électroniques et localiser l'origine ou la destination de communications électroniques.

Le service de renseignement qui entend engager ces méthodes doit informer au préalable par la voie de son directeur la commission administrative compétente, voire obtenir son autorisation.

Méthodes exceptionnelles:

- Observer et surveiller les espaces privés non accessibles au public
- Créer et utiliser une personne morale en vue de soutenir des activités opérationnelles et avoir recours à des agents du service de renseignement
- Ouvrir le courrier et en prendre connaissance
- Collecter des données sur des comptes et transactions bancaires
- S'introduire dans un système informatique
- Mettre des personnes sur écoute et enregistrer des communications.

Ces méthodes ne peuvent être mises en œuvre qu'avec l'autorisation de la commission administrative compétente.

Les services de renseignement peuvent soutenir les autorités judiciaires, mais ils n'ont eux-mêmes aucun pouvoir de police (tout au moins la loi ne s'exprime-t-elle aucunement à ce sujet).

Surveillance

SE/SGRS:

- **Comité permanent des services de renseignement et de sûreté** (organe de contrôle parlementaire): exerce la haute surveillance sur les services de renseignement et peut mener des enquêtes (il a le droit de consulter les dossiers, de convoquer des personnes et de procéder à des perquisitions et à des séquestres).
- **Commission administrative**: surveille l'application des méthodes de renseignement spécifiques et exceptionnelles
- **Ombudsman fédéral**: compétent pour les plaintes déposées par des particuliers, peut mener des enquêtes et consulter les dossiers. Les services de renseignement ne sont toutefois pas tenus de lui transmettre des informations secrètes.
- **Commission de la protection des données**: examine, à la demande des citoyens, les informations personnelles détenues par les services de renseignement; elle ne peut toutefois émettre que des recommandations et ne doit pas divulguer le contenu des dossiers.

Protection des données

SE/SGRS:

Le *SE* et le *SGRS* sont soumis aux mêmes dispositions légales. La législation en matière de renseignement régit le traitement des données personnelles et les droits des personnes concernées.

Les informations et données personnelles peuvent être cherchées, collectées, reçues et traitées. Elles peuvent aussi être transmises à certaines personnes, autorités et services de police ou à toute autre instance compétente, à condition que ces personnes ou services fassent l'objet d'une menace ou que ces données leur soient utiles dans l'accomplissement de leurs tâches. Les données ne peuvent être conservées qu'aussi longtemps que nécessaires pour atteindre l'objectif pour lequel elles ont été saisies, à l'exception des données que les Archives d'État jugent historiquement importantes. La destruction des données n'intervient qu'au terme d'un délai au cours duquel les données n'ont connu aucun traitement; ce délai est fixé par le roi ou la reine.

Les citoyens n'ont pas le droit de consulter des dossiers contenant des données personnelles qui les concernent; ils doivent s'adresser à la Commission de protection des données.

1.6 Mise en œuvre

Les mesures proposées peuvent être mises en œuvre presque totalement dans le cadre des structures fédérales (SRC, Tribunal administratif fédéral, Service chargé de la surveillance de la correspondance par poste et télécommunication, représentations suisses à l'étranger, etc.) et cantonales (autorités cantonales de police et de sûreté).

2 Commentaires des dispositions

Remarque préliminaire concernant le terme de menace

Selon la définition du Conseil fédéral figurant dans le rapport sur la politique de sécurité, «la menace présuppose une volonté de nuire à la Suisse ou à ses intérêts ou tout au moins le fait d'accepter la perspective d'un tel préjudice.» En revanche, le «danger» ne suppose pas de volonté de provoquer des dommages (par ex. dangers naturels et techniques)[14].

Le projet de loi utilise à dessein le terme de menace pour marquer clairement la différence par rapport aux dangers naturels, même si certains développements de politique de sécurité faisant partie du domaine d'activité du SRC ne sont pas ou pas encore dirigés contre la Suisse ou constituent un facteur propre à empêcher ou à détourner une menace.

Préambule

Conformément à la pratique actuelle, le préambule ne mentionne pas la compétence constitutionnelle inhérente de la Confédération pour le maintien de la sûreté intérieure ou extérieure. Selon la doctrine actuelle, cette compétence lui est donnée par l'art. 173, al. 2, Cst. («L'Assemblée fédérale traite en outre tous les objets qui relè-

14 FF **2010** 4681 4694

vent de la compétence de la Confédération et qui ne ressortissent pas à une autre autorité fédérale»).

De cette compétence découle, entre autres, le pouvoir (partiel) de la Confédération de légiférer sur les tâches des cantons, respectivement des autorités d'exécution cantonales dans le domaine de la sûreté intérieure. On se référera à cet égard aux commentaires relatifs aux art. 9 (Autorités d'exécution cantonales) et 81 (Exécution par les cantons).

Art. 1 Objet

Cet article résume la teneur de la loi.

Art. 2 But

L'importance du présent projet de codification globale pour le renseignement suisse justifie la présence d'un article qui précise le but de la loi.

L'art. 2 reprend des éléments de la LMSI. Il définit les objectifs sur lesquels les activités du renseignement doivent se concentrer et fait office à ce titre de ligne directrice pour l'exécution de la loi, sans toutefois fixer de compétences.

Art. 3 Missions dans des situations particulières

La LRens régit la sauvegarde des intérêts essentiels de la Suisse dans le domaine de la politique de sécurité. L'art. 3 permet au Conseil fédéral lors de situations particulières de charger le SRC de rechercher et d'analyser des informations et, le cas échéant, de déployer des activités opérationnelles allant au-delà de son mandat légal ordinaire. Conformément à l'art. 70, une décision spéciale du Conseil fédéral est requise à cet effet: la mission de base définie par le Conseil fédéral (art. 69, al. 1, let. a) ou la liste d'observation fixée par le Conseil fédéral (art. 71) ne suffisent pas pour de telles missions. Le SRC n'est donc pas autorisé à prendre de son propre chef ou sur la base des instruments de conduite ordinaires (mission de base ou liste d'observation) des mesures supplémentaires de sauvegarde d'intérêts essentiels de la Suisse au sens de l'art. 3. La décision du Conseil fédéral ne donne pas non plus au SRC de compétences particulières allant au-delà de celles qui lui sont conférées par la loi. Les activités de recherche d'informations sont donc soumises aux dispositions légales, en particulier pour la mise en œuvre des mesures soumises à autorisation (art. 25 ss): celles-ci doivent être demandées par la la procédure ordinaire et doivent être justifiées. Dans sa décision, le Conseil fédéral peut, par contre, fixer des conditions aux activités du SRC, en limitant par exemple à l'étranger l'activité de recherche ou en excluant certaines mesures de recherche, comme celles soumises à autorisation.

Lorsque d'autres intérêts essentiels de la Suisse au sens de l'art. 3 sont invoqués pour des missions non incluses dans le mandat ordinaire du SRC, il s'agit en règle générale de recherches d'informations à l'étranger. Ces autres intérêts essentiels doivent ressortir des compétences constitutionnelles de la Confédération. On peut aussi envisager qu'un canton ou que plusieurs cantons demandent une intervention du SRC en vue de sauvegarder d'autres intérêts essentiels de la Suisse qui relèvent en priorité de la compétence constitutionnelle des cantons, mais qui représentent un intérêt national lorsqu'ils sont menacés. Le projet de loi mentionne comme autres intérêts essentiels de la Suisse la protection de l'ordre constitutionnel (dans la me-

sure où le mandat du SRC défini à l'art. 6 est insuffisant), le soutien à la politique extérieure (par ex. en cas de crise liée à la politique extérieure, de négociations délicates ou de pressions diplomatiques) et la protection de la place industrielle, économique et financière (par ex. lors de pressions motivées par des intérêts économiques contre des secteurs économiques spécifiques d'importance nationale).

Si une telle intervention exige des ressources particulières en termes de personnel et de finances, le Conseil fédéral doit les attribuer au SRC dans la même décision, la souveraineté des Chambres fédérales en matière de budget n'étant à cet égard nullement entamée.

L'art. 3 ne limite pas la compétence du Conseil fédéral d'édicter des ordonnances se fondant sur les art. 184, al. 3, et 185, al. 3, Cst. (voir aussi les art. 7*a* à 7*d* de la loi sur l'organisation du gouvernement et de l'administration[15]).

Art. 5 Principes applicables à la recherche d'informations

La tâche principale du SRC est de rechercher et d'analyser des informations, de les transmettre sous forme de produits du renseignement aux ayants droit et de mettre à profit ses connaissances pour mener des opérations de prévention permettant de réduire les menaces pour la sûreté de la Suisse. C'est pourquoi l'art. 5 définit des principes régissant la recherche d'informations qui s'appliquent à toutes les autres dispositions de la loi. Ces principes doivent être appliqués par le SRC en tant qu'autorité d'exécution de la Confédération, de même que par les autorités cantonales chargées de l'exécution de la LRens ou agissant sur mandat du SRC.

Certains alinéas sont réglés plus en détail dans d'autres dispositions de la loi.

L'*al. 1* précise que le SRC est habilité à rechercher des informations dans des sources accessibles au public et des sources non accessibles au public. Il importe à cet égard de bien connaître les sources réputées publiques (voir art. 13) afin de pouvoir déterminer quelles informations doivent être recherchées confirmées ou infirmées à l'aide de moyens du renseignement.

L'*al. 2* renvoie au système des mesures de recherche soumises à autorisation et non soumises à autorisation présenté en détail au chap. 3. Les mesures qui ne sont pas soumises à autorisation (art. 13 ss) sont utilisées par le SRC sous sa propre responsabilité (par ex. l'observation dans des lieux publics). Elles correspondent en grande partie au catalogue des mesures fixées à l'art. 14, al. 2, LMSI.

Les mesures de recherche soumises à autorisation (art. 25 ss) ne peuvent être mises en œuvre que dans les cas prévus par la loi. Elles doivent être autorisées par le Tribunal administratif fédéral, puis avalisées par le chef du DDPS.

L'*al. 3* précise le principe de la proportionnalité pour les activités du SRC: l'idée maîtresse est de s'assurer que l'ingérence nécessaire dans les droits fondamentaux est en adéquation avec le but de la recherche d'informations. À cet effet, le SRC doit toujours opter pour la mesure qui, selon toute vraisemblance, sera la moins intrusive pour les droits fondamentaux de la personne concernée. Lorsqu'il est possible d'obtenir l'information avec une mesure non soumise à autorisation, la préférence sera donnée à une telle mesure.

15 RS **172.010**

L'*al. 4* est nécessaire pour déroger au principe général de protection des données prévoyant que la collecte des données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée (art. 4, al. 4, LPD). L'al. 4 correspond aux art. 5, al. 1, LFRC et 14, al. 1, LMSI. Le but du traitement des données ne peut généralement pas être atteint si la personne concernée sait qu'elles sont collectées et traitées. Elle dispose en revanche d'un droit d'accès aux données, qui est réglé aux art. 62 ss.

Les *al. 5 à 8* reprennent en substance les principes éprouvés de la LMSI qui interdisent la surveillance des activités politiques à des fins de renseignement; ils en reprennent aussi les exceptions. Lors de la consultation sur le présent projet, quelques participants ont demandé des dispositions plus strictes à ce sujet. Le Conseil fédéral considère toutefois que le système actuel, mis à jour en 2001, est approprié. La LRens maintient ce système et garantit ainsi la même protection que la LMSI pour le traitement à des fins de renseignement d'événements se déroulant en Suisse. Concernant l'étranger, une telle réserve ne serait pas judicieuse car elle empêcherait pratiquement l'observation et l'appréciation de l'évolution des rapports de force politiques.

Les exemples suivants illustrent l'exercice abusif des droits fondamentaux au sens de l'al. 6 pour exercer des activités mettant en danger la sécurité:

– Une association religieuse dispose d'un local de réunion pour ses membres. Une personne se rend régulièrement dans ce local et tente de convaincre les membres de l'association de se joindre à la lutte religieuse armée à l'étranger ou de participer, à l'étranger, à un entraînement pour la lutte armée. La recherche et le traitement d'informations portent alors sur cette personne, et non sur les membres de l'association en général.
– Un groupe de personnes d'une minorité ethnique qui mène dans son pays d'origine une lutte armée contre le gouvernement dispose en Suisse d'un local à des fins essentiellement culturelles. Une soirée folklorique avec la participation de musiciens se révèle être une cérémonie de commémoration des martyrs avec des orateurs qui prônent la lutte armée et qui récoltent des fonds à cet effet.

Les *al. 6 et 7* correspondent aux dispositions détaillées de l'art. 3 LMSI, entrées en vigueur en 2012. Lorsque des données doivent être effacées, le SRC a l'obligation de les proposer aux Archives fédérales. Les données sans valeur archivistique sont définitivement détruites.

L'*al. 8* précise que le SRC peut rechercher et traiter des informations sur des organisations et des groupements inscrits sur la liste d'observation visée à l'art. 71 lorsqu'elles lui permettent d'apprécier la menace. Cette règle, dont l'application comportait quelques ambiguïtés, était jusqu'à présent contenue dans les dispositions de la LMSI régissant la liste d'observation. Son nouvel emplacement lève ces ambiguïtés.

Chapitre 2, section 1

Le SRC contribue en priorité à la sécurité de la Suisse par des activités préventives, mais il peut aussi recourir à ses moyens spéciaux pour soutenir d'autres services de la Confédération dans l'accomplissement de leurs tâches (voir art. 68).

Les activités préventives du SRC doivent être clairement distinguées des activités répressives des autorités de poursuite pénale. Le but premier du SRC est de déceler à temps les menaces qui pèsent sur la sûreté intérieure ou extérieure de la Suisse et d'en faire rapport aux autorités compétentes afin d'en minimiser les risques. Le SRC n'assure pas de tâches de police ou de procédure pénale (par ex. enquêtes, arrestations, etc.): les activités du SRC et des autorités de poursuite pénale sont complémentaires, mais les unes ne sont pas le préliminaire des autres, raison pour laquelle leur surveillance relève de domaines différents (le SRC par les instances politiques, les autorités de poursuite pénale par les tribunaux). L'échange d'informations entre le SRC et les autorités de poursuite doit de ce fait obéir à des règles précises.

Art. 6 Tâches du SRC

La loi ne cite à l'*al. 1* que le SRC comme autorité d'exécution, mais les domaines d'activité définis à la let. a concernent aussi l'exécution par les cantons (voir art. 81). Les domaines de compétences fixés dans la LMSI sont complétés par la mention explicite d'attaques contre des infrastructures d'informa-tion, qui ont acquis une nouvelle importance compte tenu des développements techniques survenus depuis l'entrée en vigueur de la LMSI. Si de telles attaques se produisent par exemple en lien avec l'espionnage ou le terrorisme, elles relèvent, comme à présent, des tâches définies aux ch. 1 et 2. Toutefois, un tel lien ne se révélant souvent qu'à la suite d'investigations approfondies, il est nécessaire que le SRC puisse y participer dès le début afin d'assumer son rôle dans le cadre de la stratégie de défense cybernétique de la Confédération. Les réseaux des infrastructures d'information critiques doivent être protégés contre les attaques informatiques. Le SRC doit donc continuer à rechercher les informations nécessaires sur les menaces d'attaques ou les attaques qui se sont produites pour les services compétents et les soutenir ainsi dans leurs activités de défense contre ces attaques. A cet effet, le SRC dispose aussi de contacts exclusifs au niveau international.

La notion d'infrastructures critiques se fonde sur la terminologie du domaine de la protection de la population. Elle doit être comprise au sens large et inclut par exemple les infrastructures d'importantes organisations internationales installées dans notre pays.

La notion d'événements importants en matière de politique de sécurité se produisant à l'étranger (*let. b*) se réfère aux événements et développements à l'étranger susceptibles de menacer l'autodétermination de la Suisse, son ordre démocratique et sa situation d'État de droit, de lui infliger de graves dommages en matière de politique de sécurité ou autres ou d'entraver la capacité d'action de ses autorités. Dans de tels cas, le SRC fournit principalement des prestations pour le Département fédéral des affaires étrangères (DFAE) sous forme de rapports d'analyse ou d'informations spécifiques.

La *let. c* souligne qu'une des tâches essentielles du SRC est de fournir à temps au gouvernement les informations nécessaires pour accomplir ses tâches. «Assurer la capacité d'action de la Suisse» a de ce fait été inclue explicitement dans le catalogue des tâches du SRC.

La notion de sauvegarde des intérêts essentiels de la Suisse est également nouvelle (voir les commentaires relatifs à l'art. 3).

Notons que le présent article se borne à énumérer les tâches du SRC et les objectifs qu'elles visent: les compétences concrètes du SRC sont réglées plus en avant dans la loi.

Ainsi, la recherche et le traitement de données visant à apprécier la menace au sens de l'*al. 2* est réglée en détail dans les chap. 3 et 4. Le SRC ne donne l'alerte qu'en fonction des tâches qui lui sont confiées par la loi. D'autres types d'alerte relèvent de la compétence d'autres services (par ex. la Centrale nationale d'alarme de l'Office fédéral de la protection de la population en cas de catastrophe naturelle).

Lors d'événements particulièrement importants du point de vue de la sécurité (par ex., l'édition annuelle du Forum économique mondial ou de grandes conférences internationales telles que le Sommet de la francophonie), le SRC met sur pied un réseau national de renseignement, pour assurer les tâches définies aux al. 2 et 3. Ce dernier coordonne la recherche et la diffusion d'informations et permet aux services compétents habilités à participer à ce réseau de suivre en permanence l'évolution de la situation par le biais du système de présentation électronique de la situation (voir art. 52).

L'information d'autres services de la Confédération et des cantons au sens de l'*al. 3* est précisée plus en détail aux art. 58 ss, qui règlent la transmission de données, en particulier personnelles.

La fonction du SRC en tant d'autorité responsable des contacts en matière de renseignement avec l'étranger, réglée aujourd'hui à l'art. 8 LMSI, figure à l'*al. 4*. Cette compétence permet d'éviter les doublons et les contradictions dans les échanges avec des services de renseignement étrangers et des autorités de sûreté étrangères. Elle est décrite plus en détail à l'art. 12.

L'*al. 5* est consacré aux tâches préventives relevant de l'unité opérationnelle de renseignement de la Centrale d'enregistrement et d'analyse de la sûreté de l'information (MELANI), qui est intégrée au SRC. Cette dernière procède déjà à l'alerte précoce d'un cercle défini d'exploitants d'infrastructures critiques. Cette tâche importante va au-delà d'un simple traitement d'informations au sens de l'al. 1, let. a, ch. 4, raison pour laquelle elle est expressément réglée ici.

L'*al. 7* revêt une importance particulière pour la sécurité du SRC, de ses collaborateurs et des données qu'il traite. L'art. 7 contient des règles plus précises à ce sujet. La Confédération élabore parallèlement au présent projet une base légale régissant la sécurité des informations et des objets. Le cas échéant, cette dernière réglera certains besoins spécifiques du SRC sous une forme générale pour l'ensemble de l'administration fédérale. Pour l'instant, cependant, c'est la LRens qui doit garantir que le SRC assure une protection suffisante.

Le SRC peut également fournir des prestations de soutien dans le cadre de l'assistance administrative, mais cela ne fait pas partie de ses tâches principales et fait l'objet de règles séparées (art. 68).

Art. 7 Mesures de protection et de sécurité

Les mesures de protection et de sécurité réglées ici complètent les arrêtés fédéraux concernant la sécurité intégrale, notamment dans les domaines de la protection et de la sécurité des collaborateurs, des informations et des installations. Elles sont destinées à l'application des prescriptions relatives au secret de fonction et augmentent

de ce fait la sécurité et la crédibilité du SRC pour le traitement de données classifiées.

Pour garantir la sécurité, les mesures de formation et de sensibilisation ont priorité sur d'autres mesures. La prise de mesures d'ordre technique et de contrôle du respect des prescriptions font néanmoins aussi partie d'une gestion efficace et crédible des risques.

Let. a: les fouilles de personnes et de leurs effets personnels sont uniquement effectuées pour des raisons de sécurité et conformément au principe de la proportionnalité. Le SRC peut charger des tiers d'effectuer ces contrôles. La mesure est destinée à la protection des biens de l'employeur et au respect des prescriptions relatives à la protection des informations classifiées. Elle concerne les collaborateurs du SRC et le personnel engagé temporairement au SRC, tels que des stagiaires. Les collaborateurs des entreprises qui fournissent des prestations dans les locaux du SRC ou qui y effectuent des travaux de maintenance peuvent également être contrôlés. Les membres des organes de surveillance et les visiteurs, qui sont accompagnés en permanence lorsqu'ils se trouvent dans les locaux du SRC, ne font pas l'objet de contrôles.

Let. c: les systèmes de vidéosurveillance ne sont pas destinés à observer en permanence le comportement de personnes. Ils sont utilisés sur les parkings, les zones d'accès et les couloirs des bâtiments du SRC, les chambres fortes, les locaux d'archivage de données classifiéesou devant être particulièrement protégées ainsi que dans les entrepôts de biens de valeur.

Let. d: les locaux dans lesquels ont lieu des discussions portant sur des sujets très sensibles, confidentiels ou secrets sont si possible équipés de systèmes de protection passive (bouclier d'assourdissement et isolation acoustique) qui empêchent les informations de parvenir à l'extérieur, par exemple via des téléphones mobiles. Dans les locaux où cela s'avère impossible, des installations de télécommunication perturbatrices peuvent temporairement être engagées pour empêcher toute communication par téléphone mobile, en veillant à ce que d'autres intérêts publics ou des intérêts de tiers ne soient pas entravés de façon disproportionnée. Afin de ne pas perturber le trafic des télécommunications de tiers, l'utilisation d'émetteurs de brouillage est limitée aux locaux où ont lieu les entretiens et à la durée des discussions sur des sujets considérés comme sensibles ou classifiés secrets. Les installations de brouillage doivent être autorisées et être conformes aux prescriptions de l'Office fédéral de la communication.

L'*al. 2* constitue la base légale pour le réseau informatique hautement sécurisé que le SRC exploite déjà pour la majorité de ses applications informatiques et systèmes d'information. Le SRC traite beaucoup de données particulièrement sensibles et classifiées, raison pour laquelle la sécurité des informations revêt une importance particulière. L'accès au réseau est réservé au personnel du SRC, aux organes de surveillance des services de renseignement et à un tout petit nombre de personnes relevant du Service de renseignement militaire, qui ne dispose pas encore de réseau similaire hautement sécurisé.

Art. 8 Port d'armes

Les collaborateurs chargés de rechercher des informations dans le domaine du terrorisme, de l'espionnage, de l'extrémisme violent, du trafic d'armes ou du com-

merce illégal d'armes chimiques, biologiques ou nucléaires de destruction massive évoluent dans des milieux en partie dangereux et violents, par exemple lors de la prise ou le suivi de contacts avec des informateurs. Les collaborateurs du SRC qui ont des activités dans ces domaines en Suisse doivent être armés pour pouvoir se protéger et protéger leurs informateurs ou un tiers lorsqu'un danger immédiat menace leur vie ou leur intégrité corporelle. Dans les cas mentionnés, les activités des collaborateurs qui recherchent des informations en Suisse sont comparables à celles des agents de police qui ont recours aux services de personnes de confiance.

L'arme ne peut être utilisée qu'en cas de légitime défense (art. 15*f* du code pénal[16]) ou en état de nécessité (art. 17 du code pénal). L'usage de l'arme à feu doit en particulier respecter le principe de la proportionnalité (al. 2).

Cette disposition correspond largement à l'art. 5*a* LMSI. En plus des dispositions d'exécution du Conseil fédéral, le SRC réglera dans des directives, comme aujourd'hui, les modalités du port d'une arme de service (entre autres, justification d'une formation suffisante et de l'autorisation de porter une arme et entraînements obligatoires au tir).

Art. 9 Autorités d'exécution cantonales

Le projet prévoit que les tâches de renseignement soient exécutées en commun par la Confédération et les cantons (voir art. 81). Les autorités d'exécution cantonales recherchent sur leur territoire les informations qu'elles doivent se procurer directement en vertu de la LRens ou sur mandat spécifique du SRC. À cet effet, comme jusqu'à présent, les cantons désigneront un service spécialisé pour accomplir ces tâches. En règle générale, ce service fait partie du corps de police.

D'autres prescriptions concernant les cantons se trouvent aux chap. 4 (traitement des données) et 5 (contrôle et surveillance).

Art. 10 Information des cantons

La nouvelle loi doit aussi accorder toute son importance à l'étroite collaboration entre la Confédération et les cantons. La Confédération est chargée comme aujourd'hui d'informer les autorités cantonales compétentes des événements particuliers survenant dans le domaine d'activités du SRC et de l'état de la menace. Cette information se fait en particulier dans le cadre de la Conférence des commandants des polices cantonales de Suisse et de la Conférence des directeurs des départements cantonaux de justice et police. En outre, le SRC est en contact permanent avec les autorités d'exécution cantonales, ce qui permet d'assurer que ces dernières puissent accomplir leurs tâches sur le territoire cantonal conformément aux besoins de la Confédération. L'art. 45, al. 3, règle au surplus l'utilisation au sein des cantons des appréciations de la situation et des autres données transmises par le SRC

Art. 11 Collaboration avec l'armée

La collaboration du SRC avec les unités du Service de renseignement de l'armée (SRA), essentiellement avec le Service de renseignement militaire, et les organes

16 RS **311.0**

assurant le service de sécurité militaire, doit être maintenue telle qu'elle existe depuis la création du SRC.

Ces deux services travaillent dans des domaines thématiques apparentés pour l'appréciation de la menace et de la sécurité selon les besoins de l'armée. L'art. 11 règle l'obligation du SRC d'informer les services compétents de l'armée d'événements susceptibles d'avoir une incidence sur l'exécution de leurs tâches. L'obligation de ces services d'informer le SRC est réglée aux art. 19 (Obligation de fournir des renseignements en cas de menace concrète) et 20 (Obligation spécifique de fournir et de communiquer des renseignements). Les modalités de la collaboration seront fixées dans l'ordonnance d'exécution (en principe, selon le modèle actuel).

L'*al. 2* doit permettre au SRC de continuer de charger dans certains cas les attachés de défense de l'armée de rechercher des informations et d'assurer le suivi des contacts avec des services de renseignement étrangers et des autorités de sûreté étrangères. La recherche d'informations se fait toujours en accord avec l'ordre juridique du pays hôte, c'est-à-dire par les contacts officiels avec les autorités du pays hôte ou le réseau des relations diplomatiques. Les attachés de défense ne sont pas des espions en uniforme, mais des officiers de liaison du SRC annoncés auprès des services de renseignement concernés des États où ils sont accrédités. Cette manière de procéder a donné d'excellents résultats, par exemple, lors d'enlèvements ou de l'observation des développements du printemps arabe. La collaboration et la répartition des tâches continue à se faire en accord avec le domaine Relations internationales de l'armée.

Art. 12 Collaboration avec l'étranger

Notons tout d'abord que le Conseil fédéral a explicitement renoncé à mentionner dans la LRens le principe selon lequel les cantons peuvent collaborer avec les autorités étrangères compétentes pour les questions de sûreté dans les régions frontalières (voir art. 8, al. 2, LMSI), puisqu'il découle de l'art. 56, al. 3, Cst. L'exécution par les cantons telle qu'établie sur la base de la LMSI ne connaît donc aucun changement.

Concernant l'*al. 1*, relevons que dans le domaine du renseignement, la Suisse n'est pas liée par des traités de droit international, mais qu'elle conclut tout au plus des arrangements (*agreements*), ou, le cas échéant, des déclarations d'intention (*Memorandums of Understanding*), qui ne sont pas contraignants. La raison de cette pratique est que les services de renseignement servent en priorité les intérêts nationaux de leur pays. Là où ces intérêts se recoupent avec ceux d'autres pays, une collaboration peut s'établir. Le SRC collabore ainsi avec des services de renseignement et des autorités de sûreté d'un grand nombre de pays, par exemple dans les domaines de la défense contre le terrorisme, l'espionnage, l'extrémisme violent ou pour des questions militaires ou relatives aux rapports de force politiques. Cependant, les États veulent rester libres d'adapter leurs intérêts en matière de renseignement à leurs besoins, sans être liés par des traités. La Suisse ne fait pas exception.

La transmission de données personnelles à des autorités étrangères est réglée en détail à l'art. 60.

Cette pratique pourrait connaître une exception à l'avenir, en relation avec l'exploitation de systèmes internationaux d'information automatisés (let. e). De tels systèmes sont aujourd'hui de plus en plus demandés par les services de renseigne-

ment européens, mais ils n'ont pas encore pu être complètement réalisés car les bases légales nationales nécessaires pour des systèmes communs font encore défaut dans la plupart des États et il n'existe pas non plus d'accords internationaux à ce sujet. Le Conseil fédéral propose de fixer dans la LRens que le SRC peut participer à des systèmes d'informations automatisées. Cette forme particulière de collaboration internationale devrait, pour des raisons de protection des données, être réglée dans le cadre d'un accord technique. La compétence pour la conclusion d'un tel accord relèverait du Conseil fédéral (art. 69, al. 3).

L'*al. 2* autorise le SRC à détacher des collaborateurs de liaison dans les représentations suisses à l'étranger, de façon analogue aux attachés de migration, de défense et de police, si cela s'avère nécessaire pour la collaboration internationale. L'engagement de telles personnes n'interviendra qu'en accord avec le DFAE. Les collaborateurs du SRC seront en mission officielle: ils seront annoncés conformément aux règles établies auprès des services compétents du pays d'accueil et des éventuels États tiers lors d'accréditations collatérales et travailleront exclusivement comme agents officiels de liaison avec les services compétents. Leur mission n'est pas de collecter secrètement des informations, aussi ne violeront-ils pas le droit des États hôtes. Compte tenu des frais considérables liés à un tel engagement, le Conseil fédéral part du principe que seul un petit nombre d'agents de liaison du SRC seront appelés à remplir une telle mission et après une période d'organisation assez longue. Ces agents combleraient le cas échéant des lacunes dans le dispositif des attachés de défense et pourraient le compléter là où ces derniers ne peuvent remplir les fonctions requises. Les besoins financiers et les besoins en personnel seront assurés par le budget ordinaire.

L'*al. 3* vise à garantir que les contacts que la Suisse entretient avec d'autres pays dans le domaine du renseignement soient menés exclusivement en conformité avec les dispositions de la LRens. Le même principe figure sous une forme similaire à l'art. 8 LMSI et il est précisé aux art. 11, al. 1 et 2, de l'ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération (OSRC)[17]. Le SRC assumera cependant uniquement la responsabilité des contacts avec des services de renseignement au sens strict et avec d'autres autorités étrangères en matière de renseignement, particulièrement dans les contacts avec des autorités étrangères qui assument plusieurs fonctions (par ex. police judiciaire et service de renseignement intérieur): les contacts en matière policière (police judiciaire) restent de la compétence des autorités suisses de police.

Conformément à l'art. 69, le Conseil fédéral assume au surplus des tâches spéciales dans le domaine de la collaboration avec l'étranger et peut, à ce titre, édicter d'autres règlementations par voie d'ordonnance.

Chapitre 3

La notion de traitement des données au sens de la LPD inclut certes la recherche (ou collecte selon la terminologie de la LPD) de ces données (voir art. 3, let. e, LPD). Cependant, comme la recherche de données est d'une importance primordiale pour un service de renseignement et que, du point de vue de la personne concernée, elle peut entraîner de graves atteintes aux droits fondamentaux, les règles concernant la

17 RS **121.1**

recherche et les autres formes de traitement des données font l'objet de chapitres spécifiques dans le projet de loi.

Les dispositions du chap. 3 ne citent que le SRC comme service de recherche d'informations. Elles s'appliquent cependant également aux autorités d'exécution cantonales dans le cadre de leurs mandats d'exécution (art. 9 et 81).

Quelques participants à la consultation ont critiqué un manque de coordination entre les mesures de recherche d'informations de la LRens et le code de procédure pénale[18]. Le présent projet de loi ne doit cependant régler que le domaine du renseignement, et non celui de la procédure pénale (unité de la matière). Une nouvelle loi se doit de prendre en compte les développements des techniques (par ex. en ce qui concerne les mesures de recherche d'informations dans les systèmes et réseaux informatiques). Par ailleurs, le service de renseignement accomplit une tâche autonome: elle ne constitue pas une étape préliminaire à une poursuite pénale ni une forme moins rigoureuse de celle-ci. En revanche, les mesures de recherche soumises à autorisation prennent en compte que la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) est actuellement en cours de révision. Pour faciliter la coordination avec cette révision et pour clarifier que la LRens ne doit pas permettre de mettre en œuvre des mesures supplémentaires ou d'autres mesures, la LRens renvoie à la LSCPT.

Le souhait de certains cantons de disposer des mêmes compétences que le SRC n'a que partiellement été satisfait. Ils en disposeront pour les mesures de recherche non soumises à autorisation, mais les mesures de recherche soumises à autorisation relèveront de la compétence exclusive de la Confédération. Si un canton estime avoir besoin de compétences propres dans ce domaine, il doit légiférer à l'échelon cantonal.

Chapitre 3, section 1

Cette section comporte les mesures de recherche d'informations que le SRC peut mettre en œuvre de son propre chef et sans autorisation externe particulière étant donné que l'atteinte aux droits fondamentaux est relativement faible. Elles correspondent largement aux possibilités de recherche énumérées à l'art. 14, al. 2, LMSI. Le chapitre 3 contient tous les moyens classiques de recherche d'informations d'un service de renseignement, allant de l'observation dans des lieux publics et des lieux librement accessibles («renseignement de sources ouvertes», autrement dit les sources d'informations publiques, art. 13) à l'exploration des télécommunications et l'exploration radio («renseignement d'origine électromagnétique», art. 27 et 37 ss) en passant par les enregistrements visuels et sonores («renseignement d'origine image», art. 14, al. 2) et les informateurs («renseignement d'origine humaine», art. 15). La loi fixe des règles particulières pour l'utilisation de ces mesures selon la gravité de l'atteinte aux droits fondamentaux.

Quelques participants à la consultation ont suggéré de régler aussi dans la LRens l'accès aux données des réseaux sociaux, car celles-ci peuvent être d'un grand intérêt pour un service de renseignement. Le Conseil fédéral renonce à une telle réglementation parce que la notion de «réseaux sociaux» est trop imprécise et qu'elle pourrait être utilisée pour un volume de données incalculable. Il faut s'en tenir à des règles générales: tant qu'il s'agit de données rendues publiques, les règles

18 RS **312.0**

correspondantes sont applicables; en revanche, pour les mesures de recherche dans le domaine protégé par le secret des communications, le SRC doit obtenir une autorisation judiciaire et une autorisation politique conformément aux art. 25 ss.

Selon l'art. 81, al. 1, les cantons peuvent mettre en œuvre de manière autonome la plupart des mesures de recherche non soumises à autorisation lorsqu'ils agissent en exécution de la LRens.

Art. 13 Sources d'informations publiques

Un service de renseignement collecte beaucoup d'informations dans les sources d'informations publiques. Il n'a alors plus qu'à combler les lacunes de manière ciblée avec les moyens spécifiques du renseignement ou à vérifier ou infirmer les informations publiques à l'aide de ces moyens.

Ce type de recherche porte le moins atteinte aux droits fondamentaux puisque les informations concernées sont publiques, donc pratiquement accessibles à tout un chacun. Le fait que certaines informations ne soient proposées par des particuliers que contre paiement ne change en rien leur caractère public. Les recueils de données électroniques accessibles contre paiement ne doivent ainsi pas être traités différemment que les médias classiques, tels que des journaux ou des publications spécialisées, qui sont en règle générale aussi proposés contre paiement.

Par rapport au projet mis en consultation, la disposition concernant les informations contenues dans les registres publics des autorités a été déplacée dans cet article puisque leur recherche correspond plutôt à un accès à des sources d'informations publiques qu'à une obligation faite à l'autorité qui gère le registre de fournir des renseignements.

La qualité des informations accessibles au public peut être très diverse, raison pour laquelle leur utilisation demande une appréciation soigneuse. Le projet de loi prévoit à cette fin que le SRC enregistre les informations de sources publiques dans un système séparé (art. 53). Elles peuvent ensuite être évaluées en cas de besoin et transférées dans d'autres systèmes si elles sont utilisées pour des produits du renseignement.

Art. 14 Observation dans des lieux publics et dans des lieux librement accessibles

L'*al. 1* reprend les règles de l'art. 14, al. 2, let. f, LMSI. L'observation et la documentation d'événements se déroulant dans des lieux publics et dans des lieux librement accessibles au public fait partie des tâches standards d'un service de renseignement. Les rencontres entre officiers traitants de services de renseignements étrangers et leurs informateurs se déroulent souvent dans des lieux publics, par exemple des gares, des aéroports ou des places publiques. Certaines zones de restaurants et d'hôtels font également partie des lieux publics et librement accessibles au public.

Un exemple concret: l'officier d'un service de renseignement étranger séjournant à Genève sous couverture diplomatique allait souvent chercher son informateur dans le centre-ville avec son véhicule. Il essayait ainsi de donner l'impression de n'être qu'un diplomate ordinaire.

Pour documenter de telles rencontres, en particulier à l'aide d'enregistrements visuels et sonores, une observation de ces lieux publics ou librement accessibles au public est indispensable.

La disposition règle plus en détail les renseignements obtenus à l'aide des enregistrements visuels et sonores. Pour réaliser les tâches prévues par la loi, il peut être nécessaire, dans certains cas, de faire appel à des moyens aériens adéquats, tels que des avions, des hélicoptères ou des drones, c'est-à-dire de petits appareils de reconnaissance aérienne sans pilote et télécommandés à partir du sol. Des moyens spatiaux, par exemple des satellites, peuvent également être appropriés pour l'exploration d'images (par ex. en cas d'enlèvement de citoyens suisses à l'étranger). Des photos satellite permettent par exemple d'observer l'avancée de programmes étrangers d'armes de destruction massive. Le SRC ne dispose pas lui-même de tels moyens, mais il peut en demander l'engagement auprès de tiers. Le Service de renseignement militaire dispose d'un centre d'imagerie qui permet de rechercher et d'évaluer ce type d'informations. Les photos satellite sont essentiellement fournies par des entreprises commerciales, la Suisse ne disposant pas non plus de ses propres instruments dans ce domaine.

Ces observations sont indispensables pour une évaluation indépendante et autonome d'événements pertinents pour la politique de sécurité. Grâce à ses appréciations de la situation, le SRC soutient directement la politique étrangère de la Suisse, par exemple en fournissant au DFAE des pronostics sur le temps dont il dispose pour négocier avec un État pratiquant la prolifération d'armes de destruction massive.

Les événements au sol ne font pas partie de l'espace public lorsqu'ils se déroulent par exemple dans un appartement ou sur un terrain privé. S'il est nécessaire d'observer de tels événements de manière ciblée, le SRC doit faire une demande de mesure soumise à autorisation (art. 25 ss). S'il n'est pas possible d'éviter une observation de l'espace privé (par ex. en prenant des mesures techniques ou en limitant de la résolution de l'image de manière à ne plus pouvoir reconnaître des détails relevant de la sphère privée), les données collectées doivent être détruites. La situation est comparable à celle d'un avion de ligne survolant une zone habitée: on ne peut empêcher que des passagers observent ou photographient par les hublots des événements qui se déroulent au sol dans l'espace privé. L'utilisation de telles images pourrait toutefois être attaquée en justice.

Le Conseil fédéral estime que cette volonté claire de protéger la sphère privée protégée assure que les droits fondamentaux seront suffisamment protégés, tout en laissant la possibilité au SRC d'accéder à des moyens de surveillance qui, en raison des progrès techniques, deviennent en partie des biens collectifs.

Une règle analogue est inscrite pour le domaine militaire dans la loi du 3 février 1995 sur l'armée[19] (art. 99, al. 1^{quater}, voir modification d'autres actes).

Art. 15 Informateurs

Le terme «informateurs» utilisé dans le projet de loi est repris de l'art. 14*a* de la LMSI. Il se réfère à des personnes qui ont un accès exclusif à des informations et qui, de leur propre chef ou à la demande du SRC, sont disposées à les communiquer au SRC.

19 RS **510.10**

Lorsque par exemple un groupe terroriste en Suisse ou à l'étranger planifie des attentats en Suisse contre des citoyens ou contre des intérêts suisses à l'étranger, ces informations ne peuvent souvent être obtenues que par des personnes qui ont un accès direct ou indirect à ce groupe. Pour des raisons de sécurité, en effet, les plans et les activités du groupe ne font que très rarement l'objet de documents ou d'échanges écrits et ne sont transmis que de vive voix à un cercle restreint du groupe.

Des informateurs, en particulier à l'étranger, peuvent parfois fournir des informations au SRC sans le savoir. Le fait qu'ils n'en aient pas conscience peut servir à leur propre protection.

Selon l'*al. 2,* des indemnités peuvent être versées après entente aux informateurs au titre de remboursement de dépenses ou au titre de paiement d'informations déterminantes pour l'accomplissement des tâches confiées au SRC. Les informateurs résidant à l'étranger, en particulier, demandent souvent de l'argent pour communiquer leurs informations. L'ébruitement de l'indemnisation peut représenter un risque important pour les informateurs, tant dans leur pays d'origine que pour leur entourage. Un informateur qui est soupçonné de toucher des revenus provenant d'activités ou de relations liées au renseignement peut subir un préjudice professionnel, voir sa réputation ruinée et, selon le pays et la situation, risquer sa vie ou son intégrité corporelle. Pour toutes ces raisons, les indemnités versées aux informateurs ne peuvent dans la plupart des cas ni être déclarées ni être imposées ou assujetties aux assurances sociales. Sans cette règle, la sécurité de nombreux informateurs ne pourrait être garantie, ce qui rendrait impossible toute collaboration avec eux. Ce n'est que dans certains cas particuliers que des revenus peuvent être officialisés par le biais de structures de couverture, par exemple lorsqu'un informateur assurerait pour ainsi dire exclusivement ses revenus par les indemnités que lui verse le SRC et qu'il ne disposerait pas, de ce fait, d'une couverture sociale suffisante. Pour la Suisse, de tels cas seraient toutefois extrêmement rares.

Al. 3 à 5

En raison des informations dont il dispose et qu'il communique au SRC, un informateur peut courir un risque pour son intégrité corporelle ou pour sa vie, notamment s'il donne des informations sur des cellules terroristes ou des groupements extrémistes violents de l'étranger mais aussi dans les domaines où opèrent des organisations et des services de renseignement étatiques. Les informateurs étrangers qui travaillent pour le SRC peuvent ainsi courir un danger très important dans leur pays d'origine. Leur découverte peut signifier une condamnation à mort, pour eux ou pour leurs proches:

- des scientifiques de pays asiatiques, en particulier les spécialistes du nucléaire, qui communiquent des informations à un service de renseignement étranger peuvent être condamnés à mort dans leur pays;
- pendant les troubles du printemps arabe, le SRC a constaté à partir de plusieurs sources que des opposants vivant en Suisse faisaient régulièrement l'objet d'une surveillance ou de molestations de la part de fidèles au régime en provenance de leurs pays. La découverte d'une éventuelle collaboration avec le SRC d'informateurs appartenant à l'entourage de ces opposants pourrait mettre en danger non seulement l'intégrité corporelle et la vie des informateurs eux-mêmes, mais aussi celles de leurs proches dans le pays d'origine.

Le SRC a l'obligation de protéger au mieux l'intégrité corporelle de ses informateurs. Il veille ainsi en permanence à leur assurer une protection maximale. Les mesures qui peuvent être prises afin d'assurer cette protection comportent aussi, exceptionnellement, l'octroi de permis de séjour en Suisse pour un informateur et les membres de sa famille ou la constitution d'une couverture ou d'une identité d'emprunt. Le SRC peut également doter ses informateurs en activité d'une identité d'emprunt conformément à l'art. 18 si leur protection le requiert.

Le risque pour l'intégrité corporelle et la vie d'un informateur peut persister au terme de son activité pour le SRC. Dans ce cas, la loi prévoit également la possibilité de le doter d'une couverture ou d'une identité d'emprunt. Comme il s'agit d'une mesure à plus long terme, le délai de douze mois, avec réexamen régulier, fixé pour les informateurs en activité n'est pas applicable: cette mesure est mise en œuvre aussi longtemps que le danger persiste pour l'informateur voire pour ses proches. Comme le SRC n'a alors en règle générale plus de contacts réguliers avec l'informateur, il revient au chef du DDPS d'autoriser la constitution d'une couverture ou d'une identité d'emprunt pour que les risques politiques puissent être évalués.

Les organes de surveillance du SRC (art. 74 ss) ont accès à toutes les informations concernant le recours à des informateurs. Selon la pratique établie, ils reçoivent chaque année un rapport détaillé sur toutes les opérations de ce type et peuvent consulter les dossiers qu'ils désirent.

Art. 16 Signalements pour la recherche de personnes et d'objets

Les *al. 1 et 2* introduisent une réglementation similaire à celle que prévoyait le projet de loi sur les tâches de police de la Confédération (chap. 3: Mesures visant à prévenir les infractions), mis en suspens par le Conseil fédéral. Le présent projet n'est cependant pas axé sur la prévention d'infractions, mais sur la recherche d'informations pour lutter contre les menaces pour la sûreté intérieure et extérieure de la Suisse et la sauvegarde d'autres intérêts essentiels de notre pays au sens de l'art. 3. En vertu de l'al. 2, le signalement de personnes et de véhicules par le SRC doit donc impérativement se fonder sur une menace concrète pour la sûreté intérieure et extérieure ou sur une décision du Conseil fédéral pour la sauvegarde d'autres intérêts essentiels de la Suisse (voir l'art. 3 en relation avec l'art. 70). Seule une des conditions énoncées à l'al. 2 doit être remplie à cet égard.

Le présent projet fixe ainsi dans la loi la possibilité de pouvoir déterminer, comme aujourd'hui, le lieu de séjour et les mouvements de personnes ciblées (par ex. de membres de groupements soupçonnés de terrorisme) par leur signalement ou celle de leur véhicule dans le Système de recherches informatisées de la police (RIPOL). La législation en matière de police parle dans ce cas de «surveillance discrète». À l'avenir, un tel signalement doit aussi pouvoir figurer dans la partie nationale du Système d'information Schengen (N-SIS). Ainsi, lorsque des personnes signalées par le SRC entrent dans un pays membre de Schengen, le quittent ou sont contrôlées à l'intérieur de cet espace par la police ou par les organes chargés des contrôles à la frontière, la Suisse, ou plus précisément le SRC, en sera informée par les autorités étrangères compétentes. La communication est transmise par l'intermédiaire du bureau suisse de SIRENE (point de contact pour la collaboration SIS entre autorités compétentes des États Schengen; voir art. 8 et 9 de l'ordonnance du 8 mars 2013 sur

la partie nationale du Système d'information Schengen et sur le bureau SIRENE[20]). Il faudra naturellement examiner à chaque fois si un signalement est nécessaire et judicieux. Un signalement dans RIPOL ne donnera ainsi pas automatiquement lieu à un signalement dans le système Schengen.

L'exception fixée à l'*al. 3* pour les signalements dans RIPOL ou dans le N-SIS ne concerne que des véhicules de tiers soumis au secret professionnel et correspond à la pratique actuelle. Il s'agit des groupes de personnes qui ont le droit de refuser de témoigner (par ex. ecclésiastiques, avocats, personnes tenues d'observer le secret professionnel et professionnels des médias).

Les cantons peuvent aussi procéder à de tels signalements pour leurs propres domaines d'intérêts dans le cadre de la législation en matière de police.

Chapitre 3, section 2

Le Service du renseignement stratégique (SRS) disposait depuis 1997, sur la base de l'art. 99 de la loi sur l'armée, de la possibilité de doter ses agents d'identités d'emprunt (voir le rapport annuel 2002/2003 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales du 23 janvier 2004[21]). Depuis le regroupement du SAP et du SRS et la création du SRC qui en a découlé, l'art. 16, al. 1, let. e, OSRC, prévoit expressément l'utilisation de papiers d'identité fictifs et d'assertions trompeuses (couvertures) pour la recherche d'informations à l'étranger. Depuis 1997, des identités d'emprunt et des couvertures sont utilisées comme mesures permanentes de protection par les collaborateurs chargés de rechercher des informations à l'étranger. Les identités d'emprunt sont autorisées à l'interne par le SRC, qui est soumis à cet égard à la surveillance du chef du DDPS, de la Délégation du Conseil fédéral pour la sécurité et de la Délégation des Commissions de gestion des Chambres fédérales.

L'adoption par le Parlement de la révision du 23 décembre 2011 de la LMSI a donné au SRC la possibilité d'utiliser également des identités d'emprunt et des couvertures pour rechercher des informations en Suisse (art. 14*c*). À la différence du processus d'autorisation interne au SRC pour la recherche d'informations à l'étranger, l'octroi d'identités d'emprunt pour des personnes chargées de tâches relevant de la LMSI doit être demandé au chef du DDPS. De plus, l'art. 14*c*, al. 1, let. c, LMSI, permet de constituer également des identités d'emprunt pour les informateurs du SRC dans le cadre d'une mission spécifique de recherche d'informations.

Les art. 17 et 18 du projet de loi font clairement la distinction entre la notion de couverture et celle d'identité d'emprunt, car il s'agit de mesures différentes qui peuvent être prises indépendamment l'une de l'autre.

Le présent projet regroupe les différentes réglementations régissant les identités d'emprunt pour la recherche d'informations en Suisse et à l'étranger. En outre, l'objectif de protection permanente des personnes qui bénéficient de ces mesures est renforcé. Compte tenu des nouvelles règles introduites dans la LMSI, le Conseil fédéral propose de confier au chef du DDPS la compétence d'octroyer des identités d'emprunt, tant pour les activités en Suisse que pour celles à l'étranger.

20 RS **362.0**
21 FF **2004** 1594

La compétence de constituer de simples couvertures est attribuée au directeur du SRC, puisqu'elles ne nécessitent pas de pièces d'identité comportant de faux noms et qu'elles ne permettent pas d'effectuer des actes juridiques sous un faux nom.

Art. 17 Couverture

Une couverture permet de dissimuler l'appartenance d'une personne au SRC en indiquant par exemple un autre nom d'employeur et une autre activité professionnelle. La personne garde toutefois son vrai nom et d'autres données biographiques (date de naissance, lieu de naissance, etc.). Une couverture peut être nécessaire à une activité de renseignement, par exemple parce que les personnes auprès desquelles des informations doivent être recherchées ou leur entourage ne veulent pas avoir de contacts avec le SRC ou parce qu'un lien apparent avec ce dernier pourrait représenter un danger pour la personne en question (ce qui pourrait par ex. être considéré comme de l'espionnage dans certains États et y être sévèrement puni).

Un collaborateur du SRC ne saurait se rendre à l'étranger pour une mission secrète de recherche d'informations en étant clairement identifiable comme un collaborateur du renseignement. Les collaborateurs concernés et les informateurs avec lesquels ils sont en contact pourraient en effet être dévoilés et donc menacés. Les collaborateurs du SRC et leurs informateurs peuvent également être menacés en Suisse, notamment dans le contexte du terrorisme ou de l'espionnage, lorsqu'un lien entre eux et le SRC est identifiable.

En raison des progrès de la biométrie, il est de plus en plus difficile de se rendre à l'étranger sous une fausse identité. Afin de garantir la poursuite des activités de renseignement à l'étranger, il est donc nécessaire de pouvoir dissimuler avec une couverture la véritable identité des personnes concernées.

La constitution de couvertures est souvent une mesure à long terme et elle n'est pas liée à certaines opérations en particulier. Selon la protection requise, le temps nécessaire à leur constitution peut être assez court (par ex. achat d'un téléphone prépayé et impression de cartes de visite fictives) ou assez long (par ex. trouver ou créer un employeur fictif, garantir que la personne est atteignable par téléphone, par courriel, etc.). Les titres établis sont des écrits ou des supports de données ou d'images «destinés et propres à prouver un fait ayant une portée juridique» (voir art. 110, al. 4, CP). L'utilisation de couvertures correspond à la pratique actuelle de la recherche d'informations à l'étranger, qui repose sur l'art. 16, al. 1, let. e, OSRC. Le présent article lui donne une base légale claire. Si la constitution de couvertures implique le soutien d'autorités suisses, ces dernières seront tenues de collaborer, notamment si des documents officiels s'avèrent nécessaires pour assurer la crédibilité de la couverture (par ex. pour rendre crédible une activité commerciale).

À la demande des cantons lors de la procédure de consultation, le nouvel *al. 2* précise que la SRC ne peut pas doter de couvertures les collaborateurs de services cantonaux de sécurité sans l'accord des autorités cantonales auxquelles ils sont subordonnés.

Aucun titre n'est nécessaire pour passer sous silence ou dissimuler avec des données générales mais véridiques l'appartenance d'une personne au SRC (par ex. employé de la Confédération, collaborateur du DDPS, juriste). L'*al. 5* précise que ces cas ne requièrent pas l'autorisation du directeur du SRC.

La surveillance permanente de ces mesures est assurée par l'obligation de présenter chaque année un rapport au chef du DDPS sur le recours à des couvertures (*al. 4*).

Art. 18 Identité d'emprunt

Une identité d'emprunt donne une autre identité à une personne, c'est-à-dire un autre nom et, le cas échéant, d'autres données biographiques (date de naissance, lieu de naissance, etc.). Elle est dès lors soumise à des conditions beaucoup plus strictes que l'utilisation de couvertures. Comme ces dernières, les identités d'emprunt peuvent dissimuler le lien avec le SRC, par exemple indiquer un autre employeur. Lorsqu'un collaborateur du SRC doit être protégé en tant que personne, et non en raison de son activité pour le SRC, une identité d'emprunt peut lui être attribuée sans couverture.

Pour pouvoir remplir leurs tâches et protéger leurs collaborateurs lorsqu'ils recherchent des informations à l'étranger et dans certains milieux en Suisse, les services de renseignement ont besoin de recourir à des identités d'emprunt et aux couvertures qui s'y rapportent. Pouvoir remonter à la véritable identité des collaborateurs qui procèdent à des recherches d'informations, par exemple dans le domaine du terrorisme ou de l'espionnage, peuvent les exposer, ainsi que les membres de leurs familles, à des tentatives de pression, à des menaces voire à des risques concrets pour leur intégrité corporelle. Les identités d'emprunt sont de ce fait en premier lieu une mesure de protection permanente pour le personnel chargé de rechercher des informations.

Outre leur finalité de protection, les identités d'emprunt peuvent parfois s'avérer nécessaires pour amorcer et entretenir des contacts avec des personnes et des structures à des fins de recherche d'informations. Dans les domaines du terrorisme ou de l'espionnage ou lors d'une mission de recherche à l'étranger, tout lien du collaborateur avec le SRC peut d'emblée rendre impossible toute tentative de collecter des informations.

La constitution d'identités d'emprunt nécessite une longue préparation et ne peut que rarement débuter avec le traitement d'un cas spécifique. Selon son importance, la mise au point d'une identité d'emprunt peut demander des travaux préparatoires de plusieurs années pour qu'elle soit crédible.

L'*al. 1* crée la base nécessaire pour doter des personnes d'identités d'emprunt afin de garantir leur sécurité ou la recherche d'informations. Le cercle des personnes qui peuvent être munies d'identités d'emprunt est énuméré de manière exhaustive à l'al. 1.

Comme la constitution d'identités d'emprunt est un processus qui demande beaucoup de temps et qu'il s'agit d'une mesure permanente de protection, leur attribution à des collaborateurs du renseignement chargés de rechercher des informations est une tâche fondamentale du SRC. Cette mesure doit être autorisée par le chef du DDPS puisqu'elle implique de faux papiers. Cette autorisation, délivrée par le département, garantit la surveillance. Dans ce cas aussi, la Délégation des Commissions de gestion des Chambres fédérales aura accès à toutes les informations et dossiers qu'elle désire (voir l'art. 77).

L'utilisation des identités d'emprunt est limitée dans le temps et peut au besoin être prolongée (cf. al. 2). Elle est soumise à des critères bien précis, qui doivent dans tous les cas être respectés (cf. al. 3).

La constitution d'une identité d'emprunt comporte aussi le droit d'exécuter des actes juridiques sous cette identité, notamment de créer des structures qui dissimulent le lien avec le SRC. Contrairement aux couvertures, qui utilisent la véritable identité (art. 17), la mise au point de ces structures demande souvent un effort beaucoup plus conséquent avec des identités d'emprunt, puisqu'elles doivent être liées à une identité fictive, à un employeur plausible, à un domicile fictif, etc., pour être crédibles. Les personnes dotées d'une identité d'emprunt bénéficient d'une pleine personnalité juridique et peuvent conclure des contrats (par ex. location de locaux et de véhicules, raccordements de télécommunication, création de structures telles que des entreprises ou autres personnes morales comme base pour une identité d'emprunt et la couverture s'y rapportant).

Selon l'*al. 2*, l'utilisation d'identités d'emprunt est limitée dans le temps et doit être réexaminée après un certain délai. Ces conditions garantissent que les identités d'emprunt ne sont utilisées qu'aussi longtemps que nécessaires pour garantir la sécurité des collaborateurs et de leurs informateurs. Une limitation absolue n'est toutefois pas indiquée. En effet, un officier traitant, par exemple, doit toujours se présenter à ses informateurs sous la même identité. Une identité d'emprunt ne peut donc échoir à la fin d'une durée maximale: son utilisation doit s'adapter aux besoins du service.

Afin de préserver la flexibilité nécessaire et de mieux contrôler les risques inhérents à leur utilisation par des informateurs, les identités d'emprunt qui leur sont attribuées sont limitées à douze mois.

L'*al. 3* fixe les critères pour l'utilisation d'identités d'emprunt à des fins de recherche d'informations. Ceux-ci se fondent sur les principes de la proportionnalité et de la subsidiarité.

L'*al. 4* permet l'établissement des pièces d'identité et d'autres documents nécessaires à la constitution d'une identité d'emprunt: le SRC est tributaire à cet égard de la collaboration des autorités compétentes en la matière, qui sont tenues de coopérer. Le principal objectif d'une identité d'emprunt est de protéger les personnes qui sont particulièrement en danger en leur attribuant une autre identité pour la durée d'un tel danger. Ce n'est d'ailleurs qu'exceptionnellement et avec beaucoup de retenue que des papiers d'identité suisses seront mis à la disposition d'étrangers. Dans ces cas, l'attribution temporaire de papiers suisses ne leur accorde bien évidemment pas durablement la nationalité suisse.

Art. 19 Obligation de fournir des renseignements en cas de menace concrète

Pour accomplir les tâches qui lui sont confiées, le SRC est tributaire d'informations fournies par des tiers (autorités de la Confédération et des cantons, organisations chargés de tâches publiques). Ces informations peuvent être communiquées au SRC à sa demande ou lui être communiquées spontanément lorsque ces autorités ou ces organisations identifient une menace.

Lors de graves menaces pour la sûreté intérieure ou extérieure du pays, les intérêts de la collectivité publique à la communication d'un renseignement l'emportent sur la sauvegarde de la sphère privée. L'idée maîtresse est que les pouvoirs publics (Confédération, cantons, communes) participent solidairement à la lutte contre les menaces concrètes pour la sécurité de la Suisse et de ses citoyens.

Les *al. 1 et 2* fixent l'obligation de fournir des renseignements pour les menaces qui risquent de léser des biens juridiques importants. Les différentes sources d'où ces menaces peuvent émaner sont énumérées de manière exhaustive à l'al. 2: il s'agit d'activités terroristes, de l'espionnage politique, économique ou militaire, de la prolifération d'armes de destruction massives, d'attaques contre des infrastructures critiques et de l'extrémisme violent. Selon les règles de l'entraide administrative, cette disposition fait en principe obligation à l'ensemble des autorités et unités administratives de la Confédération et des cantons de communiquer toute information ayant trait à de telles menaces. Comme le prévoit le droit en vigueur, les demandes adressées aux services concernés n'ont pas besoin d'être détaillées ni même d'avoir un caractère de preuves. Ces services ne doivent être informés que du domaine d'activité du SRC auquel le renseignement demandé se rapporte.

L'*al. 2* précise de manière plus détaillée les tâches du SRC indiquées à l'art. 6. Il ne donne pas une définition légale des termes tels que terrorisme, mais décrit les menaces comme le fait l'art. 13*a* LMSI.

Si l'obligation de fournir des renseignements se justifie par la sauvegarde d'intérêts essentiels de la Suisse au sens de l'art. 3, elle requiert une décision du Conseil fédéral (cf. à ce sujet les commentaires concernant les art. 3 et 70).

Cet article correspond largement au nouvel art. 13*a* LMSI, introduit par la LMSI II. Les formules utilisées sont courantes dans la pratique du renseignement en matière de politique de sûreté, ce qui explique pourquoi on a renoncé à une description plus détaillée des différentes menaces telle qu'à l'art. 260^{quinquies} CP pour la poursuite pénale en cas de financement du terrorisme.

Alors que la LMSI mentionnait spécifiquement les autorités fiscales, le présent projet de loi ne les cite plus explicitement. En effet, les autorités fiscales sont également assujetties à l'obligation de fournir des renseignements puisqu'elles font partie des autorités nommées à l'al. 1. Une mention particulière pourrait au surplus donner l'impression que les autorités fiscales fournissent très souvent des informations au SRC, ce qui n'est pas le cas. Pour lever les incertitudes exprimées lors de la consultation, précisons que les banques cantonales ne peuvent pas être considérées comme des autorités des cantons au sens de l'al. 1. Les banques cantonales pourront donc continuer d'opposer le secret bancaire aux demandes du SRC.

Dans les cantons, l'obligation de fournir des renseignements s'étend aussi aux autorités administratives des communes; elles sont inclues dans le terme «canton».

Les organisations qui accomplissent des tâches publiques sont également soumises à l'obligation de fournir des renseignements. Il s'agit d'organisations ou de personnes de droit public ou privé extérieures à l'administration fédérale qui sont chargées de tâches administratives au sens de l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[22].

L'expression «cas particulier» souligne que l'obligation des autorités et des organisations de renseigner est permanente, mais qu'elle l'est uniquement dans des cas précis, concrets et sur demande du SRC (ou des autorités d'exécution cantonales agissant sur mandat du SRC). Comme cette obligation ne concerne que des cas particuliers et des menaces concrètes, le nombre relativement important des autorités et organisations qui y sont assujetties se justifie.

22 RS **172.010**

Conformément à l'art. 81, al. 1, les services de sécurité cantonaux peuvent aussi rechercher des informations de manière autonome pour l'exécution de la LRens en se fondant sur cet article. Les données issues de telles recherches qu'ils transmettent au SRC deviennent des données de la Confédération.

L'*al. 4* règle le cas d'une autorité qui constate de façon indépendante une menace pour la sûreté intérieure ou extérieure. Cette autorité doit avoir la possibilité de communiquer spontanément ce renseignement au SRC. Le pendant de cette disposition en cas de soupçon d'infraction pénale est l'art. 22*a* de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[23], qui fait obligation aux employés de la Confédération de dénoncer tous les crimes et délits poursuivis d'office.

Art. 20 Obligation spécifique de fournir et de communiquer des renseignements

L'*al. 1* énumère les autorités et services plus particulièrement chargés de tâches de sécurité et soumis à l'obligation spécifique de fournir et de communiquer des renseignements. Cette obligation va plus loin que l'obligation de renseigner en cas de menace concrète de l'art. 19, dans la mesure où elle n'est pas limitée à certains thèmes ou soumise à certaines conditions, mais doit servir à l'exécution de la loi en tant que telle. En revanche, contrairement à l'art. 19, elle ne concerne que les autorités et organes cités. Le Conseil fédéral estime qu'une extension aux autorités sociales ou fiscales, comme l'ont proposé certains participants à la consultation, serait inutile et disproportionnée.

L'obligation spécifique de fournir et de communiquer des renseignements visée à l'al. 1 n'est pas absolue, mais est liée à des organisations et des cas concrets. Elle se rapporte ainsi aux tâches spécifiques qu'accomplissent les autorités citées. Concrètement, les autorités chargées de l'exploitation de systèmes informatiques visées à la let. i, par exemple, ne sont tenues de fournir que des renseignements techniques sur l'exploitation de ces systèmes: elles ne doivent livrer aucune information sur leur contenu, en particulier celui des banques de données qu'elles exploitent. La nouvelle let. i (par rapport à la LMSI) ne vise ainsi que la sécurité cybernétique et la protection d'infrastructures critiques.

L'*al. 3* règle à nouveau le cas d'une autorité qui constaterait de façon indépendante une menace concrète pour la sûreté intérieure ou extérieure.

L'*al. 4* correspond au droit en vigueur (art. 11, al. 2, let. a, LMSI). La plus grande partie des autorités soumises à l'obligation de communiquer des renseignements sont publiées dans l'annexe 1 de l'OSRC. Les renseignements sur des événements et des constatations qui ne peuvent être publiés pour des raisons de sauvegarde du secret seront définis comme aujourd'hui dans une liste confidentielle. Les services concernés seront informés personnellement de leurs obligations. La Délégation des Commissions de gestion des Chambres fédérale aura accès par ailleurs à toutes les informations nécessaires pour ses tâches de surveillance.

23 RS **172.220.1**

Art. 21 Procédure en cas de divergences d'opinion

L'*al. 1* règle la procédure en cas de divergences d'opinion au sein de l'administration fédérale. Si celles-ci surviennent au sein du DDPS, c'est le chef du département qui statue. Si elles impliquent les services d'autres départements, cette tâche revient au Conseil fédéral, en sa qualité d'autorité de surveillance commune. Cette pratique correspond aux règles générales de l'organisation de l'administration.

L'*al. 2* règle la procédure pour les divergences d'opinion entre la Confédération et les cantons, en donnant au Tribunal administratif fédéral la compétence de trancher.

Art. 22 Communications et renseignements fournis par des tiers

Les informations fournies au SRC ou aux autorités d'exécution cantonales par des particuliers le sont sur une base volontaire. Lors de l'utilisation de couvertures dissimulant l'appartenance à un service de renseignement, la personne interrogée ne peut toutefois être rendue attentive au fait qu'elle est libre de fournir des renseignements ou de refuser d'en fournir. Lorsqu'une personne qui communique ou qui fournit des informations est soumise au secret professionnel ou à d'autres prescriptions légales lui imposant le secret, elle doit pouvoir respecter cette obligation à l'égard du SRC et des autorités cantonales d'exécution, comme elle le fait à l'égard de toute autre personne ou service officiel.

L'*al. 3* n'est pertinent que dans le cas de couvertures, puisque les identités d'emprunt utilisées lors de la recherche d'informations en Suisse n'impliquent pas obligatoirement une dissimulation de l'appartenance au SRC.

Art. 23 Identification et interrogatoire de personnes

Cet article a été ajouté au projet de loi après la procédure de consultation parce que la LMSI permet actuellement au SRC de procéder à des investigations sur l'identité et le lieu de séjour de personnes. Cette nouvelle disposition a été formulée sur la base de l'art. 215 du code de procédure pénale (CPP), qui règle l'appréhension de personnes par la police en vue d'élucider une infraction. En règle générale, les lois cantonales sur la police contiennent des dispositions comparables pour l'accomplissement de tâches relatives à la sécurité.

L'identification et l'interrogatoire de personnes prévue au présent article sert à l'accomplissement des tâches de renseignement en rapport avec les domaines classiques du renseignement en Suisse: défense contre le terrorisme, l'espionnage, l'extrémisme violent, la prolifération d'armes de destruction massive et les attaques visant des infrastructures critiques. Elle ne doit durer que le temps nécessaire pour atteindre l'objectif.

Comme dans le CPP, fixer une durée maximale n'est pas judicieux car celle-ci dépend des circonstances et doit donc être proportionnelle à ces dernières. Ainsi, un simple contrôle d'identité ne doit pas dépasser quelques minutes, alors qu'un interrogatoire peut, selon les circonstances, durer quelques heures, en particulier lorsqu'il doit se dérouler dans un lieu protégé. Par analogie à la différence établie par le CPP entre l'appréhension et l'arrestation par la police (art. 215 ss CPP), la durée totale de cette mesure doit être inférieure à trois heures.

L'interrogatoire se déroule conformément aux dispositions de l'art. 22. La personne interrogée est donc libre de répondre ou non aux questions qui lui sont posées.

Art. 24 Obligations spécifiques faites aux particuliers de fournir des renseignements

L'*al. 1* reprend l'art. 13*c* LMSI (obligation de renseigner des transporteurs commerciaux), ajouté en 2012, et l'élargit aux exploitants privés d'infrastructures de sécurité telles que les installations de vidéosurveillance ou des systèmes d'accès électroniques, qui peuvent aussi fournir des informations importantes. Comme dans la LMSI, nul n'est tenu de relever ou de conserver des données spécifiques du fait de cette disposition: celle-ci est uniquement destinée à garantir l'accès, en cas de menace concrète, à des données existantes.

De telles informations pourraient par exemple être importantes pour constater des déplacements de personnes impliquées dans des activités terroristes, d'extrémisme violent, d'espionnage ou de prolifération d'armes de destruction massive. Elles peuvent être fournies par des compagnies aériennes, des agences de voyages et des entreprises de location de véhicules, par exemple. Les exploitants privés d'infrastructures de sécurité sont en règle générale des entreprises qui protègent leurs propres infrastructures ou celles de tiers, en particulier dans le secteur du trafic routier, des transports, de l'énergie ou des ventes.

L'*al. 2* donne au SRC la possibilité, déjà prévue dans la loi du 30 avril 1997 sur les télécommunications (LTC), d'obtenir par l'intermédiaire du service chargé de la surveillance de la correspondance par poste et télécommunication (rattaché au DFJP) des informations sur les raccordements de télécommunication d'une personne et sur d'autres éléments d'adressage ainsi que sur la personne à laquelle des éléments d'adressage identifiés sont attribués (par ex. des numéros de téléphone). La LTC est modifiée pour renvoyer à la LRens (art. 14, al. 2bis, LTC[24]). Les renseignements en question ne sont pas soumis au secret des télécommunications.

En cas de nécessité, l'obligation spécifique faite aux particuliers de fournir des renseignements est imposée par une décision administrative fédérale sujette à recours, si nécessaire avec renvoi à l'art. 292 du code pénal (Insoumission à une décision de l'autorité). Soumettre la demande de renseignement à une autorisation judiciaire préalable serait dès lors disproportionné.

Conformément à l'art. 79, les décisions du SRC sont sujettes à recours. La recherche d'informations, par exemple sur des personnes soupçonnées d'activités terroristes qui menacent la Suisse, doit souvent être effectuée dans des délais très courts. S'il fallait attendre la conclusion d'une longue procédure de recours, l'information communiquée par une entreprise de transport pourrait ne plus être utile. C'est pourquoi le présent projet prévoit qu'un recours n'a pas d'effet suspensif (art. 79, al. 3).

Chapitre 3, section 4

Pour s'acquitter de ses tâches, en particulier détecter précocement et évaluer les menaces et les dangers pouvant limiter la capacité de décision et d'action des autorités suisses ou menaçant les fondements démocratiques et les structures de l'État, le SRC a besoin de moyens efficaces de recherche d' informations.

24 Dans le projet de révision totale de la LTC, (FF **2013** 2379), la disposition correspondante se trouve à l'art. 15.

Les organes de renseignement de la Confédération et des cantons sont confrontés à des adversaires toujours plus brutaux et inhumains, surtout dans le domaine du terrorisme. Ainsi, entre le 11 et le 19 mars 2012, sept personnes, dont des enfants, ont été froidement assassinées sur la voie publique dans le sud de la France, à Toulouse et Montauban. L'auteur était un Français d'origine algérienne prétendant appartenir au groupe terroriste Al-Qaïda. Les autorités françaises savaient qu'il avait effectué des voyages en Afghanistan et au Pakistan. Il était par ailleurs en contact avec un mouvement salafiste radical en France.

Le SRC a connaissance de plusieurs personnes ayant des liens avec la Suisse pour lesquelles des parallèles peuvent être tirés avec un cas de radicalisation comme celui de Toulouse et Montauban. Les personnes en question se sont radicalisées sur Internet et ont séjourné dans des camps d'entraînement terroristes à l'étranger. Les auteurs isolés radicalisés, tels que l'assassin de Toulouse et Montauban, mènent une vie discrète et, vu de l'extérieur, donnent l'impression d'être bien intégrés dans la société. Souvent, ils ne partagent pas leurs véritables desseins avec leur entourage le plus proche. Les autorités n'obtiennent donc que peu d'indices de la part de la population et sont de plus en plus tributaires de mesures de recherche particulières comme celles proposées dans le présent projet de loi pour se procurer suffisamment tôt des informations pertinentes sur de telles personnes. Même si la Suisse n'est pour l'heure pas visée par le terrorisme international, nul ne saurait dire si ce constat sera toujours valable dans quelques années.

Les activités menées dans la clandestinité sont également courantes dans d'autres domaines de compétence du SRC, que ce soit dans celui de l'espionnage, de la prolifération d'armes de destruction massive ou des attaques visant des infrastructures critiques. Il est donc très difficile de collecter des renseignements sur les activités et les intentions de ces milieux si la recherche d'informations se limite aux lieux publics.

Le Conseil fédéral estime que le SRC n'est plus que partiellement en mesure de remplir sa mission avec les moyens de recherche actuels, qui consistent pour l'essentiel dans la collecte d'informations issues de sources accessibles au public, dans les demandes de renseignements et dans les observations de lieux publics (art. 14 LMSI). De nombreux événements permettant d'apprécier la menace ne surviennent en effet pas dans des lieux publics et il est rare que des communications liées à des menaces pour la sûreté intérieure ou extérieure puissent être découvertes sur les sites publics d'Internet. Si le SRC doit jouer pleinement son rôle d'organe préventif pour la sécurité de la Confédération et remplir les tâches qui lui sont confiées à ce titre par la présente loi, il faut lui donner la possibilité de mettre en œuvre des mesures de recherche supplémentaires qui soient efficaces.

Au vu de la situation actuelle de la menace, le Conseil fédéral estime qu'une dizaine de cas impliquant des mesures de recherche soumises à autorisation se poseront chaque année, un même cas pouvant comporter plus d'une mesure (par ex. la surveillance de plusieurs raccordements de télécommunication, la localisation d'un véhicule et la fouille d'une chambre d'hôtel d'une même personne). Les cas en question comportent un potentiel de menace particulièrement élevé dans les domaines du terrorisme, de l'espionnage, de la prolifération d'armes de destruction massive et d'attaques visant des infrastructures critiques ou touchent à la sauvegarde d'intérêts essentiels de la Suisse au sens de l'art. 3 et les autres mesures de recherche ne suffiraient pas à obtenir des informations fondamentales pour le maintien de la sûreté de la Suisse.

Les mesures de recherche soumises à autorisation englobent notamment (art. 25):

- la surveillance de la correspondance par poste et télécommunication selon les règles de la LSCPT[25];
- la détermination de l'emplacement de personnes ou d'objets grâce à la localisation d'un téléphone mobile utilisé par la personne (selon les règles de la LSCPT) ou à l'aide d'appareils de localisation spéciaux (en règle générale, des récepteurs GPS avec ou sans émetteurs);
- l'utilisation d'appareils de surveillance pour mettre des conversations sur écoute et observer des événements dans des locaux privés;
- l'introduction dans des systèmes et réseaux informatiques en vue de se procurer les informations qu'ils contiennent ou qui ont été transmises à partir de ces systèmes ou en vue de perturber, d'empêcher ou de ralentir l'accès à des informations lors d'attaques visant des infrastructures critiques commises à partir de ces systèmes;
- la fouille de locaux, de véhicules ou de conteneurs emportés par des personnes en vue de se procurer les objets et informations qu'ils contiennent ou les informations qui ont été transmises depuis ces endroits. Les locaux, véhicules ou conteneurs peuvent être fouillés secrètement et à l'insu des personnes concernées.

Avant de pouvoir être mises en œuvre par le SRC, ces mesures doivent être autorisées par le Tribunal administratif fédéral et, après consultation de la Délégation pour la sécurité, être avalisées par le chef du DDPS. Le directeur du SRC peut à titre exceptionnel ordonner leur mise en œuvre immédiate si un danger est imminent. La demande d'autorisation doit alors être adressée au Tribunal administratif fédéral dans les 24 heures (art. 30, al. 2).

Il faut souligner que ces recherches d'informations ne concernent que les menaces pertinentes en matière de sécurité qui n'ont aucun lien avec des enquêtes pénales. Si la menace est liée à une présomption d'acte répréhensible, les autorités de poursuite pénale doivent être informées (voir art. 59). Une éventuelle procédure pénale et des mesures de surveillance ordonnées dans ce cadre priment les recherches d'informations prévues par la présente loi. Toutes les menaces pertinentes en matière de sécurité ne sont toutefois pas pertinentes du point de vue pénal et des présomptions ne suffisent pas forcément pour lancer une enquête pénale.

La loi ne doit autoriser de telles mesures intrusives que dans les cas importants, lorsque la sûreté de la Suisse est menacée. Pour ce faire, elle définit un cadre strict et une procédure d'autorisation à plusieurs niveaux.

Comme pour l'ensemble des champs d'application de la présente loi, la Délégation des Commissions de gestion des Chambres fédérales aura plein accès aux données et pièces nécessaires pour la surveillance.

Art. 25 Types de mesures soumises à autorisation

L'*al. 1, let. a,* permet au SRC d'ordonner la surveillance de la correspondance par poste et télécommunication selon les dispositions de la LSCPT. Contrairement aux

25 Une révision totale de la LSCPT est en délibérations au Parlement. Voir aussi les commentaires concernant le ch. 14 de la modification d'autres actes.

autorités de poursuite pénale, qui font appel à ce type de mesures dans le cadre d'une procédure pénale visant à prouver la culpabilité de l'auteur (objectif répressif), le SRC ne les ordonne qu'à des fins préventives, en vue d'identifier suffisamment tôt les menaces pour la sûreté intérieure ou extérieure de la Suisse. Si le SRC, au cours de ses recherches, soupçonne des actes répréhensibles, il en informe les autorités de poursuite pénale.

Contrairement à l'avant-projet, qui énumérait chaque mesure de surveillance dans le domaine de la correspondance par poste et télécommunication pour une meilleure compréhension durant la procédure de consultation, la disposition renvoie désormais d'une manière générale aux types de surveillance prévus dans la LSCPT, facilitant ainsi la coordination avec cette loi en cours de révision totale[26]. Ce renvoi permet aussi d'éviter les malentendus survenus au cours de la consultation, selon lesquels la présente loi introduirait d'autres formes de surveillance et de nouvelles contraintes pour les fournisseurs de prestations de télécommunication, puisque l'exécution des surveillances se fait par l'intermédiaire du service de surveillance de la correspondance par poste et télécommunication (SSCPT), rattaché au DFJP.

Au cours de la consultation, les fournisseurs de prestations de télécommunication ont souligné que les indemnités prévues pour les surveillances selon la LSCPT ne couvraient pas l'intégralité des coûts et que l'obligation légale pour les prestataires de services d'exécuter certaines mesures n'était pas toujours claire. Ces questions ne doivent toutefois pas être traitées dans le cadre de la LRens, mais lors de la révision totale de la LSCPT. Les contraintes imposées aux fournisseurs de prestations de télécommunication dans le but de garantir techniquement les capacités de surveillance sont une conséquence de l'autorisation qu'ils ont reçue de l'État de se développer dans un segment d'activités lucratif et important qui relève du service public.

Les mandats supplémentaires de surveillance que le SSCPT devrait recevoir de la part du SRC ne représentent qu'une assez faible augmentation par rapport aux prestations qu'il fournit pour les autorités de poursuite pénale (2011: 2699 mesures de surveillance en temps réel, 5758 mesures de surveillance rétroactives ou données secondaires et 3918 renseignements technico-administratifs[27]).

La *let. b* règle l'engagement de moyens techniques, tels que des GPS, qui permettent de déterminer la position d'une personne, d'un véhicule ou d'un autre objet mobile. Les enregistrements de ces instruments fournissent un «schéma de déplacements» ou transmettent un signal permettant de localiser la position de l'émetteur et de constater où se trouve la personne, l'émetteur, le véhicule ou l'équipement mobile, et le cas échéant de les enregistrer. Ces moyens sont notamment destinés à soutenir des mesures d'observation (de manière analogue aux engagements de police, où leur usage est courant depuis des années), en particulier en cas de perte de contact avec l'objectif, et même à les remplacer en partie (lorsqu'une observation directe n'est pas nécessaire) ou les préparer (en relevant les habitudes d'une personne à surveiller, ce qui permet ensuite aux équipes de mieux cibler leurs observations).

Afin de ne pas exclure les développements techniques dans ce domaine, la définition des appareils à engager est volontairement ouverte.

26 Voir à cet égard FF **2013** 2379
27 La statistique du service peut être consultée en ligne à l'adresse suivante: /www.li.admin.ch > Thèmes > Statistiques

Si la localisation d'un téléphone mobile se fait par le biais de données du fournisseur de prestations de télécommunication, elle relève de la surveillance des télécommunications selon la LSCPT, réglementée par la let. a.

La *let. c* permet notamment d'enregistrer les conversations de personnes surveillées dans des locaux privés et de procéder à une surveillance par l'image (technique vidéo). Le droit en vigueur n'autorise une telle mesure que dans le cas d'une procédure pénale. Lorsque des indices concrets laissent présumer que certaines personnes mènent des activités menaçant gravement la sécurité, le SRC doit être en mesure d'étendre ses recherches à des locaux privés. Les principes fixés à l'art. 26 sont également applicables.

L'exemple ci-après illustre une mise en œuvre possible de mesures techniques de surveillance: les contacts qu'entretiennent les petites cellules terroristes (par ex. la cellule tricéphale du *Nationalsozialistischer Untergrund* [Mouvement clandestin national-socialiste] en Allemagne) n'ont lieu que clandestinement. En public, ces personnes n'expriment jamais leurs vraies intentions. Elles n'ont de ce fait aucun contact avec des personnes extérieures à leur cellule auxquelles elles les confieraient. L'engagement d'informateurs n'est pas possible, puisque les cellules en question ne permettent aucun accès de personnes extérieures. Seuls les moyens techniques de surveillance évoqués permettent donc d'obtenir les informations dont le SRC a besoin pour empêcher que la sûreté soit mise en danger, par exemple par des attentats. Lorsque le seuil de présomption d'un acte répréhensible est franchi, le SRC informe les autorités de poursuite pénale (art. 59).

La *let. d* prend en compte le transfert de plus en plus important de déclarations et d'actions menaçant la sécurité sur des sites Internet sécurisés. Au vu des menaces croissantes qu'elles entraînent pour la sûreté de la Suisse, le SRC a besoin de nouveaux moyens adéquats pour pouvoir explorer des réseaux informatiques et évaluer ces menaces dans le cadre de ses tâches de prévention. Le projet lui permet, d'une part, de se procurer des informations (ch. 1) et, d'autre part, de perturber, d'empêcher ou de ralentir l'accès à des informations (ch. 2) lors d'attaques visant des infrastructures critiques.

Afin de pouvoir détecter et évaluer des développements importants qui présentent un danger pour la sûreté de la Suisse, le SRC doit aussi pouvoir s'introduire dans des réseaux informatiques hautement sécurisés. Les informations obtenues peuvent par exemple contribuer à identifier et à empêcher des projets d'activités terroristes.

Les attaques visant à perturber des infrastructures critiques peuvent menacer gravement la sûreté intérieure ou extérieure de la Suisse et peuvent entraîner des dommages très importants. Sont visées notamment les attaques électroniques visant l'approvisionnement en énergie (centrales nucléaires), les transports (aériens, ferroviaires ou routiers), l'industrie chimique (déchets spéciaux), les télécommunications (radio et télévision), le domaine de la santé (assistance médicale) ou celui des finances et des assurances (bourses). Le ch. 2 doit donc permettre de lutter contre un dommage imminent ou contre un dommage total ou partiel découlant d'une attaque en cours. Le principe de subsidiarité est respecté dans la mesure où le SRC n'intervient qu'en dernier recours, c'est-à-dire après d'éventuelles procédures pénales et uniquement si les conditions préalables pour une telle procédure ne sont pas (encore) réunies ou que celle-ci ne permettrait pas de lutter contre une telle attaque. Dans ce contexte, la protection préventive du pays (par ex. contre une contamination radioactive) doit être prioritaire. Soulignons que les mesures indiquées sous le ch. 2

sont toujours soumises à autorisation si elles sont dirigées contre des systèmes en Suisse, c'est-à-dire qu'elles doivent être approuvées au niveau judiciaire (autorisation par le Tribunal administratif fédéral) et politique (aval du chef du DDPS).

Au DFJP, c'est le Service de coordination de la lutte contre la criminalité sur Internet qui est chargé de la poursuite pénale des activités criminelles sur Internet.

La *let. e* donne une nouvelle compétence au SRC, à savoir la possibilité de procéder dans des cas importants, sous contrôle judiciaire et politique, à des fouilles dans des locaux, véhicules ou conteneurs pour se procurer des informations (par ex. des documents) ou des objets qui mettent la sûreté en danger. Il peut s'agir de sacs, de valises, de conteneurs, de supports de données ou d'appareils enregistreurs, tels que caméras et dictaphones. Le SRC n'est cependant pas autorisé à fouiller des personnes, cette mesure restant réservée aux organes de police.

On se référera également aux commentaires concernant la modification de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (modification d'autres actes), «Coordination avec la révision totale de la LSCPT», «Art. 25, al. 1, let. a et a^{bis} (LRens)».

L'*al. 2* prévoit que les mesures précitées peuvent être exécutées secrètement et à l'insu des personnes concernées. Cette disposition est nécessaire pour que la mesure puisse atteindre son objectif. Une double procédure d'autorisation judiciaire et politique garantit en contrepartie que ces mesures répondent aux exigences de l'état de droit. La mesure est communiquée ultérieurement à la personne concernée (art. 32) et celle-ci a alors la possibilité de déposer un recours (art. 79).

Aujourd'hui, les officiers de services de renseignement étrangers et les membres de réseaux terroristes peuvent se sentir à l'abri d'une détection précoce dans leurs communications. Cette situation est d'ailleurs exploitée en conséquence. A l'avenir, le seul fait que le SRC dispose de plus de compétences devrait inciter ces acteurs à plus de retenue et à freiner les projets de services étrangers d'agir de leur propre chef dans notre pays.

Art. 26 Principe

L'*al. 1* fixe deux conditions à l'engagement de mesures de recherche soumises à autorisation, à savoir soit l'existence d'une menace concrète pour la sûreté intérieure ou extérieure de la Suisse, à l'exception de l'extrémisme violent, soit la sauvegarde d'intérêts essentiels de la Suisse au sens de l'art. 3 sur la base d'une décision du Conseil fédéral. Dans sa décision, le Conseil fédéral détermine aussi à quelles conditions des mesures soumises à autorisation peuvent être mises en œuvre. Dans tous les cas, la procédure d'autorisation visée aux art. 28 et suivants doit être appliquée, autrement dit la décision du Conseil fédéral ne remplace pas la procédure mais est une condition formelle pour que de telles mesures puissent être prises dans les cas de figure où il n'y a pas de menace concrète au sens strict telle que définie par la loi.

En présence d'intérêts essentiels et d'une menace concrète pour la sûreté intérieure ou extérieure de la Suisse au sens de l'art. 19, al. 2, let. a à d, les deux conditions supplémentaires ci-après doivent être remplies afin qu'une mesure de recherche soumise à autorisation puisse être engagée:

– la gravité de la menace pesant sur la sûreté de la Suisse doit justifier la mesure;

– la recherche d'informations effectuée jusque-là est restée vaine et, sans recours à une mesure soumis à autorisation, elle serait vouée à l'échec ou demanderait des efforts disproportionnés.

Ces exigences supplémentaires liées au principe constitutionnel de la proportionnalité s'inspirent du droit régissant la procédure pénale (voir l'art. 269, al. 1, CPP). Le fait qu'une organisation ou un groupement figure sur la liste d'observation visées à l'art. 71 n'est donc pas suffisant. Un tel élément peut certes constituer un indice de la gravité de la menace pesant sur la sûreté intérieure, mais il faut en apporter la preuve dans le cas concret avant de pouvoir déclencher la mesure. La nécessité de la mesure au sens de la let. c doit également être prouvée dans le cas concret.

L'extrémisme violent doit être exclu de ces mesures de recherche. Le Conseil fédéral est en effet d'avis que l'extrémisme violent se rapproche davantage de mouvements politico-idéologiques, ce qui appelle une certaine retenue. En revanche, lorsque l'extrémisme violent se transforme en terrorisme, une surveillance à ce titre est possible. La désignation annuelle des groupements extrémistes violents par le Conseil fédéral conformément à l'art. 69 du projet de loi garantit à cet égard le pilotage politique et empêche que le SRC puisse assimiler de manière autonome des groupements extrémistes au terrorisme.

Les services tiers chargés selon l'*al. 3* de mettre en œuvre ces mesures sont, notamment, le SSCPT du DFJP pour la surveillance des télécommunications et les organes de sûreté des cantons pour l'engagement d'appareils techniques de surveillance ou des fouilles.

Art. 27 Mesures ordonnées à l'encontre de tiers

Il se peut qu'une personne pour laquelle les conditions visées à l'art. 26, al. 1, sont remplies et qui peut donc faire l'objet d'une mesure de recherche soumise à autorisation utilise le téléphone, l'adresse postale, l'ordinateur, le véhicule ou d'autres équipements d'un tiers pour transmettre et recevoir des informations, que ce dernier en ait conscience ou non.. Dans de tels cas, le SRC doit avoir la possibilité de faire surveiller les communications postales et téléphoniques du tiers en question, d'accéder à ses ordinateurs ou de fouiller ses locaux et véhicules afin d'obtenir les informations recherchées sur la personne concernée et d'atteindre ainsi l'objectif de la mesure mise en œuvre. La sphère privée de la tierce personne doit être protégée autant que possible et elle doit être informée de cette mesure une fois que celle-ci a pris fin (art. 32).

Il est interdit de surveiller un tiers qui bénéficie du droit de refuser de témoigner selon les art. 171 à 173 CPP, par ex. les ecclésiastiques, les avocats, les médecins et leurs auxiliaires ou les professionnels des médias. La LRens reprend ici également les règles du CPP. Une extension à d'autres groupes professionnels, comme proposé par certains participants à la consultation (par ex. aux fournisseurs de prestations financières), constituerait une très grande nouveauté sur le plan juridique et le Conseil fédéral ne la juge pas nécessaire à l'heure actuelle. Elle devrait en tout état de cause être débattue de manière plus approfondie que ne le permet le cadre de la LRens.

Art. 28 Procédure d'autorisation

La procédure d'autorisation proposée comprend deux phases: dans un premier temps, le SRC doit demander l'autorisation d'une instance judiciaire, en l'occurrence le Tribunal administratif fédéral (TAF). L'appréciation et l'autorisation de la mesure d'un point de vue politique par le chef du DDPS n'interviennent que dans un second temps, lorsque le TAF a approuvé la mesure sur le plan juridique (art. 29). Avant de donner son aval, le chef du DDPS consulte au surplus la Délégation du Conseil fédéral pour la sécurité.

Concrètement, la procédure se déroule comme suit:

1. le SRC demande au TAF l'autorisation de mettre en œuvre une mesure de recherche soumise à autorisation;
2. le président de la cour compétente du TAF examine la demande et décide d'autoriser ou de rejeter la mesure sollicitée; il peut également demander un complément d'informations;
3. si le TAF a autorisé la mesure, il incombe ensuite au chef du DDPS de donner son aval.
4. le SRC peut mettre en œuvre la mesure ou mandater un tiers à cet effet (par ex. le SSCPT).

La demande doit contenir toutes les indications permettant de vérifier si la mesure répond aux exigences légales, à savoir la description des indices effectifs de menace concrète pour la sûreté intérieure ou extérieure de la Suisse, la justification de la proportionnalité de la mesure, la désignation de la personne à surveiller, pour autant qu'elle soit déjà identifiée, les moyens à déployer et les éventuelles mesures de protection visant à préserver les droits de la personne surveillée ou de tiers. Par analogie au CPP, le président de la cour compétente du TAF doit brièvement motiver sa décision. L'art. 23 de la loi sur le Tribunal administratif fédéral prévoit la possibilité de décisions prises par un juge unique (voir également Modifications d'autres actes, ch. 5).

Le TAF constitue la bonne instance, car il est déjà chargé du contrôle juridique de mesures de politique de sécurité, par ex. lors de l'appréciation de recours contre des interdictions d'entrée dans le pays prononcées pour des motifs ressortissant à la sûreté intérieure ou extérieure. Proposé par certains participants à de la consultation, le Tribunal pénal fédéral a une approche toute différente de celle du TAF, puisqu'il applique des critères relevant du droit pénal pour évaluer des soupçons d'infraction. Le Conseil fédéral souhaite donc aussi bien séparer dans la procédure d'autorisation le renseignement et la poursuite pénale.

Par analogie avec l'art. 274, al. 5, CPP, l'autorisation est octroyée pour une durée maximale de trois mois et peut être prolongée plusieurs fois de trois mois au plus. Si une prolongation s'avère nécessaire, le SRC dépose une demande en fournissant les mêmes indications que celles exigées pour l'approbation initiale (al. 5). Pour autoriser une prolongation, le juge évalue la durée globale de la mesure dans le cadre d'un examen de la proportionnalité et apprécie d'autres facteurs tels que la gravité et le caractère concret de la menace.

Cette procédure doit tenir compte du fait que le déploiement de mesures de recherche soumises à autorisation peut porter atteinte à des droits fondamentaux sans

que la personne surveillée n'en ait connaissance et sans qu'elle ne puisse s'y opposer pendant toute la durée de validité de la mesure.

Les informations issues des mesures de recherche soumises à autorisation doivent répondre à des règles d'utilisation particulières pour les autorités de poursuite pénale afin d'éviter que de telles mesures de surveillance soient utilisées dans des procédures pénales au cours desquelles aucune mesure d'enquête comparable n'aurait été autorisée (voir à ce sujet l'art. 59, al. 3 et 4).

Certains participants à la consultation ont proposé d'obtenir l'autorisation judiciaire après l'aval politique, afin que le juge n'ait pas à se préoccuper de mesures politiquement impensables et que les décideurs politiques ne contentent pas de l'appréciation juridique. Le Conseil fédéral est toutefois d'avis que la proposition initiale doit être gardée. En en effet, si la procédure était inversée, trois conseillers fédéraux devraient traiter une demande supposément contraire à la loi avant son traitement par le juge unique. On pourrait de plus arguer qu'un juge unique pourrait appréhender de prendre une décision allant à l'encontre de la recommandation de la Délégation pour la sécurité et de la décision du chef du DDPS. La procédure d'autorisation proposée lors de la consultation a d'ailleurs été soutenue par une grande majorité des participants à la consultation.

Art. 29 Aval

Le présent article règle l'aval que le chef du DDPS doit donner aux mesures de recherche autorisées par un juge après consultation de la Délégation du Conseil fédéral pour la sécurité. Cette procédure en deux étapes permet de veiller à ce que la mise en œuvre des mesures ayant une telle incidence sur les droits fondamentaux ne soit pas envisagée seulement sous l'angle juridique mais également du point de vue politique. La conduite de la politique de sécurité dispose ainsi d'une large marge de manœuvre politique pour refuser de donner son aval à une telle mesure.

Soulignons que le chef du DDPS ne peut donner son aval qu'à des mesures qui ont préalablement été autorisées sur le plan judiciaire. Il ne peut donc pas donner son feu vert à une mesure non autorisée.

Conformément à l'art. 22 LOGA, la suppléance du chef du DDPS est assurée par un autre membre du Conseil fédéral. Une délégation au sein du département n'est pas possible.

Art. 30 Procédure en cas d'urgence

Contrairement aux autorités de poursuite pénale, qui peuvent par exemple surveiller du courrier et une ligne téléphonique immédiatement et en demander l'autorisation ultérieurement (voir à cet égard l'art. 274, al. 1, CPP), le SRC doit en principe obtenir l'approbation du TAF et l'aval du chef du DDPS, lequel consulte au préalable la Délégation du Conseil fédéral pour la sécurité, avant d'ordonner des mesures au sens des art. 25 et suivants.

En cas de danger imminent, l'art. 30 prévoit la possibilité pour le SRC d'engager immédiatement une mesure au sens des art. 25 ss. Un tel cas de figure se présente lorsque seule une action immédiate permet de constater les faits à temps ou d'observer certaines activités.

Si le SRC est par exemple informé qu'une personne importante liée à des activités relevant du terrorisme ou du renseignement se trouve dans un avion à destination de Zurich et qu'elle y atterrit dans trois heures, seules des mesures de recherche soumises à autorisation qui sont immédiatement mises en œuvre (par ex. surveillance du téléphone mobile, fouille discrète des bagages, pose d'un appareil de localisation) peuvent permettre d'acquérir les informations nécessaires pour l'appréciation de la menace actuelle. Une fois cette fenêtre passée, il n'est presque plus possible de rattraper ces recherches manquées.

Le chef du DDPS a plusieurs possibilités pour interrompre la mise en œuvre d'une mesure ordonnée dans l'urgence:

– il peut y mettre un terme immédiatement dès qu'il en a été informé par le SRC;

– il peut décider de ne pas donner son aval après avoir été informé de l'autorisation du TAF (voir à cet égard l'art. 32); il ne dispose en effet du contexte global de la mise en œuvre que sur la base de la demande écrite, alors que la première information est de nature sommaire.

Art. 31 Fin de la mesure de recherche

Les règles qui s'appliquent pour mettre un terme aux mesures de recherche soumises à autorisation correspondent aux normes habituelles (voir à cet égard l'art. 275 CPP). L'*al. 1, let. b*, explicite le principe de proportionnalité et empêche à ce titre qu'une mesure ne soit appliquée plus longtemps que nécessaire.

En informant les instances d'autorisation visées à l'*al. 4* de la fin d'une mesure, on s'assure qu'elles aussi sont toujours au courant des mesures qui sont en cours d'exécution.

Art. 32 Obligation d'informer les personnes surveillées

L'obligation d'informer a posteriori les personnes visées par des mesures soumises à autorisation découle de la protection de la vie privée et du respect de la sphère privée. Cette garantie s'appuie sur les art. 8 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)[28] et 13 de la Constitution (Cst.).

Lorsqu'une opération, c'est-à-dire une procédure concertée d'une ou plusieurs mesures de recherche relatives à des faits donnés, est terminée, le SRC doit informer les personnes visées par la mesure et les tiers dont les raccordements ont le cas échéant été placés sous surveillance, en principe dans un délai d'un mois (*al. 1*). La loi ne se réfère pas ici à la mesure individuelle, puisque d'autres mesures de recherche autorisées peuvent être en cours et qu'elles pourraient être mises en péril par la communication d'une mesure terminée (exemple typique: l'acquisition des données secondaires d'anciennes communications téléphoniques selon l'art. 25, al. 1, let. c, se termine avec la transmission des données, alors que la surveillance des télécommunications se poursuit en parallèle). Souvent, ce n'est qu'au terme de toutes les mesures que l'on peut déterminer si la personne doit être informée ou s'il fait faire une exception au sens de l'al. 2 (par ex. parce que le cas est transmis aux

[28] RS **0.101**

autorités de poursuite pénale et qu'une procédure juridique est ainsi engagée). Dans le premier cas, la personne surveillée est simultanément informée des possibilités de recours visées à l'art. 79.

L'obligation d'informer ne s'applique ni à l'exploration radio ni à l'exploration du réseau câblé (art. 36 à 42), étant donné que cette exploration n'est pas axée sur les raccordements de télécommunications des particuliers, mais sur les informations importantes du point de vue de la politique de sûreté issues d'émetteurs radio ou de transmissions du réseau câblé provenant de l'étranger. Dans ce dernier cas, ce ne sont pas les personnes ou leur vaste trafic de télécommunications qui sont le but de la recherche d'informations.

L'*al. 2, let. a*, s'inspire de la jurisprudence de la Cour européenne des droits de l'homme, qui a constaté dans l'arrêt Klass contre la République fédérale d'Allemagne du 6 septembre 1978 qu'une notification ultérieure pouvait remettre en question l'objectif à long terme d'une surveillance et qu'il était possible d'y renoncer à certaines conditions. Elle a notamment précisé ce qui suit:

«… Une notification ultérieure à chaque individu touché par une mesure désormais levée pourrait bien compromettre le but à long terme qui motivait à l'origine la surveillance. En outre, la Cour constitutionnelle fédérale l'a fait remarquer à juste titre, pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignements, leurs champs d'observation et même, le cas échéant, l'identité de leurs agents. De l'avis de la Cour, dès lors que l'‹ingérence› résultant de la législation contestée se justifie en principe au regard de l'art. 8 par. 2 (art. 8-2) [CEDH] […], il ne saurait être incompatible avec cette disposition de ne pas informer l'intéressé dès la fin de la surveillance, car c'est précisément cette abstention qui assure l'efficacité de l'‹ingérence›».

La *let. b* se fonde sur les intérêts publics prépondérants pour préserver la sûreté intérieure ou extérieure, qui sont également reconnus par la CEDH. L'objectif est également de ne pas donner aux cercles constituant une menace pour la sûreté des indications sur les activités de la Suisse en matière de défense. On pense par exemple au ressortissant somalien qui, de la Suisse, recrute dans le pays des voyageurs du djihad volontaires.

La *let. c* reprend le principe de la protection des intérêts légitimes de tiers. Le SRC peut par exemple renoncer à informer un tiers d'une surveillance si cela devait compromettre la personne directement visée par la surveillance.

La *let. d* se rapporte à une situation dans laquelle le lieu de séjour de la personne concernée ou du tiers ne pourrait être déterminé qu'au prix d'efforts disproportionnés ou dans laquelle le lieu de séjour est certes connu, mais que l'intéressé ne pourrait y être joint qu'au prix d'efforts disproportionnés (notamment à l'étranger) ou qu'il pourrait même être mis en danger dans le cas d'une communication formelle des autorités suisses.

Conformément à l'*al. 3*, la procédure qui s'applique au report de la communication ou qui permet d'y déroger est la même que pour la mesure de recherche soumise à autorisation proprement dite, soit l'autorisation du TAF puis l'aval du chef du DDPS (art. 29).

Aujourd'hui, les acteurs étatiques et non étatiques dans les domaines du terrorisme, de l'espionnage, de l'extrémisme violent, du trafic d'armes, du commerce illégal d'armes chimiques, biologiques et nucléaires de destruction massive et les acteurs dans le domaine du transfert illicite de technologies le sont à un niveau global et ne respectent ni les frontières ni les conventions internationales. Ces acteurs se servent par exemple de la zone Schengen, libre de visa, afin de se rencontrer secrètement dans d'autres pays et d'échapper ainsi aux mesures de surveillance dont ils font l'objet dans leur propre pays. Les services de renseignement de nombreux pays sont confrontés aux mêmes problèmes transfrontaliers et ne sont souvent plus en mesure de rechercher seuls les informations nécessaires.

C'est pourquoi la collaboration avec les autorités nationales et internationales, telle qu'elle est prévue à l'*al. 1*, prend toujours plus d'importance, avant tout dans les domaines de la transmission des informations, des observations transfrontalières, des opérations communes de recherche et des mesures techniques de surveillance. Ces dernières doivent cependant être exécutées conformément au droit suisse, car le SRC ne saurait contourner les prescriptions applicables aux mesures de recherche soumises à autorisation en collaborant avec des services étrangers.

L'*al. 2* règle les mandats exceptionnellement confiés à des particuliers, qui ont également la possibilité de rechercher des informations par le biais d'enregistrements vidéo et sonores. Afin de pouvoir confier un tel mandat, une condition doit obligatoirement être remplie, à savoir que sans l'engagement de ces particuliers, le SRC ne pourrait que très difficilement acquérir l'information recherchée, voire pas du tout. Pour accéder à un groupe de personnes donné à des fins de recherche de renseignements, il se peut par exemple que seul l'engagement d'un informateur (en lieu et place d'un collaborateur du SRC) permette d'installer un appareil technique. Plus une personne se fond discrètement dans un environnement, plus le succès de la recherche d'information devient probable.

Les appareils techniques de surveillance d'une grande complexité qui ne peuvent être exploités que par des entreprises privées spécialisées font ainsi partie des mesures de recherche visées à l'al. 2. Le SRC peut également faire appel à des spécialistes en informatique privés pour des réseaux de données hautement protégés.

Le SRC doit s'assurer auprès de tous les mandataires visés aux al. 1 et 2 qu'ils remplissent leur mandat dans le respect de la loi et il doit les surveiller dans l'accomplissement de ce mandat aussi étroitement que ses propres collaborateurs. Lors de l'attribution du mandat, il consignera par écrit certains points tels que la sauvegarde du secret, les droits de contrôle du SRC et du Préposé fédéral à la protection des données et à la transparence sur l'utilisation des données, l'interdiction de l'usage des données à d'autres fins ou les mesures visant à garantir la sécurité des informations. Les points 'qu'il est nécessaire de régler dépendent du type de mandat.

Le SRC ne transmet pas de mandats formels aux services officiels étrangers: il leur transmet des demandes dans le cadre de la collaboration établie avec eux. Conformément à l'art. 69, al. 1, let. f, le Conseil fédéral règle chaque année la collaboration entre le SRC et les autorités étrangères.

Les éventuelles prétentions que les particuliers qui collaborent avec le SRC élèvent contre la Confédération sont régies par la loi du 14 mars 1958 sur la responsabilité[29].

Art. 34 Protection des sources

La préservation de la protection des sources est de la plus grande importance pour un service de renseignement. Les sources ne doivent être révélées que dans des cas exceptionnels, lorsque l'intérêt public prime largement la révélation. Certaines sources doivent même être protégées de manière rigoureuse. Dans le cas contraire, la confiance dans la discrétion du SRC serait diminuée et la recherche d'informations beaucoup plus difficile.

Le droit actuel ne contient qu'une réglementation très rudimentaire pour la protection des sources, à l'art. 7 LFRC, en la déléguant au Conseil fédéral. Ce dernier est d'avis que la codification complète du renseignement doit aussi contenir une réglementation plus détaillée sur la protection des sources, ce qui permettra également d'éviter des contradictions entre les ordonnances spécifiques d'exécution et les dispositions d'autres actes.

L'*al. 1* définit le principe de la protection des sources et de la nécessité particulière de protéger des personnes qui recherchent des informations à l'étranger, laquelle figurait déjà à l'art. 7 LFRC. Cet alinéa englobe également les relations avec des services de renseignement étrangers et les autorités de sûreté étrangères: s'ils n'étaient pas complètement protégés, la Suisse serait considérée comme un partenaire non fiable et la crédibilité du SRC comme partenaire de coopération pourrait être largement entamée. Les personnes condamnées pour des crimes contre l'humanité (art. 264 et 264*a* CP) ou des crimes de guerre (art. 264*b* à 264*j* CP) ne bénéficieront en revanche d'aucune protection. La protection des sources ne s'applique pas en effet lorsqu'une procédure a été ouverte à l'encontre de la personne par un tribunal suisse ou un tribunal international reconnu par la Suisse ou lorsque la Suisse est tenue à l'entraide judiciaire internationale.

L'*al. 2* limite la protection des informateurs (art. 15) domiciliés en Suisse face aux autorités de poursuite pénale. Ces personnes ne bénéficient d'aucune protection si elles sont accusées d'un délit poursuivi d'office ou si la divulgation de leur identité est indispensable pour élucider une infraction grave. Il n'existe aucune définition juridique formelle générale de la notion d'infraction grave dans le droit pénal et le droit de procédure pénale. Il n'existe pas non plus de critères généraux permettant d'identifier des infractions graves. La qualification d'une infraction dépend du contexte. La définition qui en est donnée à l'art. 11, al. 3, de l'ordonnance du 12 novembre 2008 sur l'usage de la contrainte[30] pourrait toutefois constituer une première piste:

[3] Par infraction grave, on entend une sérieuse atteinte à la vie, à l'intégrité corporelle, à la liberté, à l'intégrité sexuelle ou à la sécurité publique.

L'*al. 3* énumère quels critères doivent être utilisés pour la protection des sources. À cet égard, c'est toujours le maintien de la source à des fins de recherche d'informations qui prime. Conformément aux règles générales régissant l'élaboration du droit d'application, le Conseil fédéral règle les spécificités dans une ordonnance.

29 RS **170.32**
30 RS **364.3**

Le Conseil fédéral estime judicieux de ne prévoir qu'une seule instance dans la loi pour l'examen des litiges dans le domaine du SRC, afin qu'elle puisse acquérir les connaissances techniques nécessaires en matière de renseignement. Il propose par conséquent de désigner à l'*al. 4* le Tribunal administratif fédéral comme instance de décision pour la protection des sources. Le renvoi à l'entraide judiciaire ne concerne que les affaires internes. L'entraide judiciaire internationale relève de la compétence des autorités judiciaires, et non du service de renseignement.

Art. 35 Dispositions générales

Remarques liminaires

La recherche d'informations relatives à des événements se produisant à l'étranger se fonde aujourd'hui sur une disposition générale figurant à l'art. 1, let. a, LFRC:

Le Conseil fédéral désigne les services fédéraux chargés des missions du renseignement civil. Ces services:

a. recherchent et évaluent à l'intention des départements et du Conseil fédéral des informations sur l'étranger importantes en matière de politique de sécurité;

Cette réglementation remonte à l'ancien art. 99, al. 1, de la loi sur l'armée (LAAM). Elle a été formulée de manière très générale dans la LFRC, puisque cette dernière avait uniquement pour but de réunir les bases juridiques existantes relatives au service de renseignement civil, sans mettre en place de nouveaux obstacles. La LFRC a donc repris la réglementation de la LAAM, qui entendait donner une grande marge de manœuvre au service de renseignement pour la recherche d'informations à l'étranger et qui n'entendait pas dévoiler à l'étranger les méthodes et possibilités de recherche d'informations utilisées par l'ancien Service de renseignement stratégique.

L'art. 16 OSRC décrit plus précisément les méthodes autorisées aujourd'hui pour rechercher des renseignements à l'étranger.

La recherche de renseignements sur l'étranger depuis la Suisse est soumise en principe aux mêmes règles que celles applicables à la recherche en Suisse (al. 2).

La recherche de renseignements à l'étranger fonctionne en revanche selon d'autres règles que celles applicables à la recherche en Suisse. Le SRC engage en effet les mesures de recherche à l'étranger sous sa propre responsabilité, y compris celles qui seraient soumises à autorisation en Suisse (art. 25 ss).

La réglementation différente de la recherche d'informations en Suisse par rapport à celle à l'étranger correspond à la pratique de la plupart des services de renseignement dans le monde et découle du fait que les activités étatiques de recherche de renseignements dans d'autres pays sont en règle générale considérées comme de l'espionnage et poursuivies pénalement. Les délits d'espionnage ne sont en revanche pas soumis à l'entraide judiciaire internationale. Le Conseil fédéral est donc d'avis qu'il n'est pas judicieux de soumettre la recherche d'informations à l'étranger à une procédure d'autorisation judiciaire ou politique. L'autorisation ne pourrait de toute manière avoir aucun effet juridique ou politique à l'étranger, mais pourrait être considérée par l'État visé comme une atteinte illégale à sa souveraineté par des autorités judiciaires et politiques suisses. La recherche d'informations à l'étranger est par ailleurs soumise aux conditions suivantes:

– la substance des droits fondamentaux doit être respectée et les atteintes aux droits fondamentaux des personnes doivent être limitées au strict nécessaire (al. 3);

– les activités de recherche doivent être documentées soigneusement à l'intention des organes de surveillance et de contrôle (al. 4);

– le DDPS, le Conseil fédéral et la Délégation des Commissions de gestion des Chambres fédérales exercent un contrôle (voir les art. 74 ss).

Dans ces conditions, les activités du SRC prévues dans le projet de loi sont conformes aux obligations internationales de la Suisse.

L'*al. 1* énonce le principe selon lequel les activités de recherche à l'étranger se déroulent en secret. Sans secret, les États ou les acteurs concernés pourraient empêcher ces activités, ce qui pourrait mettre en péril aussi bien les collaborateurs que les sources du SRC.

L'*al. 2* autorise le SRC à prendre d'autres mesures de recherche d'informations sur l'étranger en Suisse (par ex. des rencontres avec des informateurs), mais impose le respect des règles appliquées à la recherche d'informations en Suisse. Cette disposition s'applique en particulier à la mise en œuvre de mesures de recherche soumises à autorisation (section 4), à l'exception des activités particulières visées à l'art. 36 (Introduction dans des systèmes et des réseaux informatiques à l'étranger).

Le SRC engage donc les mesures de recherche secrètes à l'étranger sous sa propre responsabilité, y compris celles qui seraient soumises à autorisation en Suisse selon les art. 25 et suivants. La raison pour laquelle la solution appliquée pour l'engagement des mesures de recherche à l'étranger diffère de celle utilisée pour la recherche en Suisse réside aussi dans le fait que les collaborateurs du SRC qui s'occupent de la recherche de renseignements à l'étranger ont besoin d'une plus grande liberté d'action et de jugement dans le choix des moyens leur permettant de remplir leurs missions.

Le Conseil fédéral propose dès lors de ne pas soumettre à une procédure d'autorisation particulière les mesures de recherche secrètes que le SRC peut mettre en œuvre à l'étranger. En règle générale, en effet, les tribunaux suisses ne peuvent pas connaître les conditions prévalant sur place et ne peuvent pas se procurer dans des délais raisonnables les informations nécessaires à une prise de décision. Il n'est donc pas possible de prévoir une procédure ordinaire d'autorisation (qui constituerait de toute manière un cas unique à l'échelon international). Au surplus, une des plus hautes juridictions suisses devrait déclarer licites des mesures que les pays dans lesquels elles sont effectuées considèrent souvent comme répréhensibles. Comme le dispose expressément *l'al. 3*, le principe de la proportionnalité doit cependant aussi être respecté dans la mise en œuvre de mesures de recherche d'informations à l'étranger. L'atteinte aux droits fondamentaux d'une personne ne doit pas être disproportionnée par rapport au bénéfice escompté. Aux termes des dispositions de la Constitution, toutes les autorités doivent respecter l'essence des droits fondamentaux et le SRC ne saurait en être dispensé lorsqu'il recherche des informations sur l'étranger.

Le fait que le SRC peut mettre en œuvre en grande partie sous sa propre responsabilité des activités de recherche d'informations sur l'étranger ne signifie pas l'abandon d'un contrôle efficace. Au contraire: l'*al. 4* oblige le SRC à documenter l'ensemble de ses recherches d'informations sur les événements se produisant à l'étranger à

pour que le Conseil fédéral, le Parlement (Commission de gestion, respectivement Délégation des Commission de gestion des Chambres fédérales) et le DDPS (Surveillance des services de renseignement) puissent exercer une surveillance politique sur le SRC.

Les données collectées à l'étranger avec des méthodes similaires aux mesures de recherche soumises à autorisation (par ex. l'engagement d'appareils de localisation GPS) sont comparables aux données issues de mesures de recherche soumises à autorisation en Suisse quant à l'ampleur des données récoltées, le secret que requièrent les mesures ou les risques qu'elles impliquent pour la sécurité (par ex. la présence de maliciels dans les données collectées sur des ordinateurs). Comme prévu à l'*al. 5*, ces données peuvent être enregistrées dans des systèmes d'information distincts, au même titre que les données comparables collectées en Suisse (voir art. 57). Une fois traitées, elles peuvent être transférées dans d'autres systèmes si les conditions requises pour leur enregistrement sont remplies. Ce transfert s'opérera principalement vers le système d'analyse intégrale (art. 48).

Les collaborateurs du SRC engagés à l'étranger sont exposés à un risque accru et séjournent aussi dans des régions en guerre et en crise, parfois sous couverture et identité d'emprunt. L'*al. 6* prévoit dès lors de les soumettre à l'assurance militaire.

Les mesures de protection prévues à l'*al. 7* peuvent prendre la forme d'équipements techniques, mais aussi de couvertures et d'identités d'emprunt ou encore d'un appui opérationnel, par ex. l'engagement de mesures de contre-observation visant à identifier rapidement les menaces existantes dans le cadre d'une intervention.

Art. 36 Introduction dans des systèmes et des réseaux informatiques

L'*art. 36* régit certains cas particuliers de la recherche d'informations sur l'étranger. L'*al. 1* règle ainsi l'introduction depuis la Suisse dans des systèmes et des réseaux informatiques qui se trouvent à l'étranger dans le but de perturber, empêcher ou ralentir l'accès à des informations (voir art. 25, al. 1, let. d, ch. 2). L'exercice de conduite stratégique 2013 a montré que de telles mesures sont sensibles du point de vue de la politique extérieure et qu'elles ne peuvent de ce fait relever de la seule compétence du SRC: elles ne doivent être effectuées que sur décision du Conseil fédéral et uniquement si les systèmes étrangers correspondants sont utilisés pour des attaques contre des infrastructures critiques. Pour les raisons indiquées au commentaire de l'art. 35, le Conseil fédéral est d'avis qu'une autorisation judiciaire n'est pas judicieuse.

L'*al. 2* règle l'introduction depuis la Suisse dans des systèmes et des réseaux informatiques qui se trouvent à l'étranger en vue d'y rechercher des informations (voir art. 25, al. 1, let. d, ch. 1). L'élément qui motive l'intérêt de la recherche doit être situé à l'étranger (par ex. le programme de prolifération d'un État étranger). Comme les systèmes étrangers ne doivent dans ce cas ni être perturbés ni ralentis, les risques en matière de politique extérieure sont beaucoup plus faibles que dans le cas de mesures prises en vertu de l'al. 1. Le SRC doit donc être autorisé à mettre en œuvre une telle recherche depuis la Suisse et sous sa propre responsabilité, d'autant que les services de renseignement étrangers y ont recours de manière intensive. Toutefois, s'il y a lieu de craindre des risques politiques particuliers, le directeur du SRC devra préalablement obtenir l'aval du chef du DDPS.

Art. 37 Exploration radio

En adoptant l'art. 4*a* LFRC, les Chambres fédérales ont créé dans le cadre de la révision LMSI II une nouvelle disposition légale qui règle pour la première fois à ce niveau l'exploration radio à des fins de renseignement. Cette disposition n'est entrée en vigueur que le 1er novembre 2012, après l'adaptation de l'ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio[31]. Le Conseil fédéral l'a donc reprise telle quelle ou presque dans la LRens, avec quelques légères adaptations d'ordre terminologique et relatives au champ d'application de la présente loi. C'est ainsi que la sauvegarde d'intérêts essentiels de la Suisse sur mandat direct du Conseil fédéral (voir art. 3 et 70) a été intégrée aux conditions pouvant présider à l'engagement de l'exploration radio (al. 2).

L'exploration radio est axée sur l'étranger, ce qui veut dire qu'elle ne peut porter que sur les systèmes radio qui se trouvent à l'étranger. En pratique, cela concerne avant tout les satellites de télécommunications et les émetteurs à ondes courtes. Le service chargé de l'exécution de l'exploration radio est le Centre des opérations électroniques de l'armée suisse (COE), qui est le seul à disposer des infrastructures techniques nécessaires. L'al. 4 garantit que les émissions radio ne puissent être exploitées que si leur contenu a un lien avec l'étranger. Il est tout à fait possible que des informations sur des personnes qui se trouvent en Suisse soient récoltées, notamment lorsque l'interlocuteur d'une personne ou d'un équipement étranger faisant l'objet d'une telle mesure utilise un raccordement de télécommunications suisse. Le COE ne peut transmettre ces informations au SRC qu'après les avoir rendues anonymes si elles n'indiquent pas de menace concrète pour la sûreté intérieure (al. 5). La LFRC renvoie ici au traitement ultérieur au sens de la LMSI. Dans la LRens, les menaces en question sont celles qui figurent à l'art. 6, al. 1, let. a.

L'exploration radio est déjà contrôlée par un organe indépendant. Ici aussi, le Conseil fédéral reprend sans grand changement dans la LRens (art. 75) les dispositions correspondantes de la LFRC (art. 4*b*). Aux termes de l'al. 3, le Conseil fédéral règle les modalités de l'exploration radio: l'al. 3 ne fixe que la teneur minimale de l'ordonnance. Comme jusqu'à présent, le Conseil fédéral y inscrira d'autres dispositions, telles que les règles relatives au traitement des données imparties au service chargé de cette tâche ou celles relatives à la sécurité des données.

La LRens reprend ainsi la réglementation et la pratique de la LFRC et de la LMSI. A l'époque, le professeur Giovanni Biaggini, professeur de droit public, administratif et européen à l'Université de Zurich, a largement participé aux travaux d'élaboration de la LMSI à la demande des Chambres fédérales. Les présentes dispositions de la LRens et de la section 7 ci-après concernant l'exploration du réseau câblé ont à nouveau été élaborées avec la collaboration du professeur Biaggini.

Art. 38 Dispositions générales

Outre l'exploration radio, pratiquée en Suisse comme à l'étranger, l'exploration du réseau câblé gagne en importance à l'échelle internationale. Comme elle doit être mieux réglementée, elle a fait l'objet d'une section distincte dans le présent projet, mais elle relève également de la recherche d'informations sur des événements survenant à l'étranger. L'exploration radio d'événements survenant en Suisse continuera d'être interdite.

31 RS **510.292**

Au cours de ces dernières années, avec l'élargissement des réseaux très performants de fibre optique, les télécommunications passent de plus en plus de moyens sans câble (radio) à des réseaux reliés par des conduites (appelées ci-après «câble» par souci d'intelligibilité). Parallèlement, les possibilités d'obtenir des résultats à partir de l'exploration radio diminuent quelque peu. L'avant-projet se fondait en partie sur une législation similaire que la Suède avait édictée en 2008 (loi 2008:717 sur l'exploration des signaux au sein du Service de renseignement militaire, qui possède en Suède la fonction de service de renseignement sur l'étranger) et qui règle également l'exploration du réseau câblé. Il ne sera en effet possible de procéder en Suisse à des examens techniques plus approfondis et à des tests que lorsque les bases légales nécessaires seront entrées en vigueur. La faisabilité purement technique est assurée, comme nous le montre l'étranger. Ce n'est toutefois qu'en analysant les flux de données à travers la Suisse qu'il sera possible de déterminer si l'exploration du réseau câblé permet également d'obtenir en Suisse des informations suffisamment utiles. Une base légale formelle est toutefois nécessaire pour procéder à une telle exploitation.

À l'instar de l'exploration radio, l'exploration du réseau câblé sert à rechercher des informations sur l'étranger et n'est dès lors pas conçue comme une mesure de recherche soumise à autorisation. Pour atteindre des objectifs d'exploration similaires ayant trait à la Suisse, une mesure de recherche soumise à autorisation devrait être demandée. L'exploration du réseau câblé ne peut toutefois être exécutée qu'avec la participation de prestataires suisses de services de télécommunication et ceux-ci doivent disposer d'un ordre juridiquement valable pour transmettre au COE les flux de données correspondants. Étant donné qu'une procédure de recours par les personnes visées par la mesure d'exploration n'est pas possible ici, la loi prévoit une procédure d'autorisation similaire à celle utilisée pour les mesures de recherche soumises à autorisation en Suisse (art. 28). Le traitement des données se fait toutefois différemment, en ce sens qu'il n'a pas lieu dans des systèmes séparés, mais dans le système de stockage des données résiduelles et dans le système d'analyse intégrale (art. 46 ss), comme pour les données issues de l'exploration radio.

Dans l'exploration du réseau câblé, certains flux de données sont interceptés sur des câbles de télécommunication internationaux et, comme pour l'exploration radio, ils sont examinés, triés et exploités selon leur contenu. Contrairement à la surveillance des télécommunications en Suisse, qui est une mesure de recherche soumise à autorisation, l'exploration du réseau câblé est un instrument de recherche d'informations à l'étranger et n'est pas prévue pour enregistrer tout le trafic de télécommunication de certains raccordements: cela n'est d'ailleurs pas possible sur le plan technique de la même manière que pour la surveillance des télécommunications en Suisse, puisque la cible se trouve à l'étranger.

La Suisse ne dispose encore d'aucune base juridique pour ces moyens d'exploration. Il s'agit en effet d'une forme d'exploration nouvelle, axée sur l'étranger, qui n'est pas comparable aux formes de surveillance prévues dans la LSCPT. Les terminologies ne doivent et ne peuvent dès lors pas être identiques et elles ne doivent pas trop étroitement s'inspirer des notions techniques existantes, afin de ne pas exclure les évolutions techniques.

Comme pour l'exploration radio, le service chargé de l'exécution visé à l'*al. 1* est le COE, qui dispose des compétences techniques ainsi que des équipements nécessaires. Afin de protéger les droits fondamentaux des personnes dont les données de communication sont enregistrées mais qui ne répondent pas aux critères de re-

cherche dictés par le mandat du SRC, il est indispensable que le triage des données soit effectué non par le SRC, mais par un organe tiers. Comme pour l'exploration radio, le COE ne transmet au SRC que les données qui correspondent à un mandat de recherche ou qui contiennent des indices directs de mise en danger de la sûreté intérieure ou extérieure. Ces critères ainsi que les procédures correspondent largement à la pratique de l'exploration radio. Une participation du SSCPT, qui est rattaché au DFJP, n'est ni nécessaire ni judicieuse puisque l'exploration du réseau câblé n'est pas un type de surveillance que ce service propose en vertu de la LSCPT. Le COE, en tant que service compétent, prendra directement contact avec les exploitants de réseaux câblés et les fournisseurs de prestations de télécommunications pour planifier et exécuter l'exploration dans des cas concrets.

L'*al. 2* garantit qu'aucune communication purement suisse ne soit enregistrée. Lorsque cela n'est pas possible techniquement (par ex. lorsque le cheminement de lots de données IP ne peut pas être prédit, même si l'expéditeur et le destinataire se trouvent en Suisse), de telles données doivent être détruites dès que leur origine suisse et leur adresse cible suisse ont été identifiées. Cette contrainte s'applique tant au COE qu'au SRC.

L'*al. 3* définit les prescriptions applicables aux termes de recherche que le SRC définit pour le mandat. Ceux-ci doivent être formulés de manière aussi précise que possible, afin le volume des données enregistrées et que les atteintes à la sphère privée des personnes concernées soient aussi faibles que possible. En d'autres termes, il est par exemple plus efficace et plus mesuré de faire des recherches sur l'identité concrète de personnes étrangères soupçonnées d'activités terroristes ou sur les raccordements de télécommunications que ces dernières utilisent que d'utiliser un mot de recherche aussi simple que «Al-Qaïda» ou «attentat à l'explosif». L'exploration radio dispose à cet égard d'une pratique éprouvée qui est, juridiquement correcte et contrôlée.

Comme l'al. 3 le prévoit pour l'exploration radio, l'*al. 4* charge le Conseil fédéral d'édicter le droit d'application par voie d'ordonnance.

Art. 39 et 40 Obligation d'obtenir une autorisation et procédure d'autorisation

Par analogie avec les mesures de recherche soumises à autorisation, ces articles règlent l'autorisation des mandats d'exploration du réseau câblé. Étant donné que les fournisseurs de télécommunications doivent recevoir l'ordre de transmettre certains flux de données et que les personnes concernées n'ont aucune possibilité de s'y opposer, un contrôle judiciaire est nécessaire. C'est pourquoi l'organe de contrôle indépendant pour l'exploration radio n'intervient pas non plus dans ce cas. S'il le faisait les autorités d'approbation, de contrôle et de surveillance seraient en concurrence les unes avec les autres et seraient mal délimitées.

La demande visée à l'*art. 40, al. 1,* doit également contenir les catégories de termes de recherche sur la base desquelles les données doivent être sélectionnées pour le SRC. Les expériences faites avec l'exploration radio montrent que ces termes de recherche doivent être traités de manière dynamique et peuvent être régulièrement affinés. Il est dès lors prévu de travailler également avec des catégories de termes de recherche, afin qu'une nouvelle approbation ne doive pas être obtenue à chaque fois que les termes de recherche sont précisés. Un groupe de membres d'une organisation terroriste donnée peut par exemple constituer une catégorie de termes de recherche, ainsi que les personnes ayant un contact opérationnel avec ces derniers. Ces per-

sonnes ne peuvent être identifiées nommément qu'au cours de l'exploration. Les indications se rapportant aux éléments d'adressage relevant de la technique de télécommunication (par ex. numéros de téléphone), les adresses ou les désignations de dossiers et de projets par exemple sont des termes de recherche précis qui ne sont définis que lorsque la mesure est exécutée.

Contrairement aux mesures de recherche soumises à autorisation, qui ne peuvent être autorisées que pour une durée de trois mois tout en étant renouvelables, l'exploration du réseau câblé doit pouvoir être autorisée pour une durée de six mois lors du premier mandat (*al. 3*). Une telle mesure se justifie par le fait que l'enregistrement de la saisie ainsi que la formation et l'intégration des collaborateurs qui procèdent au triage dans un mandat nécessitent plus de temps que par exemple pour une surveillance des télécommunications au sens de l'art. 25, al. 1, let. a (où le SRC reçoit toutes les communications surveillées). Le même délai que pour les mesures de recherche soumises à autorisation s'applique en revanche à la prolongation des mesures, soit trois mois.

Art. 41 Mise en œuvre

L'exécution est similaire à la procédure utilisée pour l'exploration radio, à l'exception du fait que le service chargé de l'exploration du réseau câblé n'enregistre pas lui-même (à l'aide d'antennes) les signaux des installations de télécommunication, mais les obtient des fournisseurs de télécommunications. Les fournisseurs concernés doivent être déterminés dans chaque cas en fonction de des voies de transit à travers la Suisse.

La suite de la procédure et les critères dictant le choix des données qui doivent être transmises au SRC se fondent pour l'essentiel sur les règles applicables à l'exploration radio (al. 2 à 5).

Le SRC est responsable de l'exploitation des données sur le plan du renseignement. Il décide également quelles données sont déposées conformément aux bases légales dans ses systèmes d'information pour y être traitées (voir le chap. 4). Le COE pourra assortir les données transmises d'explications techniques ou matérielles, de résumés ou de traductions, comme il l'a fait jusqu'ici.

Art. 42 Obligations des exploitants de réseaux câblés et des opérateurs de télécommunications

Etant donné que l'exploration du réseau câblé ne peut être effectuée qu'avec la participation des opérateurs de télécommunication et des exploitants de réseaux câblés, l'art. 42 fixe les obligations auxquelles ils sont soumis dans ce cadre. Seuls les exploitants proposant des prestations publiques en matière de trafic transfrontalier au sens de la LTC y sont toutefois soumis. Les renseignements techniques sont notamment nécessaires pour formuler les différents mandats et les demandes adressées aux instances d'approbation. Leur délivrance n'est donc pas limitée à l'exécution concrète d'un mandat autorisé et avalisé. En règle générale, les questions techniques devront être clarifiées entre le COE et les fournisseurs. Afin de justifier et documenter ses mandats, le SRC a toutefois également besoin de renseignements directs de la part des fournisseurs de services de télécommunication et des exploitants de réseaux câblés.

Comme mentionné plus haut, une participation du SSCPT, qui est rattaché au DFJP, n'est pas prévue, puisque l'exploration du réseau câblé n'est pas un type de surveillance que ce service propose en vertu de la LSCPT. Les modalités techniques devront être clarifiées directement entre le SRC, le COE et les exploitants pour chaque cas.

À l'heure actuelle, par manque d'expérience, il n'est pas possible d'estimer le temps nécessaire pour la réalisation de l'exploration du réseau câblé. On ne sait notamment pas exactement quels flux de données pertinents sur le plan du renseignement transitent aujourd'hui et transiteront à l'avenir à travers la Suisse. Comme mentionné plus haut, ces informations ne pourront être récoltées que lorsque les bases légales seront entrées en vigueur.

Lors de la consultation, les fournisseurs ont demandé une pleine indemnisation de leurs coûts. Or, la révision en cours de la LSCPT maintient la réglementation actuelle (indemnisation adéquate des fournisseurs pour l'utilisation de leur infrastructure de surveillance); ce principe doit aussi être repris dans le cas présent. Il n'y aurait dans le cas contraire aucune incitation pour les fournisseurs à rechercher des solutions économiques. L'aménagement concret des indemnités dans l'ordonnance sera encore discuté avec les fournisseurs.

Le Conseil fédéral estime que les préparatifs concrets de l'exploration du réseau câblé et les premières exploitations test de la part du SRC et du COE exigeront dans un premier temps deux postes supplémentaires au sein de chacune de ces entités. Ces postes seront demandés dans les planifications ordinaires du personnel.

Chapitre 4, section 1

Pour s'acquitter des tâches que la présente loi lui confie, à savoir la détection précoce et l'appréciation globale des menaces pesant sur la sûreté intérieure ou extérieure de la Suisse, le SRC a besoin comme n'importe quel service de renseignement d'une base d'information aussi large que possible, alimentée par des sources aussi variées que possible.

Les attentats, les activités d'espionnage et les activités extrémistes violentes, par ex., sont généralement préparés en secret et le restent aussi longtemps que possible. Comme ils peuvent entraîner des dommages considérables, leur détection précoce et leur neutralisation sont de la plus haute importance. C'est pourquoi le traitement de l'information doit intervenir à un moment où il n'existe encore aucun soupçon juridiquement suffisant de préparation ou de l'existence d'une infraction. Ces menaces, le SRC doit les rechercher activement et les neutraliser en collaboration avec les autres autorités.

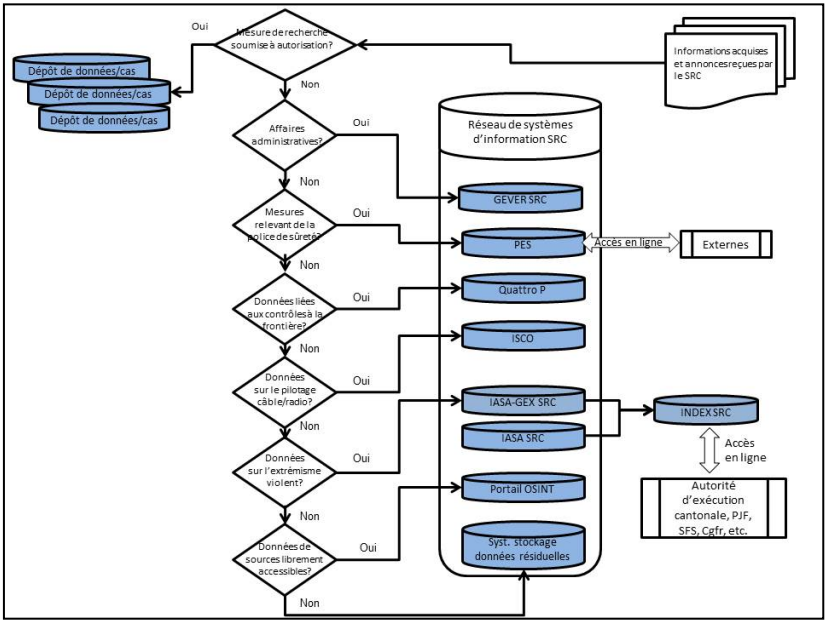
La présente loi renonce logiquement à la séparation entre sûreté intérieure et sûreté extérieure, devenue obsolète, de sorte que cette distinction ne joue pas non plus de rôle déterminant pour le traitement des données par le SRC.

Le SRC est a en revanche besoin d'une réglementation uniforme de la saisie, de la conservation et de l'exploitation des données, afin de réaliser le gain en efficacité visé par la fusion des deux services qui l'ont précédé et l'exploitation intégrale des données relevant du renseignement. A cet égard, il y a lieu de tenir compte de manière adéquate des points qui ont fait leur preuve dans la longue pratique suivie par les services de renseignement avec les bases légales actuelles (LMSI et la LFRC).

Le présent projet prévoit que les informations qui sont collectées par le SRC ou qui lui sont communiquées soient saisies dans des systèmes d'information intégrés en fonction de la thématique, de la source et de la sensibilité des données. Le SRC ne peut pas collecter et conserver des données en vrac. Celles-ci doivent toujours avoir un lien suffisant avec les tâches qui lui incombent en vertu de la loi. Le SRC doit de plus tenir compte des restrictions de traitement pour les données relatives à l'exercice des droits politiques (art. 5, al. 5 à 8). Enfin, il doit s'assurer que la pertinence et l'exactitude des données soient vérifiées avant leur enregistrement dans les systèmes d'information. Cette vérification doit intervenir avant que des données personnelles n'aient un impact à l'extérieur, à savoir lorsqu'elles sont utilisées dans le cadre d'un produit du SRC (par ex. un rapport d'analyse, une annonce à un service de renseignement étranger, une appréciation de la situation).

Les données que le SRC reçoit par le biais d'une mesure de recherche soumise à autorisation ou par suite de contrôles à la frontière sont traitées spécialement et ne sont accessibles qu'aux spécialistes au sein du SRC.

Les différents systèmes d'information du SRC permettent une réglementation différenciée de la conservation des données. Alors que le traitement des données n'a par exemple presque jamais donné lieu à des critiques dans le domaine de la lutte contre l'espionnage, de la non-prolifération ou de la protection des infrastructures critiques, celui touchant au domaine de l'extrémisme violent s'est toujours avéré particulièrement sensible, tant sur le plan politique que sur celui de la protection des données. Les conditions les plus strictes en matière de traitement des données sont donc prévues pour ce domaine hautement sensible, comme c'est le cas dans la LMSI (contrôle systématique de la qualité à intervalles rapprochés). Les conditions applicables aux données issues de sources publiquement accessibles sont en revanche moins strictes (vérification moins fréquente, durée de conservation plus longue, cercle plus large de personnes ayant accès aux données), puisque de telles données pourraient en règle générale être déduites des sources d'origine, même si elles sont structurées différemment et que leur disponibilité est moins grande.



Art. 43 Principes

Les principes fixés à l'art. 43 valent pour tous les systèmes d'information du SRC, ce qui permet de garantir un standard uniformément élevé de la qualité du traitement des données, indépendamment du système dans lequel les données personnelles sont enregistrées. Les systèmes peuvent contenir des données sous la forme de textes, de sons, d'images ou d'autres formats appropriés.

Pour s'acquitter de ses tâches, le SRC reste tributaire du traitement de données sensibles telles que l'appartenance religieuse pour les terroristes à motivation fondamentaliste, l'exécution de peines d'emprisonnement ou l'état de santé de figures d'identification ou de politiciens étrangers. Il établit et traite des profils de personnalité, par ex. dans le but d'évaluer la menace que posent des extrémistes violents agissant seuls ou en groupes. L'*al. 1* crée la base légale formelle nécessaire au traitement de ces données.

Contrairement aux conditions habituelles en matière de protection des données, le SRC doit aussi pouvoir conserver les données qui s'avèrent inexactes et exploitées comme telles, conformément à l'*al. 2*. En ce qui concerne l'appréciation d'informations relevant du renseignement, il doit identifier la désinformation et les fausses informations. De telles informations permettent de déterminer les intentions des producteurs et des fournisseurs d'informations. Une fois reconnue comme telle, une désinformation ou une fausse information doit rester disponible afin de ne pas provoquer d'erreurs d'interprétation ultérieurement. De même, il doit être possible d'accéder aux fausses informations identifiées dans le cadre de la collaboration internationale, afin d'apprécier correctement la transmission ultérieure de fausses informations (par ex. identification erronée d'une personne comme membre d'un

groupement terroriste) et, le cas échéant, de réagir en conséquence. Les données identifiées comme incorrectes peuvent par ailleurs être utiles pour l'évaluation de la fiabilité, de l'honnêteté ou des intentions d'un informateur ou d'un service de renseignement étranger. La désignation claire de telles données permet d'éviter qu'elles soient traitées par erreur comme des données correctes.

Les systèmes d'information du SRC constituent un réseau et visent tous à permettre au SRC de remplir les tâches qui lui sont confiées par la loi. Souvent, les données doivent être transférées dans un autre système à cet effet. L'analyste qui doit rédiger un rapport sur un groupement terroriste est par exemple tributaire des annonces faites par des services de sûreté étrangers, des articles de presse, des entrées constatées en Suisse, etc. Il ne peut exécuter son travail d'analyse et l'étayer dans le système d'information prévu à cet effet que lorsqu'il a rassemblé les données nécessaires dans ce système. Comme ces mêmes données peuvent encore servir d'autres desseins dans le système d'origine ou que seule une partie d'une annonce suffit souvent à l'établissement d'un produit donné, l'annonce en question doit systématiquement rester dans le système d'origine, où elle est à la disposition d'autres utilisateurs et où on vérifie régulièrement sa pertinence et son exactitude (voir à cet égard l'art. 44, Contrôle de qualité). Les données peuvent ainsi être copiées d'un système à l'autre et sont soumises aux prescriptions respectives des différents systèmes d'information.

La mise en réseau des données dans les systèmes, déjà pratiquée dans les systèmes ISIS et ISAS, améliore la qualité de l'enregistrement et des possibilités d'exploitation par rapport à un simple archivage d'objets individuels. Elle permet ainsi de saisir et de représenter efficacement les relations entre les personnes et avec des événements. L'*al. 4* crée la base légale expresse pour de telles mises en réseau et l'usage de programmes automatisés de recherche et d'exploitation.

Art. 44 Contrôle de qualité

Divers rapports d'organes de surveillance ont montré à quel point un contrôle de qualité fiable et exploitable est important pour la qualité des données du SRC. La mise en place d'un organe de contrôle de qualité interne au SRC a fait ses preuves et doit à présent également être inscrite dans la loi. Les moyens servant à contrôler la qualité sont engagés de manière ciblée, par analogie avec le modèle différencié de saisie des données:

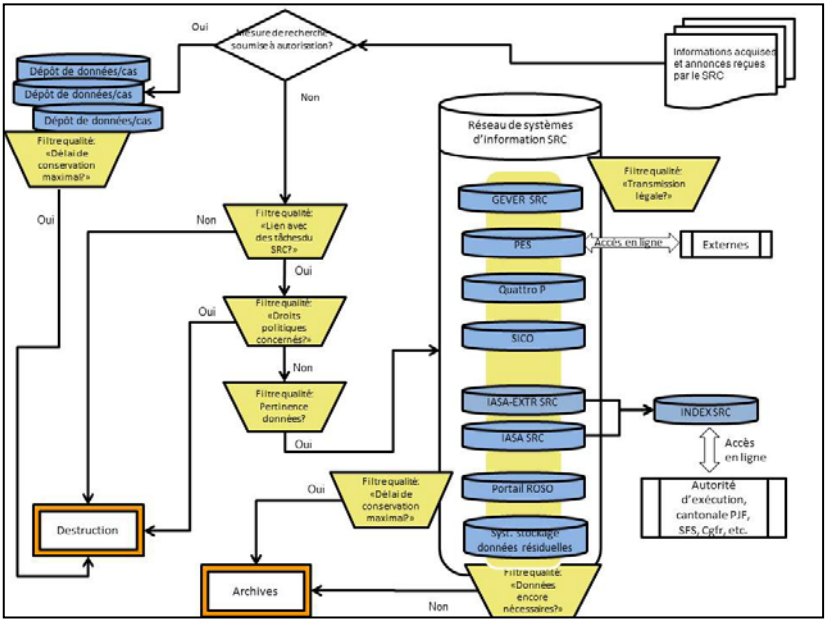
– Un contrôle immédiat et complet est assuré par l'organe interne de contrôle de la qualité pour le traitement des données relevant de l'extrémisme violent (al. 5, let. a) et pour la saisie des rapports cantonaux dans l'INDEX SRC (al. 5, let. b). Alors que dans les domaines de l'espionnage, de la prolifération d'armes de destruction massive ou du terrorisme, les observations portent sur des développements qui s'étendent sur plusieurs années, les cycles de qualité des données devraient être beaucoup plus courts dans le domaine de l'extrémisme violent: le risque d'avoir des données dans le système qui sont devenues inutiles est beaucoup plus élevé et exige donc des cycles de contrôle plus courts. Les contraintes actuellement très strictes applicables aux banques de données LMSI cantonales plaident également en faveur d'un contrôle périodique strict et d'un effacement périodique des rapports cantonaux ainsi que des travaux préalables qui y sont liés. La centralisation de la

souveraineté des données à l'échelon fédéral ne doit pas entraîner un assouplissement de ces contraintes.

- Pour tous les autres systèmes d'informations du SRC, ce sont en priorité les utilisateurs qui sont responsables de l'exécution régulière du contrôle de qualité (al. 4). L'organe interne de contrôle de la qualité veille à ce que les filtres de traitement des données prescrits soient utilisés correctement en organisant notamment des formations, en édictant des prescriptions et en procédant à des contrôles. Il est prévu que les collaborateurs ne puissent accéder aux systèmes d'information qu'après avoir réussi l'examen correspondant.
- L'organe interne de contrôle de la qualité effectue de plus des vérifications par sondage dans tous les systèmes, au cours desquelles il vérifie la légalité, l'utilité et l'efficacité du traitement de données. Ces critères se fondent sur ceux des organes de surveillance (art. 73 ss). Les enseignements qui en sont tirés sont intégrés aux cours de formation destinés aux collaborateurs.
- S'agissant du système de stockage des données résiduelles, un contrôle périodique des annonces garantit que seules les annonces qui répondraient aux exigences liées à un nouvel enregistrement restent enregistrées dans le système. On ne vérifie toutefois pas en détail l'ensemble des données personnelles, mais on s'assure que l'annonce soit globalement pertinente et exacte (cf. art. 56, al. 2).

Concrètement, les étapes de triage décrites ci-après permettent de garantir une qualité élevée des données au sein du SRC:

- triage d'entrée: limitation aux données personnelles qui peuvent être traitées sur la base du mandat légal, respect des droits politiques, contrôle de l'exactitude et de la pertinence de toutes les données;
- contrôle périodique: les données enregistrées dans les systèmes d'information du SRC sont régulièrement contrôlées pour déterminer si elles sont encore nécessaires pour l'accomplissement des tâches prévues par la loi (examen de la pertinence); le contrôle porte toujours sur un bloc de données complet, ce qui permet soit de confirmer l'ensemble des données relatives à une personne ou à une organisation, soit de les effacer toutes; un contrôle périodique de ce type est pratiqué depuis longtemps pour le système ISIS; il correspond également aux procédures appliquées par les services partenaires du SRC qui soumettent leurs données à un contrôle périodique;
- triage de sortie: les données personnelles ne peuvent avoir un impact à l'extérieur que si le traitement des données est légal (voir l'art. 58);
- délais de conservation maximaux: le Conseil fédéral détermine le délai de conservation maximal pour chaque système d'information.



Les *al. 1 et 2* définissent l'appréciation effectuée d'entrée par le SRC avant chaque saisie de données dans un système d'information.

L'élément déterminant en vertu de l'*al. 1* est la pertinence et l'exactitude des données personnelles. Dans le système de stockage des données résiduelles, qui n'est pas organisé sur la base d'objets ou de personnes, l'appréciation ne porte pas sur chaque donnée personnelle contenue dans l'annonce, mais sur l'annonce dans son ensemble.

Selon l'*al. 2*, le SRC ne peut traiter des données que si elles ont un lien avec ses tâches légales (art. 6, al. 1). Concrètement, le SRC doit s'assurer lors du contrôle d'entrée et avant toute saisie dans un système d'information que les renseignements et les annonces présentent un lien avec l'extrémisme violent, le terrorisme, l'espionnage, la prolifération d'armes de destruction massives, des attaques visant des infrastructures critiques ou des événements importants du point de vue de la politique de sécurité. Il doit aussi veiller à ce que l'annonce ou les informations ne tombent pas sous le coup des restrictions de traitement relatives à la protection des droits politiques (art. 5, al. 5 à 8).

Les annonces des autorités cantonales d'exécution peuvent leur être renvoyées pour clarification et complément d'information lorsqu'elles ne sont pas suffisantes pour que le SRC puisse les traiter. Si le SRC n'est pas compétent pour traiter ces données, l'expéditeur peut avoir un intérêt propre ou une compétence propre pour traiter l'affaire; dans de tels cas de figure, l'annonce est également renvoyée.

Conformément à l'*al. 4*, le SRC veille à ce que les données personnelles enregistrées dans ses systèmes d'information soient régulièrement contrôlées. Les données dont il n'a plus besoin pour l'exécution de ses tâches sont effacées de ses systèmes pour

être archivées conformément aux prescriptions des Archives fédérales (art. 67). Quelques participants à la procédure de consultation ont demandé l'abandon des saisies multiples (à savoir l'enregistrement de la même personne dans plusieurs systèmes) ou leur contrôle régulier. Le Conseil fédéral considère que de telles restrictions ne sont pas appropriées puisqu'une saisie multiple est par exemple obligatoire dans les systèmes réservés au SRC et dans le système INDEX SRC. Les saisies multiples sont aussi nécessaires et judicieuses en raison de l'architecture des bases de données, qui englobe plusieurs systèmes aux contenus et aux desseins différents. Les données se trouvent ainsi toujours à l'endroit où elles doivent l'être en fonction de leur pertinence tout en étant soumises aux prescriptions applicables au système concerné en matière de vérification et de contrôle de qualité. Si ces prescriptions sont respectées, un contrôle supplémentaire des saisies multiples ne conduira pas à des appréciations différentes.

Art. 45 Traitement des données par les cantons

L'*al. 1* se fonde sur l'idée suivante: tant que les autorités cantonales d'exécution interviennent dans le domaine d'application de la loi, elles travaillent exclusivement avec les systèmes d'information que la Confédération met à leur disposition. Le système INDEX SRC permet par exemple aux cantons de saisir des enquêtes préalables aux rapports adressés à la Confédération, de gérer les mandats et d'archiver leurs rapports (voir à cet égard l'art. 50). Les données sont exclusivement administrées par la Confédération, par le truchement du SRC, et sont soumises au droit fédéral de la protection des données. La Confédération est le seul maître des données dans le domaine d'application de la présente loi.

Les données visées à l'*al. 2* sont traitées par les cantons soit dans le cadre de leur propre activité en matière de renseignement (hors de la responsabilité de la Confédération, respectivement du SRC) soit dans le cadre d'autres tâches policières liées à la sûreté ou à la criminalité. Les cantons traitent ainsi de leur propre chef les données liées aux demandes d'autorisation pour des manifestations. Si des débordements extrémistes violents sont à craindre, le SRC les traite sous cet angle. Si la manifestation donne effectivement lieu à des actes de violence, le SRC traite ces informations sous l'angle l'extrémisme violent d'après la présente loi alors que les autorités cantonales traitent de leur propre chef les infractions telles que les déprédations matérielles, les violations de l'ordre public ou les lésions corporelles. En raison des diverses réglementations applicables à l'obligation de fournir des renseignements pour ces traitements de données, il faut éviter qu'une banque de données contienne des indications menant à d'autres données. Les prescriptions d'exécution peuvent prévoir des exceptions, par exemple lorsque des annonces ne contiennent aucune donnée personnelle ou que les personnes concernées sont au courant du double traitement, par exemple lorsque les annonces sont produites au cours d'interrogatoires.

L'al. 3 a été complété sur la base des résultats de la consultation, de manière à ce que les cantons puissent utiliser les observations issues des appréciations de la situation, comme le prévoit actuellement la LMSI. Les dispositions se rapportant au stockage des données des cantons (art. 50) et à leur surveillance cantonale (art. 78) ont aussi été complétées et précisées.

Art. 46 Systèmes d'information du SRC

L'art. 46 définit le réseau de systèmes d'information que le SRC exploite pour s'acquitter de ses tâches. Le réseau est comparable à celui des systèmes d'information de police réglé à l'art. 2 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[32].

L'article donne un aperçu de tous les systèmes d'information du SRC dont la base légale se trouve dans la présente loi. Chaque système d'information fait ensuite l'objet d'un article séparé.

L'*al. 2* charge le Conseil fédéral de déterminer les spécificités du traitement des données pour chaque système d'information, notamment la fréquence des contrôles périodiques et la durée de conservation maximale. La délégation de ces modalités au Conseil fédéral correspond à la réglementation actuelle et à la procédure usuelle pour les systèmes d'information. L'ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC)[33] fixe ainsi les délais maximaux de conservation: pour les données concernant l'exploration à l'étranger, le délai est de 30 ans après le dernier traitement, mais de 45 ans au maximum; pour ce qui est des données suisses, ces délais se situent entre cinq (données issues des contrôles de sécurité relatifs aux personnes) et 45 ans (données issues de sources accessibles au public) selon la provenance des données. De même, l'OSI-SRC fixe les délais de contrôle périodique des données issues de l'exploration en Suisse à cinq ans après leur première saisie, puis à tous les trois ans jusqu'à ce que la durée maximale de conservation soit atteinte. La LRens prévoit pour sa part que le Conseil fédéral doit tenir compte des spécificités des données et des besoins inhérents aux différents domaines d'activités lorsqu'il fixe les délais en question. Cette réglementation doit permettre de trouver comme auparavant des solutions différenciées pour les divers systèmes et catégories de données.

Les dispositions d'exécution contiendront des réglementations détaillées, spécifiant quelles personnes sont autorisées à effectuer quels types de traitement des données (lire, écrire, modifier, effacer) et quelles autorités fédérales et cantonales issues des domaines de la police, de la justice et de la procédure pénale peuvent accéder au système INDEX SRC en dehors du SRC.

De plus, le SRC édictera des directives d'utilisation pour tous les systèmes d'information en se fondant sur les consignes générales applicables en matière de protection des données et des informations. Ces directives décriront notamment l'organisation interne, ainsi que les procédures de traitement de données et de contrôle, et contiendront les documents concernant la planification, la réalisation et l'exploitation de la banque de données et des moyens informatiques.

Art. 47 Versement des données dans les systèmes d'information

Les données qui parviennent au SRC font dans un premier temps l'objet d'un examen permettant de déterminer leur pertinence pour l'exécution de la mission et leur exactitude. L'organe compétent du SRC les enregistre ensuite dans le système prévu pour ce type de données. Aucune donnée n'est directement versée dans les systèmes IASA SRC et INDEX SRC. IASA permet aux analystes du SRC de compiler,

32 RS **361**
33 RS **121.2**

d'analyser et de documenter les données et renseignements nécessaires à la production. Le SRC verse dans le système INDEX SRC principalement les données d'identification de personnes, d'organisations, d'objets et d'événements qui sont copiées à partir des systèmes IASA SRC et IASA-EXTR SRC.

Art. 48 IASA SRC

L'art. 48 crée la base légale formelle du système d'analyse intégrale du SRC (IASA SRC), qui permet d'analyser du point de vue du renseignement tous les champs d'activité du SRC à l'exception de l'extrémisme violent. Selon la nouvelle procédure, ces données peuvent uniquement être traitées dans le système IASA-EXTR SRC (art. 48). À quelques détails près, IASA SRC remplace les systèmes ISIS (système d'information sécurité intérieure) et ISAS (système d'information sécurité extérieure).

Les domaines spécialisés du SRC responsables de la saisie des données effectuent le contrôle périodique des données enregistrées dans IASA dans leurs domaines respectifs. L'organe interne de contrôle de la qualité effectue de plus régulièrement des contrôles par sondage, afin de s'assurer que les données sont traitées conformément à la loi (art. 44).

Art. 49 IASA-EXTR SRC

Les données liées à l'extrémisme violent ont souvent des liens exclusifs plus prononcés avec la Suisse que celles relevant d'autres secteurs d'activités du SRC. Elles sont souvent aussi plus sensibles, puisque la proximité est plus grande avec les activités politiques protégées par les droits fondamentaux, qui sont soustraites à la recherche et au traitement en vertu de l'art. 5, al. 5, LRens. Ces données sont par conséquent saisies dans un système d'information particulier, le système d'analyse intégrale de l'extrémisme violent (IASA-EXTR SRC), qui sert à saisir, traiter et analyser de manière centralisée toutes les données se rapportant à ce domaine. Elles sont également soumises à un contrôle plus strict et régulier de la part de l'organe interne de contrôle de la qualité du SRC (art. 44, al. 5, let. a).

Conformément à l'art. 69, al. 1, let. c, le Conseil fédéral détermine chaque année les groupements qui entrent dans la catégorie des extrémistes violents.

Art. 50 INDEX SRC

Le système d'indexation des données (INDEX SRC) sert d'une part à déterminer si le SRC traite des données se rapportant à une personne, une organisation, un objet ou un événement donné. Toutes les personnes saisies dans IASA SRC et IASA-EXTR SRC peuvent y être consultées. Concrètement, le système contient les principales données d'identification des personnes concernées, telles que le nom, la date de naissance et la nationalité. Ont également accès à l'index les organes autorisés qui ne sont pas raccordés au réseau hautement sécurisé du SRC.

Le système INDEX SRC sert ainsi à coordonner les activités relevant du renseignement de la Confédération et des cantons, mais aussi celles ressortissant au renseignement avec celles relevant de la police de sûreté et de la police criminelle. Aujourd'hui, une telle coordination est possible parce que les services officiels situés en dehors du SRC ont un accès direct au système ISIS, limité aux données d'identification. Les services situés en dehors du SRC et les autorités cantonales d'exécution

n'ont aucun accès à des informations autres que les données d'identification. Ils doivent prendre contact avec le SRC pour éventuellement obtenir un accès à d'autres données par le biais d'une collaboration formelle et d'une transmission de données (art. 58 ss).

Le système INDEX SRC est nécessaire à ces fins comme système particulier, puisque IASA SRC et IASA-EXTR SRC doivent être exploités dans le réseau hautement sécurisé du SRC auquel les services extérieurs au SRC n'ont pas le droit d'accéder. Il permet aux services tiers autorisés de chercher rapidement des données d'identification, alors que les données intégrales du SRC restent protégées des accès extérieurs.

L'INDEX SRC sert d'autre part de plateforme pour le traitement des données par les autorités cantonales d'exécution. Elles y traitent les données en amont d'un rapport destiné au SRC. Le système leur permet en outre d'avoir une vue d'ensemble des mandats de la Confédération et de les archiver. Cette centralisation à l'échelon fédéral de tous les traitements de données intervenant dans le cadre de la LRens permet de garantir une réglementation et un contrôle uniformes.

Lors de la consultation, quelques cantons ont exprimé le souhait d'avoir mutuellement accès à leurs données cantonales. Après clarification, il s'est avéré que ce besoin visait plutôt à obtenir la possibilité d'une transmission de données en toute sécurité entre les cantons. Cette demande a dès lors été prise en compte à l'al. 2.

Art. 51 GEVER SRC

Le système de gestion des affaires du SRC (GEVER SRC) permet une administration standardisée des affaires, comme dans d'autres secteurs de l'administration fédérale. Toutefois, le SRC traite typiquement des affaires qui relèvent principalement du renseignement, telles que des rapports d'analyse, des appréciations de situation écrites ou orales ou des réponses à des demandes individuelles. Ces affaires sont gérées dans ce système central comme des affaires purement administratives (par ex. prises de position lors de consultations d'offices, processus financiers, affaires liées au personnel, etc.), ce qui permet d'avoir une vue d'ensemble de toutes les affaires en cours et de toutes les affaires terminées et de pouvoir les contrôler. Le système GEVER SRC permet en outre de garantir l'archivage des produits du SRC, grâce à un système de référencement harmonisé avec les Archives fédérales.

Afin de protéger les données issues du renseignement, le SRC exploite également le système GEVER SRC dans son réseau hautement protégé, auquel aucun service tiers n'a accès.

Art. 52 PES

L'art. 52 crée la base légale formelle du système de présentation électronique de la situation (PES), qui figure actuellement à l'art. 10*a* LMSI. La disposition correspond largement à la révision de la LMSI entrée en vigueur le 16 juillet 2012.

Les données personnelles ne sont exploitées dans le système PES que si elles sont absolument nécessaires pour la présentation et l'appréciation de la situation.

L'accès au système à titre exceptionnel de particuliers ou d'autorités étrangères a donné lieu à de nombreuses discussions dans le cadre de la LMSI II. La pratique actuelle a confirmé l'application restrictive de cette disposition par le SRC. Le

Conseil fédéral reste toutefois convaincu que la Suisse, en sa qualité d'hôte de manifestations internationales, doit veiller à la sécurité en collaboration avec des partenaires privés et étrangers. Les expériences faites par exemple dans le cadre de l'EURO 08 ont montré qu'il peut être nécessaire lors de manifestations d'envergure présentant un risque accru de donner immédiatement accès à certaines données du système PES à des organisations privées ou à des partenaires étrangers. Dans un tel cas, il faut toutefois systématiquement veiller à ce que le principe de proportionnalité soit respecté, en ce sens que le SRC ne doit donner accès qu'aux données qui sont nécessaires pour lutter contre cette menace particulière.

Art. 53 Portail ROSO

L'art. 53 constitue la base légale formelle du portail d'accès aux renseignements de source ouverte (portail ROSO), qui sert aux collaborateurs du SRC à compiler des données provenant de sources accessibles au public. L'enregistrement de données publiées sur Internet est par exemple indispensable à une analyse ciblée, faute de quoi il faudrait à chaque fois recommencer les recherches sur l'ensemble de la Toile. De plus, rien ne garantit la permanence des données publiées sur Internet.

Les données enregistrées dans le système étant en principe accessibles à tout le monde, elles peuvent être traitées de manière moins restrictive que les données issues d'autres sources. L'*al. 3* n'en limite donc pas l'accès à certains domaines du SRC.

Comme l'ont souhaité les cantons lors de la consultation, l'al. 4 a été complété de manière à ce que les autorités cantonales d'exécution aient accès à certaines parties du portail ROSO. Un accès intégral n'est pas possible, notamment pour des questions de droits d'auteur.

Art. 54 Quattro P

Le SRC fait déjà saisir par les organes aéroportuaires suisses de contrôle à la frontière les données d'entrée dans le pays de personnes provenant de certains États à des fins de détection précoce des activités d'espionnage et de prolifération d'armes de destruction massive. Ces données doivent être traitées dans un système d'information séparé portant le nom de Quattro P («Programme préventif de contrôle des passeports», actuellement intégré au module informatique P4 visé à l'art. 25, al. 1, let. h, OSI-SRC). Cet article ayant donné lieu à quelques malentendus dans le projet mis en consultation, il a été formulé de manière plus précise.

Conformément à l'*al. 3*, seul un petit cercle de personnes au sein du SRC y a accès, à savoir celles qui sont chargées de saisir, de rechercher et d'analyser ces données (moins de dix personnes à l'heure actuelle). C'est aussi la raison pour laquelle aucun accès n'est prévu pour les cantons.

Le Conseil fédéral détermine chaque année selon l'*al. 4* l'étendue des catégories de personnes à enregistrer, c'est-à-dire les pays d'origine qui sont déterminants et les éventuelles restrictions à certaines catégories de personnes (par ex. uniquement les hommes ou les titulaires de certains types de passeports). La procédure est comparable à celle découlant de l'art. 20, al. 4, pour la détermination des événements et des constatations qui doivent être annoncés spontanément au SRC. La durée maximale de conservation des données enregistrées dans le système Quattro P est actuellement de cinq ans (art. 33, al. 1, let. i, OSI-SRC).

Art. 55 SICO

Le système d'information en matière de communication (SICO) permet au SRC de gérer et de piloter les mandats qu'il confie au COE. Le pilotage de l'exploration radio et de l'exploration du réseau câblé se fait par le biais de mandats écrits du SRC (voir les art. 37 ss). Ceux-ci contiennent l'ordre d'exploration, les informations relatives aux objets concrets qui doivent être explorés, les résultats attendus et d'autres conditions générales applicables au développement du mandat. Les résultats des contrôles périodiques internes au SRC sur la légalité, l'utilité et l'efficacité des mesures d'exploration font aussi partie du SICO. Les données du SICO servent de base pour les activités des organes de surveillance (en particulier l'autorité de contrôle indépendante visée à l'art. 75).

Seuls quelques rares collaborateurs du SRC chargés du pilotage direct des mandats ont accès au SICO (moins de dix à l'heure actuelle).

La saisie des résultats issus de l'exploration radio et de l'exploration du réseau câblé à des fins d'analyse et d'utilisation dans des produits, suivis de situation, etc. s'effectue dans le système de stockage des données résiduelles (art. 56).

Art. 56 Système de stockage des données résiduelles

Toutes les informations qui n'ont pas pu être versées dans un autre système lors du triage effectué après le contrôle d'entrée sont enregistrées dans le système de stockage des données résiduelles. Il s'agit avant tout des annonces provenant d'autorités étrangères de sûreté, de données issues de l'exploration radio et de l'exploration du réseau câblé, de renseignements provenant d'informateurs et d'informations qui ne sont pas activement recherchées par le SRC. Le système de stockage des données résiduelles ne contient pas non plus de données liées à l'extrémisme violent, qui sont toutes saisies et traitées dans IASA-EXTR SRC.

Les informations du système de stockage des données résiduelles sont transférées dans le système IASA SRC, surtout à des fins d'analyse, lorsqu'elles sont nécessaires pour l'établissement de produits, de suivis de situation, d'études ou d'éléments similaires relevant du renseignement.

Grâce à des contrôles périodiques, le SRC s'assure que les informations contenues dans le système de stockage des données résiduelles soient toujours pertinentes (lien avec un domaine d'activité du SRC, respect de l'art. 5, al. 5 à 8, LRens) et exactes. Dans le cas contraire, les données sont effacées et les informations incorrectes qui sont nécessaires seront désignées comme telles. Comme pour le contrôle d'entrée, l'appréciation périodique est globale, c'est-à-dire qu'aucune déclaration spécifique contenue dans un document volumineux tel qu'une liste de personnes n'est examinée.

Art. 57 Données provenant de mesures de recherches soumises à autorisation

Les données qui sont acquises par des mesures de recherche soumises à autorisation nécessitant l'engagement de moyens techniques (comme une surveillance de communication) peuvent d'une part être très volumineuses et d'autre part contenir de nombreuses informations n'ayant aucun rapport avec le but de la recherche, parce qu'elles sont par ex. de nature strictement privée. Il faut également tenir compte de la protection de la personnalité des tiers qui utilisent par ex. le raccordement de

télécommunication de la personne surveillée. Souvent, il n'est pas possible de déterminer de prime abord si des communications sont pertinentes ou non, parce que le réseau de contact de la personne surveillée doit par ex. encore être identifié ou que celle-ci utilise des éléments secrets dans ses communications pour les protéger. Les informations ne peuvent donc pas être immédiatement identifiées comme nécessaires ou non.

L'enregistrement dans des systèmes séparés sert également à protéger l'infrastructure informatique du SRC, car des logiciels malveillants (virus, cheval de Troie) peuvent s'infiltrer lors de la surveillance de communications Internet ou de l'introduction dans des systèmes ou des réseaux informatiques. Or, ces maliciels ne doivent pas contaminer les systèmes du SRC.

L'art. 57 prévoit dès lors que les données issues de telles mesures de recherche soient enregistrées et consultées dans des systèmes distincts du réseau des systèmes intégrés d'information. Conformément à l'*al. 2*, le SRC ne reprend que les données nécessaires aux fins du mandat pour les analyser ultérieurement dans les systèmes d'information correspondants du réseau, en règle générale dans IASA SRC.

L'art. 35, al. 5, prévoit la possibilité d'enregistrer dans des systèmes d'information distincts les données provenant de l'étranger recherchées à l'aide de mesures comparables.

L'*al. 3* restreint logiquement l'accès à ces données aux personnes chargées de l'exécution directe de la mesure et de l'analyse de ses résultats. Il s'agira en règle générale des collaborateurs compétents pour la recherche et l'analyse du cas en question.

Les systèmes entrant en ligne de compte sont en général des systèmes informatiques qui ne sont pas reliés au réseau hautement sécurité du SRC. Le Conseil fédéral en règlera également les modalités par voie d'ordonnance (catalogue des données, droits de traitement et droits d'accès, notamment).

Art. 58 Vérification avant la transmission de données

Sont tenus d'évaluer la qualité des données avant transmission non seulement les organes du SRC chargés du contrôle de qualité, mais chaque personne qui participe à une transmission d'informations du SRC. Ces personnes sont tenues de veiller à ce que les conditions légales régissant la transmission des données soient respectées et que les données personnelles soient traitées correctement.

Art. 59 Transmission de données personnelles à des autorités suisses

Pour s'acquitter de sa mission d'alerte précoce et de prévention, le SRC doit pouvoir transmettre des données personnelles à des autorités politiques, des autorités de poursuite pénale, des autorités judiciaires ou des autorités de sûreté. A Les dispositions du projet correspondent largement à l'art. 17 LMSI. Elles ont toutefois été précisées et différenciées.

La transmission de données issues de mesures de recherche soumises à autorisation en particulier exige des mesures de protection élargies, afin d'éviter que de petites infractions qui ont par exemple été constatées lors de surveillances de télécommunications soient annoncés aux autorités de poursuite pénale. Le droit de procédure pénale contient une réglementation similaire pour de telles découvertes dites for-

tuites (art. 278 CPP). La LRens reprend à l'*al. 3* le principe selon lequel le SRC peut uniquement utiliser les données se rapportant à des infractions pour la poursuite desquelles la mesure de surveillance correspondante ressortissant au droit de procédure pénale aurait pu être ordonnée. Une harmonisation plus poussée avec le droit de procédure pénale n'est toutefois pas judicieuse, puisque la LRens vise en premier lieu d'autres buts que la poursuite pénale et que d'autres secteurs administratifs sont tenus de transmettre aux autorités de poursuite pénale les informations dont ils disposent sur d'éventuelles infractions.

Lors de la consultation, des demandes parfois contradictoires ont été formulées pour que davantage ou moins de données soient transmises aux autorités de poursuite pénale. Le Conseil fédéral est d'avis que la solution proposée est équilibrée.

Art. 60 Transmission de données personnelles à des autorités étrangères

Cet article reprend largement les dispositions de l'art. 17 LMSI. Le droit de la protection des données prévoit en règle générale que des données personnelles ne peuvent être transmises qu'aux États qui garantissent un niveau de protection des données comparable à celui de la Suisse (art. 6, al. 1, LPD). Cette disposition exclurait la plupart des pays non européens de toute collaboration avec le SRC si les exceptions prévues à l'art. 6, al. 2, LPD ne pouvaient pas s'appliquer dans des cas particuliers. Le SRC serait alors privé d'importantes sources d'information dans les régions en crise.

Aussi la LMSI contient-elle des règles particulières pour la collaboration en matière de renseignement et l'échange de données personnelles avec l'étranger, règles que la LRens reprend dans le présent article. Il existe à cet égard une longue pratique, accompagnée et contrôlée par les organes de surveillance (surveillance des services de renseignement du DDPS et autrefois du DFJP et Délégation des Commissions de gestion des Chambres fédérales).

La collaboration et l'échange de données avec des autorités étrangères de sûreté qui ne sont pas des services de renseignement au sens strict se limitent aux fonctions qu'elles revêtent qui sont comparables aux tâches du SRC. La collaboration d'autres services suisses dans leurs champs de compétences avec des autorités étrangères de sûreté n'est ainsi pas restreinte. Ils sont seuls responsables de la transmission de leurs données conformément à leurs propres bases légales.

L'*al. 2, let. d*, concerne les demandes de conformité ou les contrôles de sécurité mentionnés à l'art. 12, al. 1, let. d, pour les personnes (généralement suisses) qui doivent avoir accès à l'étranger à des projets, informations, installations, etc. classifiés. La transmission de tels renseignements est en règle générale dans l'intérêt de la personne concernée, afin qu'elle puisse occuper le poste qu'elle vise ou exercer une activité commerciale.

Art. 61 Transmission de données personnelles à des tiers

Les activités en matière de renseignement requièrent parfois la transmission de données à des particuliers. Le cas le plus fréquent consiste à motiver une demande de renseignement. En d'autres termes, lorsqu'il recherche des renseignements sur des personnes physiques ou morales, le SRC doit pouvoir indiquer à la personne interrogée sur qui il a besoin d'un renseignement et dans quel contexte. Cette disposition correspond à l'art. 17, al. 3, LMSI.

Art. 62 à 65 Droit d'accès

S'agissant du droit d'accès d'une personne aux données qui la concernent, le projet reprend largement la solution adoptée par le Parlement dans le cadre de la LMSI II réduite sur la base de la LSIP (art. 18 LMSI, entré en vigueur le 16 juillet 2012). Cette réglementation est subdivisée en quatre articles pour en améliorer la lisibilité.

Le Tribunal fédéral a jugé que l'ancien droit d'accès indirect prévu par la LMSI était conforme à la Constitution, pour autant qu'il soit assorti d'une possibilité efficace de recours. La version initiale de la LMSI II contenait une telle solution, mais celle-ci a été rejetée. Le Conseil fédéral avait alors demandé que la protection des données soit régie intégralement par la LPD. Le Parlement a toutefois sciemment opté pour une réglementation analogue à la LSIP. Le Conseil fédéral n'a pas changé d'avis: il considère que d'autres solutions sont praticables, mais il ne serait pas judicieux de soumettre au Parlement une nouvelle réglementation en matière de droit d'accès.

Le processus prévoit que le SRC examine d'abord l'opportunité de donner un renseignement, mais qu'il diffère sa réponse au cas où des intérêts visant à préserver un secret entrent en jeu ou que la personne concernée n'est pas répertoriée dans les systèmes. Celle-ci peut ensuite s'adresser au Préposé fédéral à la protection des données et à la transparence (préposé), qui applique par analogie l'ancienne procédure du renseignement indirect.

Le Conseil fédéral propose de revenir dans l'*art. 63, al. 5*, à la formulation de la LSIP, qui prévoit que, en cas de report de la réponse, des renseignements peuvent exceptionnellement être donnés sur recommandation du préposé (en raison d'intérêts liés au maintien du secret ou lorsque la personne n'est pas répertoriée dans les systèmes du SRC), pour autant que leur communication ne constitue pas une menace pour la sûreté intérieure ou extérieure de la Suisse et qu'une personne rend vraisemblable que le report de la réponse la léserait gravement et de manière irréparable. La LMSI a en effet renversé le fardeau de la preuve par rapport à la LSIP, en prévoyant que le SRC doit donner le renseignement demandé sur recommandation du préposé dans la mesure où cela ne constitue pas une menace pour la sûreté intérieure ou extérieure du pays. Or, le SRC ne peut guère apporter cette preuve pour les personnes non répertoriées, puisqu'il ne dispose précisément d'aucune information sur elles. Reprendre la réglementation de la LMSI viderait au surplus l'art. 62, al. 2, let. c, de son contenu, puisqu'il dispose que la réponse est différée pour les personnes non répertoriées. La procédure prévue dans la LSIP semble donc techniquement plus juste.

Art. 66 Exception au principe de la transparence

Les expériences faites par le SRC avec les demandes de consultation fondées sur la loi du 17 décembre 2004 sur la transparence (LTrans)[34] ont montré que le besoin de protection particulier lié aux informations ressortissant au renseignement est difficilement conciliable avec la transparence préconisée par la LTrans.

Les demandes d'accès déposées concernent essentiellement des documents et des dossiers sur la recherche d'informations par le SRC ou sur ses opérations (ou celles de ses prédécesseurs). Ponctuellement, un accès a été expressément demandé à d'autres documents, concernant par exemple les échanges avec des services de

34 RS **152.3**

renseignement étrangers ou d'autorités de sûreté étrangères. Eu égard aux personnes ou aux services étrangers impliqués et conformément aux exceptions prévues par la LTrans, le SRC doit chaque fois refuser l'accès aux dossiers de recherche et de collaboration après avoir effectué un examen approfondi de la question et justifié le refus en interne. Par conséquent, il n'est pas judicieux de vouloir maintenir le principe selon lequel il convient d'accorder un droit de consultation des documents relatifs à la recherche d'informations relevant du renseignement s'il est clair d'emblée que ces documents sont soumis aux exceptions prévues par la LTrans.

La question d'exclure intégralement le SRC du champ d'application de la LTrans s'est posée. Étant donné toutefois que le SRC s'occupe aussi d'affaires purement administratives, pour lesquelles il est tout à fait possible de fournir des renseignements conformément aux principes de la LTrans, le Conseil fédéral propose de n'excepter que les documents portant sur la recherche d'informations relevant du renseignement.

Art. 67 Archivage

Les données et dossiers du SRC sont globalement soumis à la loi fédérale du 26 juin 1998 sur l'archivage (LAr)[35], qui prévoit un archivage intégral de tous les dossiers ayant une valeur archivistique pour les Archives fédérales. Toutefois, les dossiers du SRC contiennent aussi des documents provenant de services de renseignement étrangers qui ont été transmis sous réserve de la protection des sources. Si une telle protection n'est plus garantie, ces informations se tariraient et la Suisse se trouverait isolée dans la lutte contre des menaces globales telles que le terrorisme, la prolifération d'armes de destruction massive, l'extrémisme violent et l'espionnage.

Les *al. 1 et 2* prennent en compte l'intérêt des Archives fédérales à un archivage aussi complet que possible des dossiers et l'intérêt légitime des autorités de sûreté à une protection effective des sources. Les données et dossiers du SRC sont intégralement archivés par les Archives fédérales dans des locaux hautement sécurisés. En cas de demande concrète de consultation, les dispositions de la LAr prévoient que la consultation peut être limitée ou interdite dans un cas particulier lorsque des intérêts publics ou privés prépondérants et dignes de protection s'y opposent. L'al. 2 énonce qu'un tel intérêt public est donné lorsque le service étranger a de bonnes raisons de refuser la consultation. Le SRC désignera clairement les documents concernés lorsqu'il les proposera aux Archives fédérales, de sorte que celles-ci puissent aisément identifier les cas où la consultation du SRC s'impose. D'autres pays procèdent de la même façon à l'égard de la Suisse.

Dans certains cas particuliers, le SRC doit pouvoir consulter des données personnelles archivées (*al. 3*). Des règles analogues existent pour les autorités de poursuite pénale. Exemple: le SRC reçoit une demande d'un service de renseignement étranger en relation avec la reprise d'une enquête sur un attentat, mais le SRC a déjà effacé les données issues de ses recherches de l'époque et les a remises aux Archives fédérales.

35 RS **152.1**

Art. 68 Prestations

À l'instar de tout autre service officiel, le SRC a le droit et est tenu de fournir une assistance administrative dans les domaines où il est compétent et en mesure de le faire avec le personnel dont il dispose et sur le plan technique. Il peut fournir des moyens et méthodes de type opérationnel particuliers, par exemple des prestations de transmission, de transport et de conseil dont les autres services ne disposent pas.

Les moyens de communication sécurisés du SRC, notamment des téléphones mobiles chiffrés, sont ainsi régulièrement utilisés dans le cadre de la gestion internationale des crises (par ex. lors d'enlèvements). Les organes de sûreté de la Confédération et d'organisations internationales font appel aux compétences du SRC dans les domaines de la confidentialité et de la protection des informations, par ex. lors de fouilles de locaux visant à trouver des installations d'écoute. Le SRC conseille les organes compétents de la Confédération pour ce qui est de l'acquisition de coffres-forts et de techniques de fermeture spéciales des locaux. Les services de renseignement étrangers et les autorités de sûreté étrangères sont soutenus par le SRC notamment par l'organisation de transports spéciaux.

Le SRC a participé dans un cas concret d'enlèvement à l'issue heureuse à la gestion de la crise en fournissant les prestations suivantes:

- il a fourni des moyens de communication sécurisés pour assurer la liaison entre le centre de gestion des crises du DFAE et la représentation de ce dernier sur place et a fourni le soutien technique;
- il a fourni ses moyens de communication sécurisés pour l'échange quotidien des informations;
- il a mis en place dans la représentation locale un environnement de travail protégé et sécurisé, parfaitement adapté au contexte sensible;
- il a mis à la disposition permanente de l'ambassadeur suisse un collaborateur pour assurer la liaison avec le service de renseignement local et les représentants d'autres services de renseignement et pour analyser en continu la situation en matière d'information;
- il a soutenu le centre de gestion des crises à l'aide d'une cellule interne chargée de l'appréciation de la situation, de la prise de contact avec des services de renseignement étrangers et de la collaboration avec d'autres services suisses;
- il a assuré avec le service de renseignement étranger concerné la base de négociation et de communication.

Les particuliers ne sont soutenus qu'à titre exceptionnel, dans les cas où le soutien revêt également un intérêt du point de vue du renseignement et, partant, un intérêt public. Il peut ainsi s'avérer nécessaire lors d'un enlèvement d'équiper un proche de la personne enlevée avec des moyens de communication chiffrés. Dans des cas particuliers, il peut également être intéressant du point de vue du renseignement de fouiller, avec son assentiment, les locaux d'une entreprise privée pour y rechercher des installations d'écoute illégales (micros). L'intérêt de l'État en la matière, et non le souhait du particulier, est déterminant à cet égard. Le SRC ne doit notamment pas entrer en concurrence avec des fournisseurs privés de prestations comparables. En présence d'intérêts essentiels de la Suisse, au sens de l'art. 3, le Conseil fédéral peut également confier de telles tâches au SRC.

Il semble dès lors opportun de créer une base légale explicite pour ces prestations de soutien et les restrictions auxquelles elles sont soumises.

Art. 69 Pilotage politique par le Conseil fédéral

Le SRC sert particulièrement les intérêts du pays et du gouvernement. Le rôle que joue le Conseil fédéral dans le pilotage politique et l'orientation des activités du SRC ne doit dès lors pas seulement être repris des bases légales actuelles, mais être explicité et renforcé. L'art. 69 reprend donc différents éléments de la législation actuelle et les réunit dans une disposition centrale sur le pilotage politique. La Délégation des Commissions de gestion des Chambres fédérales aura plein accès à tous les instruments de pilotage politique mentionnés, au même titre qu'à tous les autres documents du SRC.

La *let. a* approfondit le système existant selon lequel le Conseil fédéral donne au SRC une mission stratégique de base. Cette dernière s'en tient au cadre de la loi tout en fixant des priorités thématiques et régionales. En raison de sa petite taille, le SRC n'est pas en mesure de couvrir de la même manière l'ensemble des régions et des évolutions ressortissant à la politique de sécurité, notamment à l'étranger. La mission stratégique de base du Conseil fédéral lui dicte donc une direction générale. De plus, des événements et des développements à court terme peuvent bien évidemment influer sur l'activité du SRC dans le respect du cadre légal. Lorsque de tels développements ont un impact à long terme, la mission de base doit être adaptée hors de la période ordinaire de contrôle de quatre ans. Le pilotage politique doit toutefois viser la continuité. Une autorisation judiciaire, comme proposé par certains participants à la consultation, n'est pas judicieuse pour cet instrument de pilotage politique, d'autant qu'elle reporterait sur un tribunal la responsabilité du Conseil fédéral.

Actuellement, la mission de base est réglée à l'échelon de l'ordonnance (art. 2, al. 2, OSRC). Elle est classée «secret» en raison de son importance et de son contenu.

La *let. b* renvoie à la liste d'observation, qui est réglée dans le détail à l'art. 71 et que connaît le droit en vigueur (art. 11, al. 3 à 7, LMSI).

La *let. c* découle du nouveau régime de traitement des données, compte tenu de la distinction et du traitement plus strict des données liées à l'extrémisme violent qu'il introduit. Afin que le SRC puisse faire cette distinction de manière univoque, le Conseil fédéral désigne chaque année les groupements qui ressortissent à l'extrémisme violent. Aucune mesure soumise à autorisation au sens des art. 25 et suivants ne peut ainsi être prise contre de tels groupements; de plus, les données concernant les groupements extrémistes violents sont versées dans le système d'information spécial IASA-EXTR SRC dans le cadre du traitement des données par le SRC (art. 49). Le Conseil fédéral prend acte au surplus du nombre de personnes entrant dans le spectre de l'extrémisme violent qui n'ont pas pu ou pas encore pu être assignées à un groupement donné. Il obtient ainsi une image d'ensemble de l'extrémisme violent en Suisse.

Comme le prévoit le droit en vigueur, le Conseil fédéral approuve la collaboration du SRC avec les organes de sûreté d'autres États (*let. f*), essentiellement les services de renseignement avec lesquels le SRC a des contacts institutionnalisés. Ces contacts sont regroupés sur une liste spéciale que le DDPS soumet au Conseil fédéral pour approbation.

Notons que la collaboration avec des autorités étrangères dans le domaine du renseignement n'est normalement pas réglée de façon formelle, par ex. par des traités internationaux. Le plus souvent, elle repose sur des accords informels non contraignants (déclarations d'intention) ou des conventions administratives.

L'*al. 3* prévoit que le rattachement du SRC à une banque de données commune qui serait exploitée en réseau avec des services de renseignements étrangers partenaires du SRC doit en revanche être réglé dans un traité international conclu par le Conseil fédéral. À l'heure actuelle, il n'existe aucune banque de données ou accord de ce type, même si des réflexions sont fréquemment lancées sur le plan international pour améliorer la collaboration à l'aide de tels instruments. Compte tenu des questions que posent actuellement les pratiques internationales en matière d'écoutes développées par d'importants services de renseignement étrangers, il est aussi question de régler à l'avenir les activités mutuelles relevant du renseignement dans des traités (par ex. «convention de non-espionnage»). Il est trop tôt pour dire si une nouvelle pratique va se développer à l'échelle internationale et si elle impliquer des règles contraignantes et applicables. Le Conseil fédéral considère dès lors qu'il est judicieux que la nouvelle codification du service de renseignement permette à la Suisse de participer le cas échéant à de tels développements. Il part du principe que, jusqu'à nouvel ordre, seules des questions techniques de moindre importance feront l'objet d'accords dans le domaine du renseignement.

Art. 70 Sauvegarde d'autres intérêts essentiels de la Suisse

Cet article découle de l'art. 3 et fixe la procédure qui permet, dans des situations particulières, de charger le SRC de prendre des mesures visant à sauvegarder d'autres intérêts essentiels de la Suisse. Cette procédure ne donne pas au SRC de compétences supplémentaires et les dispositions relatives à l'obligation d'obtenir une autorisation pour certaines mesures de recherche restent applicables. L'attribution formelle d'un mandat constitue même une condition nécessaire pour que le SRC puisse agir dans un domaine qui dépasse le cadre normal délimité par la loi et la mission de base.

Art. 71 Liste d'observation

Prévue dans la LMSI, la liste d'observation est un instrument de conduite du Conseil fédéral. Elle est établie par le DDPS et doit être approuvée chaque année par le Conseil fédéral (art. 69, al. 1, let. b). Depuis le 11 septembre 2001, la communauté internationale a intensifié ses efforts dans la lutte contre le terrorisme. Comme la révision LMSI II réduite du 23 décembre 2011 a introduit la prise en compte des listes internationales, la liste d'observation se fonde sur les listes internationales de terroristes dans le présent projet. À la différence de la LMSI, qui charge le Conseil fédéral de désigner les organisations et communautés internationales pertinentes, la LRens ne mentionne plus que l'ONU et l'UE à l'*al. 2*. Il est peu probable que d'autres organisations internationales se mettent à publier des listes d'une importance similaire.

Une organisation ou un groupement placé sur la liste suisse d'observation ne subira aucune sanction (par ex. interdiction), contrairement aux règles du système de liste

appliqué par le Conseil de sécurité de l'ONU sur la base de la résolution 1267[36]. De même, on ne retrouvera pas d'individus sur la liste suisse d'observation. L'enregistrement d'une organisation, d'un groupement (ou d'une personne) sur une liste internationale n'entraîne pas automatiquement son inscription sur la liste d'observation suisse: lorsqu'une organisation donnée ou qu'un groupement donné est sans importance pour la Suisse, une inscription n'est pas nécessaire. D'autres organisations ou groupements figurant sur des listes internationales peuvent toutefois être inscrits sur la liste suisse d'observation sans autre justification.

Au surplus, la procédure régulière d'autorisation par le Conseil fédéral donne une marge de manœuvre suffisante pour biffer un groupement de la liste s'il s'avère que celui-ci ne menace plus la sûreté intérieure ou extérieure de la Suisse.

La restriction de traitement imposée par l'art. 5, al. 5, (activités politiques et exercice de droits fondamentaux) ne s'applique pas à la liste d'observation (voir à cet égard l'art. 5, al. 8). Le SRC peut rechercher et traiter toutes les informations disponibles sur les organisations et groupements figurant sur la liste lorsque celles-ci peuvent aider à évaluer la menace qu'ils représentent. Il n'y a toutefois pas d'autres effets directs pour les organisations ou les groupements concernés, tels que des sanctions, des interdictions ou des mesures similaires. De telles mesures continueront le cas échéant à être prises dans le cadre de décisions spéciales ou d'ordonnances qui ne relèvent pas de la compétence du service de renseignement.

Art. 72 Interdiction d'exercer une activité

Du point de vue matériel, cette disposition correspond presque entièrement à l'art. 9 LMSI dans sa version modifiée du 23 décembre 2011 (LMSI II réduite).

La disposition règle la compétence du Conseil fédéral d'interdire à une personne physique d'exercer une activité dans les cas prévus par la LRens, sans restreindre sa compétence globale d'édicter des ordonnances et de prendre des décisions sur la base de l'art. 185, al. 3, Cst. lors d'autres perturbations graves de l'ordre public ou de la sûreté intérieure ou extérieure. Cette compétence du Conseil fédéral subsiste en parallèle dans les cas qui ne sont pas réglés par la loi.

La disposition proposée donne au Conseil fédéral la possibilité de prononcer dans le domaine de la sûreté intérieure ou extérieure une interdiction d'activité pour une durée maximale de cinq ans et de la prolonger à plusieurs reprises de cinq ans, pour autant que les conditions nécessaires soient encore remplies. Grâce à cette nouvelle disposition, le Conseil fédéral pourrait par exemple prononcer des interdictions d'exercer une activité pour des sous-groupes d'organisations terroristes. En ce qui concerne Al-Qaïda, une ordonnance de l'Assemblée fédérale interdisant Al-Qaïda en tant qu'organisation expire à la fin de 2014. Il faudra examiner s'il vaut mieux que ces interdictions se fondent sur l'art. 9 LMSI, ou sur la LRens si elle est adoptée, ou ou que le Parlement prononce et prolonge des interdictions d'organisation en se fondant sur sa compétence d'édicter des ordonnances.

Les expériences faites par le passé laissent penser qu'il y aura très peu de cas par an. La charge de travail liée à de telles interdictions ne peut dès lors pas être calculée séparément, puisqu'elle s'inscrit dans le cadre des affaires politiques courantes.

36 Résolution 1267 (1999) sur la situation en Afghanistan. Ce document peut être consulté à l'adresse suivante:
www.un.org/fr > Conseil de sécurité > Documents > Résolutions > 1999.

L'interdiction visée au présent article est une mesure préventive visant à neutraliser de graves menaces pour la sûreté ou à empêcher des infractions. S'il existe un soupçon d'acte répréhensible, il faut engager une procédure pénale ordinaire et coordonner étroitement les éventuelles interdictions préventives avec les autorités compétentes en matière de poursuite pénale afin de ne pas mettre en péril une procédure en cours. Dans de tels cas, il peut toutefois aussi être judicieux d'ordonner des mesures préventives d'accompagnement, afin de garantir la sûreté intérieure et extérieure.

L'*al. 1* donne au Conseil fédéral la compétence de prononcer une interdiction de droit administratif contre les activités représentant une menace concrète pour la sûreté intérieure ou extérieure de la Suisse. Tous les départements auront la possibilité de déposer des demandes dans ce but.

La portée et le contenu des activités interdites doivent être décrits aussi précisément que possible dans la décision afin que l'interdiction puisse être appliquée et contrôlée de manière efficace. Comme ils dépendent des activités des personnes concernées, ils ne peuvent pas être décrits de manière exhaustive dans la loi.

Étant donné que les interdictions prononcées en vertu de l'*al. 1* peuvent entraver les personnes visées dans l'exercice de leurs droits fondamentaux, elles doivent être limitées dans le temps conformément à l'*al.* 2. Les autorités sont ainsi tenues, au terme de la durée de validité de l'interdiction, de réexaminer si les conditions d'une interdiction sont encore remplies ou si elles sont caduques.

Si les conditions sont encore remplies, la durée de validité d'une interdiction être prolongée de cinq nouvelles années aussi longtemps que les circonstances l'exigent. Si aucune prolongation n'est nécessaire, l'interdiction échoit automatiquement.

Conformément à l'art. 79, les interdictions d'exercer une activité prononcées sur la base du présent article peuvent être attaquées devant le Tribunal administratif fédéral selon la procédure décrite dans la loi fédérale du 20 décembre 1968 sur la procédure administrative[37], puis être portées devant le Tribunal fédéral.

Chapitre 6, section 2

Les art. 73 à 77 contiennent les différents échelons des prescriptions en matière de surveillance et de contrôle:

1. Autocontrôle du SRC
2. Surveillance par le département
3. Organe de contrôle indépendant
4. Surveillance et contrôle par le Conseil fédéral
5. Haute surveillance parlementaire.

Les différents niveaux et éléments de contrôle correspondent pour l'essentiel au droit en vigueur (art. 4*b* LFRC, art. 25 ss LMSI et art. 31 ss OSRC).

L'organe de contrôle indépendant veille à la légalité de l'exploration radio à l'étranger au sens de l'art. 37.

La surveillance parlementaire cantonale est aussi soumise à une réglementation, qui permet de séparer clairement les compétences de surveillance de la Confédération et

37 RS **172.021**

des cantons et d'éviter ainsi à la fois les doublons en matière de responsabilité et les lacunes dans la surveillance (art. 78, al. 2).

Certains participants à la consultation ont souhaité que la rentabilité des activités de renseignement soit également contrôlée. Le Conseil fédéral n'a pas spécialement pris en considération cette demande, parce que ce contrôle est déjà assuré par les dispositions générales sur la surveillance financière des autorités fédérales et est encore renforcé par la mention de la Délégation des finances à l'art. 77. De plus, la nécessité de garantir la sûreté intérieure et extérieure ne peut se fonder que de manière limitée sur des questions de rentabilité. L'aspect monétaire est souvent relégué au second plan dans la présente loi en raison de ses finalités, telles que la sauvegarde des bases démocratiques et de l'état de droit, la sûreté de sa population et des Suisses à l'étranger ou la préservation de la capacité d'action des organes de l'État.

Art. 74 Surveillance par le département

Comme jusqu'à présent, le DDPS doit disposer d'un organe de surveillance interne, à savoir la Surveillance des services de renseignement. Il est désormais régi par une base légale (al. 2), parce que des compétences accrues doivent lui être octroyées.

La structure des organes de surveillance doit absolument prévoir un organe de contrôle au sein du département. À défaut, en effet, le Conseil fédéral ne pourrait pas exercer sa surveillance de manière autonome, au contraire de la haute surveillance parlementaire. L'organe de surveillance interne dispose de droits de consultation et de renseignement très larges.

On pourrait envisager de subordonner cet organe à la Délégation des Commissions de gestion des Chambres fédérales (similaire au contrôle parlementaire de l'administration vis-à-vis des Commissions de gestion) ou de le rattacher du point de vue administratif à la Chancellerie fédérale comme organe d'état-major du Conseil fédéral ou au Secrétariat général du DDPS (solution actuelle); jusqu'à présent, l'organe de surveillance rapportait directement au chef du DDPS en lui transmettant des recommandations. Le Conseil fédéral est d'avis que la solution où l'organe de surveillance répond directement et sans influence externe au chef du DDPS est celle qui tient le mieux compte de la responsabilité en matière de conduite politique étant donné que le chef du DDPS assume personnellement et directement la responsabilité suprême du département.

Il n'existe aucun office fédéral qui soit autorisé de manière analogue au service de renseignement à porter atteinte aux droits fondamentaux des personnes concernées, le plus souvent à leur insu, ces atteintes touchant en particulier la sphère privée et le droit de disposer de ses propres données personnelles (« autodétermination informationnelle»). En constituant l'organe de surveillance interne au 1er janvier 2010 en même temps que SRC, le Conseil fédéral a tenu compte d'une demande du Parlement, qui souhaitait un contrôle intégral permanent des services de renseignement. L'organe de surveillance interne possède donc un caractère unique dans le droit administratif fédéral.

L'organe de surveillance interne établit au moins une fois par an un plan de contrôle confidentiel, qui doit être concerté avec la Délégation des Commissions de gestion des Chambres fédérale et soumis à l'approbation du chef du DDPS. Ce dernier peut lui confier des missions de contrôle supplémentaires relatives à une situation particu-

lière. Afin de renforcer l'indépendance et l'efficacité de la surveillance et conformément à une recommandation de la Délégation des Commissions de gestion des Chambres fédérales, la réglementation nécessaire figure désormais dans la loi. L'*al. 2* précise ainsi le statut, les compétences et l'indépendance de l'organe de surveillance interne. Les dispositions de la loi sur l'organisation du gouvernement et de l'administration restent applicables au surplus.

Les activités de contrôle de l'organe de surveillance interne auprès des autorités cantonales d'exécution doivent également être réglées dans la loi (*al. 3*). Ces contrôles portent sur les domaines dans lesquels les cantons recherchent des informations sur la base de missions fédérales (voir à cet égard l'art. 81) et complètent les activités de contrôle et de pilotage du DDPS visés à l'al. 1.

Quelques participants à la consultation ont proposé de remplacer l'organe de surveillance du département par un organe externe totalement autonome. Le Conseil fédéral considère qu'un tel système de surveillance, qui serait inédit, n'est pas approprié. Il porterait en effet atteinte à l'obligation légale de surveillance et à la responsabilité du chef du DDPS et pourrait remettre en question la conduite politique par le Conseil fédéral et le département. Le système de surveillance proposé, qui correspond aux règles prévues par la LOGA et la loi fédérale sur la responsabilité, est approprié pour garantir une surveillance efficace.

Art. 75 Organe de contrôle indépendant pour l'exploration radio

Comme celle applicable à l'exploration radio (art. 37), la réglementation relative à l'organe de contrôle indépendant pour l'exploration radio correspond dans une large mesure à la réglementation entrée en vigueur le 1er novembre 2012, que le Parlement a inscrite directement dans la LFRC (art. 4*b*; cf. également les commentaires concernant l'art. 37). Cet organe est actuellement composé de membres de l'administration, mais la LFRC n'exclut pas des membres externes à l'administration, ce qui peut être judicieux pour un certain temps lorsqu'un membre très compétent de l'organe de contrôle indépendant quitte l'administration fédérale, par exemple.

L'activité de contrôle exercée par cet organe était réglée de manière similaire dans l'ordonnance sur la guerre électronique et elle a fait ses preuves au cours de ces dernières années. Elle répond à un besoin dans un domaine sensible de l'exploration à l'étranger. L'al. 2 régit les tâches dévolues à l'organe de contrôle indépendant pour l'examen des missions et de leur traitement. Comme jusqu'à présent, cet organe ne peut ni ne doit contrôler ce traitement de manière approfondie, mais doit s'assurer par des vérifications appropriées que tant le service exécutant cette mission que le SRC respectent les dispositions légales.

Des dispositions similaires s'appliquent à l'exploration du réseau câblé. Celle-ci est toutefois soumise à une autorisation judiciaire et politique semblable à la procédure applicable aux mesures de recherche soumises à autorisation parce que les recherches requièrent la collaboration de fournisseurs privés de télécommunications en Suisse, contrairement à l'exploration radio qui peut être exécutée de manière autonome par les autorités fédérales (COE et SRC).

Un contrôle supplémentaire de l'exploration du réseau câblé par l'organe de contrôle indépendant pourrait entraîner une certaine confusion dans les compétences des instances concernées (Tribunal administratif fédéral et chef du DDPS d'un côté,

organe de contrôle indépendant de l'autre). Il n'est donc pas opportun de l'y soumettre.

Art. 76 Surveillance et contrôle par le Conseil fédéral

Cet article reprend le principe du contrôle de la légalité, de l'adéquation et de l'efficacité des activités de renseignement, inscrit à l'art. 26 LMSI. Selon l'art. 8 LFRC, il s'applique à tous les services civils qui remplissent des missions de renseignement. La LRens maintient le niveau élevé de surveillance et de contrôle. L'information régulière du Conseil fédéral sur les observations des organes de surveillance du DDPS et de la Délégation des Commissions de gestion des Chambres fédérales en fait également partie.

Art. 77 Haute surveillance parlementaire

L'art. 25 LMSI est repris et précisé: la haute surveillance parlementaire de l'exécution de la LRens relève exclusivement de la Délégation des Commissions de gestion et de la Délégation des finances des Chambres fédérales dans leurs champs de compétences respectifs. Ce contrôle englobe aussi bien les activités du SRC que celles des autorités d'exécution cantonales, pour autant que ces dernières exécutent un mandat direct de la Confédération, c'est-à-dire une mission concrète confiée par le SRC. Les activités des cantons découlant de la liste d'observation (art. 71) font aussi partie des mandats directs, puisque cette liste est remise chaque année aux cantons avec ordre de rechercher toutes les informations disponibles sur les organisations et groupements qui y figurent et de les transmettre au SRC.

Les activités réalisées de manière autonome par les autorités d'exécution cantonales en application directe de la LRens peuvent en revanche être soumises à la haute surveillance des parlements cantonaux. Cette répartition des compétences en matière de surveillance permet d'éviter des doublons ou des lacunes. Le système d'information INDEX SRC (art. 50) comportera des rubriques spéciales pour les cantons où ces derniers pourront enregistrer leurs informations et qui permettront de distinguer clairement les deux champs de surveillance.

S'agissant des activités menées par les autorités cantonales d'exécution sur ordre direct de la Confédération, le Conseil fédéral est d'avis que le législateur fédéral a réglé la haute surveillance parlementaire de manière exhaustive en créant la Délégation des Commissions de gestion et la Délégation des finances pour la surveillance des activités dans le domaine du renseignement et en leur octroyant des compétences particulières en vertu des art. 51 et 53 de la loi du 13 décembre 2002 sur le Parlement[38]. Il ferait preuve d'inconséquence en donnant en parallèle des compétences aux cantons à l'échelon cantonal.

Art. 78 Surveillance cantonale

Le projet prévoit un partage de la surveillance des autorités d'exécution cantonales entre la Confédération et les cantons.

38 RS **171.10**

Surveillance par la Confédération

La haute surveillance sur l'exécution des mandats fédéraux confiés en vertu de la présente loi et sur les activités correspondantes des autorités d'exécution cantonales incombe à la Délégation des Commissions de gestion des Chambres fédérales. L'organe de surveillance interne au DDPS peut effectuer des contrôles supplémentaires auprès de ces autorités (art. 74, al. 3).

Surveillance par les cantons

Les cantons sont chargés d'assurer une surveillance administrative par les instances auxquelles les autorités d'exécution cantonales sont subordonnées. Celles-ci vérifient:

- que les procédures administratives cantonales correspondent aux prescriptions légales déterminantes,
- que l'autorité d'exécution cantonale traite séparément les données fédérales et les données cantonales,
- comment l'autorité d'exécution s'acquitte des missions qui lui sont confiées par la Confédération,
- où et comment l'autorité d'exécution recherche les informations, et
- que l'autorité d'exécution respecte les exigences en matière de protection des données (sécurité des données, protection de la personnalité).

Cette répartition des tâches correspond au droit en vigueur (art. 6, al. 3, LMSI et art. 35 OSRC) et a donné de bons résultats dans la pratique. Elle doit donc être conservée.

Les dispositions sur la surveillance cantonale prévoient par ailleurs que les organes de surveillance de la Confédération apportent leur soutien à la surveillance administrative exercée par les cantons (par ex. par un organe de surveillance similaire à l'actuelle Surveillance des services de renseignement) et que les services cantonaux qui exercent cette surveillance ont accès aux informations qui leur sont utiles à cet égard(*al. 3*).

Les solutions suivantes ont été examinées pour l'exercice de la surveillance sur les autorités d'exécution cantonales:

a. *Solution exclusivement fédérale*: celle-ci signifierait que l'intégralité de la surveillance sur les autorités d'exécution cantonales serait confiée à la Confédération, plus précisément au SRC. Cette solution globale couvrirait tous les aspects de la surveillance, notamment la surveillance des services et de la protection des données. Dans ce modèle, la Confédération serait seule responsable d'édicter les prescriptions légales en la matière. Les employés chargés de l'exécution de la LMSI qui étaient jusqu'à présent au service d'un canton seraient transférés dans l'administration fédérale.

b. *Solution exclusivement cantonale*: à l'inverse de la solution actuelle, un tel modèle signifierait que la Confédération n'aurait plus aucune compétence pour la surveillance des autorités d'exécution cantonales et que la haute surveillance exercée par la Délégation des Commissions de gestion des Chambres fédérales sur ces dernières tomberait. Les organes chargés de la surveillance cantonale devraient alors être habilités à consulter intégralement

les données qui sont traitées par l'autorité d'exécution cantonale afin de garantir le respect de la protection des données.

La *solution fédérale* a l'avantage de mettre en place une réglementation uniforme de la surveillance des autorités d'exécution cantonales. Elle contredit toutefois la conception fédéraliste de la sûreté intérieure, selon laquelle la Confédération et les cantons se partagent la responsabilité de la sécurité du pays et de la protection de sa population, chacun dans son secteur de compétences (art. 57, al. 1, Cst.). L'introduction d'une solution exclusivement fédérale irait à l'encontre de la structure fédéraliste de notre État et ne bénéficierait pas d'un ancrage local auprès des autorités de sûreté. Elle doit dès lors être rejetée.

La *solution exclusivement cantonale* présente également l'avantage de mettre en place une réglementation uniforme pour tous les cantons. La répartition de la surveillance entre la Confédération et les cantons tomberait: le canton serait seul responsable de la surveillance. Cette solution aurait toutefois l'inconvénient que les parlements cantonaux, à qui incomberait désormais l'intégralité de la haute surveillance sur les activités des autorités d'exécution cantonales, pourraient développer des pratiques différentes. De plus, en cas de solution exclusivement cantonale, les organes cantonaux de surveillance devraient obtenir un accès intégral aux données de la Confédération qui sont traitées par les autorités d'exécution cantonales. Si tel n'était pas le cas, ils ne pourraient pas assumer leur fonction intégrale de surveillance. De la sorte, ils empièteraient obligatoirement sur la sphère de compétence des organes de surveillance fédéraux et entreraient le cas échéant en conflit avec eux. Des questions difficiles de délimitation se poseraient pour la surveillance des missions confiées par l'organe fédéral. Le SRC pourrait aussi devoir rendre des comptes aux organes cantonaux de surveillance, ce qui irait à l'encontre du système. Par conséquent, la solution cantonale ne convainc pas non plus.

Pour toutes ces raisons, le Conseil fédéral est d'avis qu'il faut s'en tenir à une surveillance partagée entre la Confédération et les cantons.

Le principe de la surveillance partagée n'a du reste rien d'inhabituel, puisqu'on ne le retrouve pas uniquement dans le domaine du renseignement: dans la plupart des cantons, la police criminelle dépend en effet du commandement de police, que ce soit d'un point de vue organisationnel ou administratif. Si elle mène toutefois des enquêtes sur ordre des autorités judiciaires, elle se retrouve sous la surveillance de ces dernières.

L'*al. 2* définit et délimite le champ de surveillance qui peut être confié à la responsabilité des organes parlementaires cantonaux, à savoir les activités que les autorités d'exécution mènent dans leur domaine en application directe de la LRens, sans recevoir dans chaque cas une mission formelle du SRC. L'art. 81, al. 1, contient à cet égard un renvoi aux compétences correspondantes des cantons en matière de mesures de recherche autonomes. Cette réorganisation est judicieuse, car les organes fédéraux ne sont en règle générale pas au courant de ces activités cantonales. Il est dès lors plus difficile de les englober dans les activités de surveillance. Grâce à une responsabilité à l'échelon cantonal, on évite des lacunes sans pour autant créer des doublons. Le système d'information INDEX SRC contiendra des rubriques spéciales pour le traitement des données correspondantes et leur contrôle.

Les parlements cantonaux restent évidemment autonomes dans les domaines où les autorités d'exécution cantonales veillent à la sûreté intérieure de leur canton en dehors du champ d'application de la LRens. Cette dernière ne demande pas qu'ils

interviennent exclusivement pour son exécution. En règle générale, il existe des synergies utiles lors de l'exécution de la LRens et de la législation cantonale en matière de police, auxquelles la Confédération ne veut pas mettre un terme.

Art. 79 Voies de droit

La LRens définit des mesures et des décisions parfois intrusives pour lesquelles il faut garantir des voies de droit appropriées. L'*al. 1* prévoit à cet égard la voie judiciaire ordinaire vers le Tribunal administratif fédéral, puis vers le Tribunal fédéral. Ces mesures sont donc clairement exclues du champ d'application de l'art. 83, let. a, de la loi fédérale du 17 juin 2005 sur le Tribunal fédéral[39], qui déclare irrecevable les recours en matière de droit public contre les décisions concernant la sûreté intérieure ou extérieure du pays.

L'*al. 2* dispose que les recours contre les décisions du SRC relatives à l'obligation spécifique faite aux particuliers de fournir des renseignements (art. 24) n'ont pas d'effet suspensif. Aux termes de l'art. 55, al. 1, de la loi fédérale sur la procédure administrative, les recours ont un effet suspensif à moins que le législateur ne prévoie le contraire. S'il fallait attendre l'issue d'une procédure de recours pour obtenir des informations indispensables, il serait la plupart du temps impossible d'apprécier à temps les situations de menaces pour la sûreté intérieure ou extérieure de notre pays. La LRens prévoit donc expressément en sa qualité de loi régissant un domaine spécifique que les recours n'ont pas d'effet suspensif.

L'*al. 3* empêche que des recours retardent la remise au SRC de renseignements nécessaires pour la sûreté du pays jusqu'à ce qu'il soit trop tard pour écarter la menace. Étant donné que, selon les circonstances, la communication d'une mesure de recherche soumise à autorisation n'intervient que longtemps après qu'elle ait pris fin (par ex. pour ne pas mettre en danger d'autres mesures de recherche en cours), l'*al. 3* fixe le début du délai de recours à la date de réception de la communication.

Lors de la procédure de consultation, le Tribunal administratif fédéral a émis quelques doutes sur l'opportunité de lui confier tant une fonction d'instance d'autorisation de certaines mesures qu'une fonction d'autorité de recours. Il a dès lors proposé le Tribunal pénal fédéral comme autorité de recours. Le Conseil fédéral tient toutefois à conserver une séparation très stricte entre les autorités chargées du droit administratif et celles chargées du droit de la procédure pénale il tient aussi à concentrer les compétences juridiques et techniques pour l'appréciation des questions liées au renseignement au sein du Tribunal administratif fédéral. Une réglementation appropriée des compétences au sein du Tribunal administratif fédéral permettra le cas échéant d'éviter d'éventuels conflits d'intérêts entre le président de la chambre autorisant les mesures en tant qu'autorité d'approbation et celui de la chambre fonctionnant comme autorité de recours. Les avantages de la concentration de la procédure dans le domaine du droit administratif l'emportent clairement.

Art. 80 Dispositions d'exécution

Conformément à l'art. 7 LOGA, le Conseil fédéral édicte des ordonnances dans la mesure où la Constitution ou la législation l'y autorise (voir aussi à cet égard l'art. 182, al. 1, Cst.). L'art. 80 charge au surplus le Conseil fédéral d'édicter des

39 RS **173.110**

prescriptions générales en matière d'exécution pour les délégations spéciales prévues par la loi.

Art. 81 Exécution par les cantons

L'*al. 1* pose tout d'abord le principe selon lequel les cantons veillent à l'exécution de la présente loi sur leur territoire en collaboration avec la Confédération. Il y a lieu à cet égard d'apporter quelques précisions sur la répartition des tâches entre la Confédération et les cantons dans le domaine de la sûreté intérieure.

L'art. 57 Cst. contient certes la compétence inhérente de la Confédération de veiller à sa sûreté intérieure et de prendre des dispositions légales là où il est question d'assumer de véritables responsabilités fédérales (mesures pour sa propre protection et pour la protection de ses institutions et de ses organes). La Confédération n'a toutefois qu'une compétence législative sectorielle, et non intégrale, dans le domaine de la sûreté intérieure (voir à cet égard le rapport du Conseil fédéral du 2 mars 2012 donnant suite au postulat Malama « Sécurité intérieure. Clarification des compétences »[40]). Les cantons sont dès lors libres de développer des activités propres et d'édicter des dispositions légales dans le domaine du renseignement, pour autant qu'il ne s'agisse pas de domaines au sein desquels il incombe à la Confédération de légiférer (compétence originelle ou inhérente). Le présent projet de loi concrétise la compétence inhérente de la Confédération pour la sauvegarde de la sûreté intérieure.

S'agissant de la compétence des cantons, le rapport précité précise ce qui suit (pp. 4181 et 4182):

«… La compétence des cantons de veiller sur leur territoire au maintien de la sécurité publique et de l'ordre est réputée compétence originelle des cantons. Ces derniers exercent sur leur territoire la souveraineté en matière de police et disposent à ce titre de la compétence législative dans la perspective de l'accomplissement de leur mandat global de lutte contre les dangers. Le principe de la responsabilité primaire des cantons pour la sécurité sur leur territoire n'est pas contesté par la doctrine et par la jurisprudence. Pour sa part, le Conseil fédéral a confirmé dans sa pratique constante que la législation en matière de police relevait en principe des cantons. Le fait que la Confédération n'ait pas de mandat général de lutte contre les dangers se reflète également sur le plan institutionnel: alors que chacun des 26 cantons dispose de son propre corps de police, on ne trouve au niveau fédéral aucune autorité de police couvrant tous les secteurs d'activités.

Lorsque, dans un domaine matériel donné, la Constitution fédérale ne prévoit aucune attribution de compétences à la Confédération, la compétence pour ce domaine en particulier échoit aux cantons, conformément aux règles générales d'attribution des compétences. Pour les cantons, cela signifie qu'ils sont en droit de s'attribuer toutes les compétences qui n'ont pas été déléguées à la Confédération. Partout où, dans le domaine de la sécurité, aucune compétence spécifique n'est attribuée à la Confédération, les cantons conservent la compétence primaire. L'art. 43 Cst. précise que les cantons déterminent les tâches qu'ils assument dans le cadre de leurs compétences et comment ils accomplissent ces tâches. Ce principe n'est toutefois pas intangible: dans l'exercice de leurs compétences, les cantons ne sont pas toujours libres de définir leurs tâches et la manière de les accomplir, notamment lorsque la Constitution leur confie des tâches particulières ou leur

40 FF **2012** 4161

prescrit la manière d'accomplir une tâche. Dans ces cas de figure, l'autonomie cantonale est restreinte dans la mesure où la Constitution pose certaines exigences quant à l'accomplissement des tâches. On trouve un exemple de cette nature à l'art. 57, al. 1, Cst.; les droits fondamentaux garantis par la Constitution fédérale (art. 35 Cst.) limitent également la marge d'action des cantons.»

Les principes contenus aux *al. 1 et 2* (recherche d'informations, de manière autonome ou sur la base d'un mandat du SRC, communication spontanée au SRC) ont été repris du droit en vigueur (art. 12 LMSI). Ils ont fait leur preuve et doivent être conservés. À la suite d'une suggestion émise par de nombreux cantons lors de la procédure de consultation, l'al. 1 a été complété d'une deuxième phrase contenant une énumération des mesures de recherche non soumises à autorisation que les autorités d'exécution cantonales ont le pouvoir de mettre en œuvre pour exécuter les dispositions de la LRens de manière autonome. Il s'agit de de l'exploitation des sources d'informations publiques (art. 13), de l'observation dans des lieux publics et dans des lieux librement accessibles (art. 14), du recours à des informateurs (art. 15), de la recherche d'informations ou de la réception de communications fournies par d'autres autorités (art. 19 et 20), et de la réception de communications faites par des tiers et de l'interrogatoire de tiers (art. 22 et 24). Les autorités d'exécution cantonales n'exécutent les autres mesures de recherche, en particulier celles sujettes à autorisation, que sur mandat du SRC, mais elles peuvent lui soumettre des demandes à cet effet. Par ailleurs, les autorités d'exécution cantonales peuvent également exercer des activités relevant de leur législation cantonale en matière de police. Aux termes de l'art. 20, al. 1, leurs résultats peuvent aussi être transférés dans le domaine de la LRens lorsque le SRC en a besoin pour accomplir les tâches qui lui sont confiées par la LRens.

Le soutien technique et opérationnel mutuel, tel que prévu aux *al. 3 et 4*, existe depuis des années et permet une utilisation efficace des ressources en personnel et des moyens techniques de la Confédération et des cantons.

L'indemnisation des cantons prévue à l'*al. 5* pour les prestations liées à l'exécution de la présente loi correspond également au droit en vigueur (voir à cet égard l'art. 28, al. 1, LMSI). Au vu de la situation particulière en matière d'exécution, le Conseil fédéral souhaiterait maintenir cette indemnisation spéciale, qui ne couvre qu'une partie des frais engagés par les cantons: les prestations liées à l'exécution de la LRens ne sont pas couvertes par la péréquation financière globale entre la Confédération et les cantons.

Au surplus, le respect des principes de la législation sur les subventions découle, d'une part, du fait que les cantons sont contraints par la loi de désigner une autorité chargée de collaborer avec le SRC pour l'exécution de la présente loi et plus généralement de collaborer à la demande de la Confédération ou du SRC (aménagement et pilotage matériel: voir à ce sujet essentiellement l'art. 9 et les commentaires concernant cet article). Les travaux concernés sont sujets à un contrôle très strict de la part des organes de contrôle et de surveillance de la Confédération et des cantons (cf. section 2 du projet de loi.). D'autre part, l'indemnité accordée aux cantons (qui ne couvre certes pas leurs frais) est une indemnité forfaitaire, mais celle-ci se fonde sur une clé de répartition en fonction du nombre des personnes chargées dans un canton d'exécuter de manière prépondérante des tâches de la Confédération. Cette indemnisation se fait d'ailleurs exclusivement dans le cadre des crédits accordés, ce qui garanti la transparence et les possibilités de pilotage financier. Il faut dès lors maintenir cette pratique efficace: il n'y a aucune raison de s'en écarter.

Abrogation d'autres actes

Le présent projet de loi reprend les dispositions en matière de renseignement de la LMSI, mais non celles du droit policier (protection de personnes et de bâtiments, mesures contre la violence lors de manifestations sportives, saisie du matériel de propagande incitant à la violence). En effet, comme les travaux relatifs à une loi codifiant les tâches de police ont été interrompus, la LMSI doit rester en vigueur pour les domaines régissant le droit policier. Elle sera complétée par de nouvelles dispositions reprises de l'avant-projet de la loi sur les tâches de police et qui sont nécessaires pour l'exécution des dispositions qui restent dans la LMSI. La LMSI ne peut donc pas être abrogée intégralement; seules les parties consacrées au renseignement sont supprimées.

Une nouvelle base légale est également en préparation pour les contrôles de sécurité relatifs aux personnes: la loi sur la sécurité de l'information reprendra cette partie de la LMSI.

La LFRC est en revanche reprise dans son intégralité par la LRens et peut par conséquent être abrogée.

Modification d'autres actes

Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[41]

Remarques préliminaires

Il était prévu à l'origine de transférer les dispositions en matière de police contenue dans la LMSI dans une nouvelle loi, la loi sur les tâches de police (LPol). Si ces dispositions avaient été reprises dans la LPol, la LMSI aurait pu être abrogée. Une procédure de consultation relative à l'avant-projet de LPol (AP-LPol)[42] a été menée auprès des cantons, des partis politiques et d'autres organisations (de novembre 2009 à mars 2010). Le 26 juin 2013, le Conseil fédéral a décidé de suspendre les travaux relatifs aux projets et de modifier ponctuellement, en cas de besoin, les bases légales existantes. La LMSI est donc maintenue, contrairement à ce qui avait été prévu dans l'avant-projet de la LRens (cf. annexe, Abrogation et modification d'autres actes, I, ch. 1), parallèlement à la nouvelle LRens. Son contenu se réduira cependant, à l'entrée en vigueur de la LRens, aux dispositions régissant les tâches de police attribuées à l'Office fédéral de la police (fedpol), à savoir en particulier les mesures concernant le matériel de propagande incitant à la violence, les mesures concernant la violence à l'occasion de manifestations sportives, les tâches de police de sécurité visant à protéger les personnes et les bâtiments de la Confédération et les obligations de protection de personnes et de bâtiments découlant du droit international. Des adaptations rédactionnelles résultant de la création de la LRens ont été apportées aux dispositions maintenues dans la LMSI.

Trois nouvelles réglementations qui figuraient dans l'AP-LPol sont ajoutées à la LMSI. Directement liées aux tâches de sécurité assumées par fedpol en vertu de la

41 RS **120**

42 Ce document peut être consulté à l'adresse suivante: www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2009 > Département fédéral de justice et police

LMSI, elles en garantissent l'exécution: il s'agit des art. 13*f* (mise sous séquestre d'objets dangereux; art. 32 AP-LPol), 23, al. 3bis, (mesures préventives, art. 31 AP-LPol) et 23*a* à *c* (Système d'information et de documentation du Service fédéral de sécurité; art. 75 s. AP-LPol). Ces dispositions ont déjà été contrôlées dans le cadre de la procédure de consultation de l'AP-LPol. Le résultat de cette consultation n'a pas mis en évidence la nécessité de procéder à leur modification[43], aussi sont-elles reprises presque tel quel dans la présente modification de la LMSI.

Le principe de l'unité de la matière requiert d'un projet qu'il présente une unité matérielle et qu'un lien clair relie ses différents domaines thématiques. Cette exigence est remplie. Le nouveau champ d'application de la LMSI ne la relie certes pas directement à la LRens, mais ces deux lois sont unies par un lien plus large: tant les tâches et les compétences de la Confédération en matière de renseignement que ses tâches limitées de sécurité maintenues dans la LMSI servent un but supérieur, à savoir garantir la sûreté intérieure dans le domaine de compétence de la Confédération. Par ailleurs, fedpol assume aussi des tâches de sécurité en dehors du domaine susmentionné (protection des personnes et des bâtiments de la Confédération et des personnes jouissant d'une protection en vertu du droit international public). Ainsi, la Police judiciaire fédérale (PJF) peut se voir amenée, dans le cadre de l'accomplissement de ses tâches, à protéger ses propres enquêteurs et les procureurs concernés, mais aussi des tiers non impliqués (passants, voisins, etc.) quand des personnes présumées violentes sont arrêtées. Dans le cadre de l'exécution d'une mesure de contrainte prévue par la procédure pénale, la PJF assume donc aussi, en appoint, des tâches de sécurité (prévention des risques). Cette fonction n'est toutefois pas autonome, dans le sens qu'elle est toujours liée à un mandat concret de police criminelle. Elle ne relève pas non plus du domaine de la sécurité intérieure et ne fait par conséquent pas l'objet de la présente modification de la LMSI.

Art. 2 Tâches

Cette disposition a été reformulée parce que la LMSI ne régit désormais plus que les tâches de fedpol.

Al. 1: Les activités de renseignement dans les domaines du terrorisme, de l'espionnage, du trafic d'armes et du transfert de technologie sont désormais réglées dans la LRens (cf. art. 6, al. 1). Ainsi, l'ensemble des «mesures au sens de la présente loi», à savoir le LMSI, sont désormais qualifiées de mesures «policières». L'al. 2 précise de quels domaines ces mesures relèvent.

Les *al. 2 et 3* de la LMSI en vigueur peuvent être abrogés puisque leur contenu est intégralement repris dans la LRens. L'actuel al. 4 devient ainsi l'al. 2.

Al. 2: L'évaluation périodique de la menace et le traitement des informations relatives à la sûreté intérieure et extérieure (art. 2, al. 4, let. a et b, de la LMSI en vigueur) ont été retirés de la liste des tâches policières préventives car elles sont désormais réglées dans la LRens. Les quatre domaines restants sont repris tels quels. La nouvelle let. d complète la liste (mise sous séquestre d'objets dangereux).

43 Cf. rapport sur le résultat de la procédure de consultation concernant l'avant-projet de loi fédérale sur les tâches de police de la Confédération, Office fédéral de la police, octobre 2010, pp. 24 et 25 (art. 31 et 32 AP-LPol) et p. 29 (art. 75s. AP-LPol).

Art.. 3 Limites

Les limites posées au traitement des informations en lien avec la recherche et l'analyse d'informations relevant du renseignement sont désormais réglées dans la LRens (cf. art. 5, al. 5 et 6). Les domaines restés dans la LMSI n'ont pas besoin d'une réglementation générale concernant les limites posées au traitement des informations, étant donné qu'ils disposent de règles spécifiques à ce sujet (cf. art. 20, al. 1, dernière phrase, qui porte sur les contrôles de sécurité relatifs aux personnes et le nouvel art. 23*b*, al. 3, concernant le système d'information du Service fédéral de sécurité). Cette disposition peut par conséquent être abrogée.

Art. 5 Tâches exécutées par la Confédération

Pour fixer le niveau de protection dont doivent bénéficier les représentations diplomatiques et consulaires étrangères, fedpol se fonde sur le plan directeur du Conseil fédéral. Ce mandat de protection incombe, en vertu de la répartition des compétences prévue par la Constitution en matière de sécurité intérieure, en premier lieu aux cantons, tandis que la Confédération exerce une fonction de conseil et de coordination (cf. rapport du Conseil fédéral donnant suite au postulat Malama 10.3045 «Sécurité intérieure. Clarification des compétences»[44]).

Les al. 2 et 3 de la LMSI en vigueur réglant des domaines désormais régis par la LRens (cf. art. 9 et 11 LRens), ils ne figurent plus dans la version révisée de l'article.

Art. 5a

Le contenu de cette norme étant régi par la LRens, il faut l'abroger dans la LMSI.

Art. 6, al. 1

La norme est adaptée au nouveau contenu de la LMSI: fedpol est désormais le seul partenaire pour la collaboration avec les cantons.

Art. 7 à 9

Ces normes règlent des tâches spécifiques au SRC et doivent par conséquent être abrogées dans la LMSI.

Art. 10 Devoir d'information de fedpol

La norme est adaptée au nouveau contenu de la LMSI: fedpol est désormais la seule autorité soumise à ce devoir d'information.

Art. 10a à 13d

Ces normes règlent des tâches spécifiques au SRC et doivent par conséquent être abrogées dans la LMSI.

44 FF **2012** 4161 4205, ch. 2.3.2.2.1.2

Art. 13e, al. 2

Le SRC apparaît pour la première fois à cet endroit dans la version remaniée de la LMSI. Il faut donc introduire son nom complet en plus de son sigle.

Art. 13f Mise sous séquestre d'objets dangereux

Conformément à l'art. 28*a* de la loi du 20 juin 1997 sur les armes (LArm)[45], le port d'objets dangereux dans les lieux accessibles au public et la détention de tels objets à bord d'un véhicule sont interdits s'il ne peut être établi de manière plausible qu'ils sont justifiés par un usage ou un entretien conforme à leur destination et s'il y a lieu de penser que les objets en question seront utilisés de manière abusive, notamment pour intimider, menacer ou blesser des personnes. Par objets dangereux au sens de l'art. 4, al. 6, LArm, on entend les objets qui, tels les outils, les ustensiles ou le matériel de sport, peuvent être utilisés pour menacer ou blesser des êtres humains. Les couteaux de poche tels que les couteaux de l'armée suisse et autres produits comparables ne sont pas considérés comme des objets dangereux. Selon l'art. 31, al. 1, let. c, LArm, l'autorité compétente met sous séquestre les objets dangereux portés de manière abusive; si les conditions de l'art. 31, al. 3, LArm, sont réunies, elle peut les confisquer définitivement. L'art. 38, al. 1, LArm dispose que l'exécution incombe aux cantons dans la mesure où elle ne relève pas de la Confédération.

Conformément à l'*art. 13f*, fedpol est désormais autorisé, dans son domaine de compétence, à mettre sous séquestre les objets dangereux de ce type. Dans le cadre de la protection des autorités et des bâtiments de la Confédération, il est indispensable que fedpol mette lui-même ces objets dangereux sous séquestre et les confisque définitivement. Lorsqu'il accomplit ses tâches de sécurité relevant de la police criminelle, fedpol doit en outre pouvoir assurer la sécurité des personnes impliquées et empêcher les tentatives d'intimidation et les menaces.

Art. 14, al. 1

La disposition a été adaptée au nouveau contenu de la LMSI: elle ne s'applique plus qu'à fedpol, et non aux «organes de sûreté de la Confédération» en général.

Art. 14a à 18

Ces normes règlent des tâches spécifiques au SRC et doivent par conséquent être abrogées dans la LMSI.

Art. 21, al. 2

Cette modification est purement formelle.

Art. 23, al. 1, let. a et c, et 3bis

Al. 1, let. a et c: Cette norme a été doublement précisée. D'une part, elle indique clairement que seules les personnes qui exercent une fonction d'intérêt public pour la Confédération peuvent en principe être protégées, comme les parlementaires fédéraux, les magistrats et certains agents de la Confédération. Ces personnes figu-

45 RS **514.54**

rent déjà dans l'ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale[46]. D'autre part, ces personnes doivent être particulièrement exposées à des risques en raison de la fonction qu'elles exercent pour avoir un droit à des mesures de protection. La durée de ces mesures en résulte: elles ne sont accordées qu'aussi longtemps que la personne exerce pour la Confédération une fonction présentant des risques particuliers. Par exemple, si l'une de ces personnes se retrouve pour des raisons strictement privées dans une situation dangereuse ou est menacée, ce sont, comme pour tout citoyen, les autorités policières cantonales qui sont responsables de sa protection en vertu de leur pleine compétence en matière de sûreté.

L'art. 23, al. 1, let. c, (bâtiments et manifestations pour lesquels les tâches de protection sont confiées à d'autres services) n'a jamais été appliqué et doit par conséquent être abrogé.

Al. 3bis: C'est désormais la police – le Service fédéral de sécurité de fedpol (SFS) ou, le cas échéant, la police cantonale – qui est habilitée à entrer directement en contact avec une personne susceptible de constituer une menace sérieuse pour une personne ou des bâtiments à protéger. La police confrontera la personne aux indices concrets donnant à penser qu'elle va commettre une infraction et l'informera des conséquences pénales qu'elle encoure si elle passe à l'acte (mesures préventives). La personne concernée doit prendre conscience des mesures policières ou des mesures de droit administratif qui seront prises selon son comportement. Les expériences faites en Allemagne et dans le canton de Zurich dans le domaine de la violence domestique, mais aussi avec les hooligans durant l'EURO 2008, ont montré que les personnes constituant des menaces potentielles peuvent être dissuadées de mener à bien leurs projets lorsque la police s'adresse directement à elles. Les mesures préventives susmentionnées sont de nature non formelle. Elles sont consignées dans le système d'information et de documentation visé à l'art. 23a. Elles n'ont pas de conséquences pour la personne concernée et ne sont transmises à aucune autre autorité ou registre.

Art. 23a Système d'information et de documentation

Al. 1: En vertu de l'art. 17, al. 2, LPD, le traitement des données doit se fonder sur une base légale formelle étant donné que le SFS traite aussi des données personnelles. Actuellement, le traitement des informations collectées par le SFS pour accomplir son mandat de protection visé à la section 5 de la LMSI se fonde sur l'art. 3, al. 4, LMSI. L'art. 13 OSF précise cette norme. À l'origine, il était prévu d'élaborer une nouvelle base légale formelle dans le projet de révision LMSI II. Après le renvoi du projet à fedpol en août 2005 pour remaniement la nouvelle réglementation a été intégrée à la LPol. Ce projet législatif ayant été suspendu, la nouvelle réglementation doit désormais être intégrée à la LMSI.

Pour le traitement des informations du SFS relevant du domaine de l'art. 22, al. 1, LMSI, l'AP-LPol avait prévu deux systèmes d'information indépendants, à savoir un tableau des événements et une banque de données relatives aux personnes menacées (art. 75 et 76 AP-LPol). Certains participants à la consultation ont déploré que la délimitation entre les deux systèmes d'information ne soit pas très claire. Cette critique a été prise en considération: les deux systèmes d'information, actuellement

46 RS **120.72**

gérés séparément, seront regroupés dans un seul système. C'est de ce système dont il est question dans le nouvel art. 23a et dans les articles suivants. Il ressort de l'art. 14, al. 1, dont la teneur est générale, que le service compétent de fedpol est autorisé à rechercher les informations nécessaires. Le présent art. 23a crée donc la base légale formelle spécifique au système d'information électronique du SFS.

Al. 2: Afin de pouvoir accomplir son mandat de protection, fedpol requiert et traite des informations concernant des événements présentant un intérêt pour la sécurité et des informations concernant des personnes liées à ces événements. Il est en effet possible de déduire des événements les dangers qu'encourent des personnes ou les risques auxquels sont exposés des bâtiments. Ces événements doivent être documentés afin de pouvoir être analysés en dehors de l'actualité du jour et être situés dans un contexte plus large. Les informations relatives à ces événements sont issues à quelque 90 % de sources accessibles au public. Le cercle des personnes concernées par des événements présentant un intérêt pour la sécurité comprend deux catégories de personnes différentes: d'une part les personnes devant être protégées par fedpol et d'autre part les personnes susceptibles de menacer les personnes et les installations. Pour que les données d'une personne figurent dans le système d'information, il faut que des indices concrets laissent supposer qu'elle représente un danger pour certaines personnes et certains bâtiments.

Art. 23b Données, catégories de données et limites du traitement des données

Al. 1: Des données de sources très différentes sont saisies et traitées dans le système d'information. La saisie de données fait le plus souvent suite à une lettre de menace, anonyme dans la plupart des cas. Afin de pouvoir évaluer la dangerosité d'une personne, il est important de savoir dans quelle mesure une personne est encline à la violence, de quelle manière cette tendance à la violence s'est développée dans le passé et si cette personne a déjà été condamnée pour des infractions avec violence. Dans le but d'identifier l'auteur des menaces et de juger de sa dangerosité, il est nécessaire de regrouper toutes les informations pertinentes à partir de différences sources. La majorité des informations proviennent de sources accessibles au public.

Al. 3: Cette disposition fixe les limites du traitement des informations. Elle est tirée de l'art. 3, al. 1, de la LMSI en vigueur (lequel est abrogé, comme expliqué plus haut). Pour un commentaire détaillé, on se référera au commentaire de l'art. 5, al. 5 et 6, LRens, qui a trait au même sujet.

Art. 23c Droits d'accès et communication de données

Il existe plusieurs types d'accès aux données: seules quelques unités organisationnelles de fedpol, à savoir les services qui apprécient la menace ou qui accomplissent des tâches de protection des personnes et de l'État, disposeront d'un accès direct en ligne (*al. 1).* Les services et les personnes figurant à l'*al. 2* peuvent se voir communiquer des données dans des cas concrets. Ainsi, les collaborateurs contrôlant l'accès aux bâtiments où siègent les chefs de départements doivent par exemple pouvoir être informés de la présence d'individus représentant un danger pour le conseiller fédéral qui se trouve dans le bâtiment. Outre l'identité de l'individu et sa photo, des données spécifiques à sa personnalité comme sa propension à la violence peuvent être transmises. Ce genre de données peut également être communiqué aux fins de protection des personnes jouissant d'une protection en Suisse en vertu du droit international public. Ainsi, les représentations étrangères peuvent recevoir des informations sur

des personnes qui constituent un danger pour la sécurité de leurs chargés d'affaire. De la même manière, ces informations peuvent par exemple être communiquées à des entreprises de sécurité privées assurant la surveillance de bâtiments sur mandat de fedpol.

Art. 25 à 27

Le contenu de ces dispositions figure désormais dans la LRens: elles doivent par conséquent être abrogées dans la LMSI.

Art. 28, al. 1

L'indemnisation des prestations fournies par les cantons dans la recherche d'informations relevant du renseignement est désormais régie par l'art. 81, al. 5, LRens. Cette norme peut par conséquent être abrogée dans la LMSI.

Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile[47]

Art. 9, al. 1, let. c et l, et 2, let. c et k

Les autorités fédérales responsables de la sûreté intérieure sont aujourd'hui mentionnées à l'art. 9, al. 1, let. c (accès en ligne), mais cet accès en ligne au système d'information de l'Office fédéral des migrations est limité pour le SRC à l'examen de mesures d'éloignement, ce qui ne couvre pas l'ensemble des tâches du SRC. Ce dernier intervient en effet dans de nombreuses procédures touchant aux domaines des étrangers et de l'asile afin d'évaluer les risques pour la sûreté intérieure ou extérieure. Le projet fixe dès lors les conditions d'accès en ligne sur la base des tâches légales du SRC et les règle dans une lettre séparée de l'art. 9, al. 1. Étant donné que la loi fédérale du 16 décembre 2005 sur les étrangers[48] et la loi fédérale du 26 juin 1998 sur l'asile[49] contiennent de nombreuses réserves en cas de menace pour la sûreté intérieure ou extérieure, le présent texte de loi ne renvoie pas spécifiquement aux dispositions concernées.

Il en va de même par analogie pour l'al. 2, let. c et k.

Loi du 17 juin 2005 sur le Tribunal administratif fédéral[50]

Art. 23, al. 2, et 36b

La let. b est ajoutée à l'art. 23, al. 2, pour donner au président de la cour compétente du Tribunal administratif fédéral la compétence d'autoriser des mesures de recherche d'informations soumises à autorisation et l'exploration du réseau câblé.

47 RS **142.51**
48 RS **142.20**
49 RS **142.31**
50 RS **173.32**

L'art. 36*b* fixe le principe de la compétence du Tribunal administratif fédéral pour l'autorisation de mesures de recherche d'informations du SRC.

Art. 33, let. b, ch. 4

Le recours contre les décisions du Conseil fédéral liées à l'interdiction d'exercer une activité (art. 72) doit être prévu explicitement, car il n'est pas compris pour l'heure dans l'énumération exhaustive de l'art. 33, let. b.

Code civil[51]

Art. 43a, al. 4, ch. 5

Le complément apporté à cette disposition donne au SRC accès au système Infostar (registre de l'état civil) afin d'identifier des personnes ainsi que leur lieu de séjour actuel, voire passé. Le Conseil fédéral va cependant devoir régler plus en détail dans l'ordonnance l'accès en ligne du SRC à Infostar (par ex. s'agissant de son étendue). La numérotation tient compte de la révision en cours de cet article, qui donnera la possibilité à d'autres services d'y accéder. Les accès du SRC se feront par des interfaces analogues à celles qu'utilisent d'autres services de la Confédération et des cantons.

Code pénal[52]

Art. 317bis, al. 1 et 2

Le renvoi à la LMSI est remplacé par un renvoi à la LRens.

Art. 365, al. 2, let. r à u

Les tâches pour l'exécution desquelles le SRC a besoin d'un accès en ligne au casier judiciaire informatisé (VOSTRA) sont énumérées dans ces lettres. Le SRC dispose déjà d'un accès en vertu de l'art. 367, al. 3, CP en relation avec l'art. 21, al. 4, de l'ordonnance du 29 septembre 2006 sur le casier judiciaire (ordonnance VOSTRA)[53], mais il est limité à l'entrée en vigueur d'une base légale au sens formel, qui verra le jour avec la LRens. Les nouvelles dispositions précisent les buts pour lesquels le SRC doit avoir accès au système et renvoient aux dispositions pertinentes de la LRens.

Art. 367, al. 2, let. m, et 4

Le SRC doit également être mentionné formellement à l'art. 367 CP, qui énumère les autorités ayant accès en ligne au casier judiciaire. Pour accomplir les tâches que lui confie la loi, le SRC doit en effet non seulement connaître les jugements pénaux prononcés (cf. art. 367, al. 2, let. m; y compris les acquittements assortis de mesures

51 RS **210**
52 RS **311.0**
53 RS **331**

judiciaires), mais aussi les procédures pénales en cours (cf. art. 367, al. 4). On évite ainsi que des activités de renseignement se recoupent avec celles des organes de poursuite pénale et on permet au SRC de donner des renseignements corrects aux autorités étrangères de sûreté qui demandent des informations au sens de l'art. 12, al. 1, let. d, LRens pour clarifier si une personne présente des risques. S'agissant de la transmission de renseignements se rapportant à des procédures pénales en cours, le SRC s'entendra comme auparavant avec l'autorité de poursuite pénale compétente afin d'éviter tout impact négatif sur les enquêtes en cours.

Code de procédure pénale[54]

Art. 289, al. 4, let. a

Les modifications apportées à cette disposition sont purement rédactionnelles. Elles visent à assurer la cohérence terminologique du code de procédure pénale avec la LRens et le code pénal.

Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[55]

Dans le domaine des accès aux systèmes d'information de police, la LRens se contente de mettre à jour les bases légales existantes (art. 15 LSIP, système de recherches informatisées de police) et d'inscrire dans la loi la possibilité de diffuser des signalements en vue de rechercher des personnes et des objets conformément à l'art. 16 LRens. L'accès aux données ne sera pas donné à l'ensemble du personnel du SRC, mais seulement aux collaborateurs qui en ont besoin pour remplir leurs tâches légales. Comme il est d'usage, c'est le Conseil fédéral qui fixera en détail dans les ordonnances d'exécution le cercle des collaborateurs du SRC autorisés à accéder à ces données et l'étendue de leur droit d'accès.

Loi du 3 février 1995 sur l'armée[56]

Art. 99, al. 1bis, 1^{quater} et 3bis

La disposition régissant l'exploration radio effectuée par le Service de renseignement de l'armée figure à l'art. 99, al. 1bis. Jusqu'à présent, l'art. 99, al. 1bis, renvoyait à l'art. 4*a* LFRC.

L'al. 1^{quater} met à la disposition du Service de renseignement de l'armée les mêmes moyens d'observation depuis les airs que pour le SRC (art. 14 LRens) et reprend également les mesures de protection de la sphère privée prévues dans la LRens.

L'al. 3bis correspond à l'art. 68, al. 2, LRens.

54 RS **312.0**
55 RS **361**
56 RS **510.10**

Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[57]

Art. 16, al. 1, let. h

Le SRC aura désormais accès en à la banque de données SIPA afin de pouvoir identifier les menaces pour la sûreté de l'armée émanant de personnes qui appartiennent par exemple à des groupements extrémistes violents et qui sont incorporées dans l'armée. L'objectif est d'empêcher que des personnes enclines à la violence mettent en péril la sécurité de l'armée et soient formées par l'armée au maniement d'armes et d'explosifs et aux techniques de combat.

Loi du 21 mars 2003 sur l'énergie nucléaire[58]

Art. 101, al. 3

L'office central ATOME, dont il est question ici, est subordonné au SRC. La tâche de cet office consiste à rechercher et à traiter les données nécessaires pour exécuter la loi sur l'énergie nucléaire, pour prévenir des délits et pour lancer des poursuites pénales. La pratique a montré qu'il était nécessaire d'étendre le champ d'activités de l'office central au domaine de la loi du 22 mars 1991 sur la radioprotection[59], qui est étroitement lié à celui de la loi sur l'énergie nucléaire. Cette modification permet d'éviter des questions de délimitation sur le type de substances radioactives (matériel fissible ou non fissible), qui sont certes déterminantes pour leur affectation au champ d'application des deux lois en question mais qui ne sont pas importantes dans la pratique du renseignement ou qui ne peuvent, par exemple, pas encore être évaluées lors de la réception du traitement d'un cas de trafic nucléaire.

Loi fédérale du 19 décembre 1958 sur la circulation routière[60]

Art. 104c, al. 5, let. c

L'adaptation de l'art. 104*c*, al. 5, donne au SRC le droit d'accéder en ligne au registre des autorisations de conduire La vérification des autorisations de conduire délivrées à une personne déterminée est nécessaire pour préparer de manière suffisante l'exécution de mesures relevant du renseignement telles que des observations.

57 RS **510.91**
58 RS **732.1**
59 RS **814.50**
60 RS **741.01**

Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[61]

Cette loi fait actuellement l'objet d'une révision totale pour adapter la surveillance de la correspondance par poste et télécommunication aux nouveaux besoins[62].Le projet de révision ne change pas la pratique, puisqu'il n'autorise que les surveillances en vue d'une poursuite pénale et pour des buts policiers définis très précisément. La LRens étend cependant le but de la surveillance au domaine du renseignement, ce qui requiert une modification de la LSCPT.

Un message ne peut cependant modifier qu'un texte existant. Voilà pourquoi le message de la LRens se réfère à la LSCPT en vigueur dans les modifications d'autres actes législatifs. L'harmonisation avec la révision totale de la LSCPT aura lieu lors des délibérations parlementaires au sujet de la LRens et de la LSCPT et, le cas échéant, à leur entrée en vigueur.

Les commentaires ci-après portent donc sur les modifications à apporter à la LSCPT pour étendre la surveillance à des buts relevant du renseignement.

Art. 1, al. 1, let. d

Le SRC peut désormais ordonner une surveillance de la correspondance par poste et de la correspondance par télécommunication (art. 25, al. 1, let. a à d). L'exécution de ces mesures doit respecter les procédures prévues dans la LSCPT et passer par l'organe compétent en la matière au sein du DFJP, à savoir le SSCPT. À cette fin, le SRC doit être inscrit dans la LSCPT comme organe habilité à donner un tel ordre.

Art. 11, al. 1, let. a, et 13, al. 1, let. a

Dans ces deux dispositions, le SRC est désormais également désigné comme organe habilité à confier des missions de surveillance. Cette modification découle de la compétence du SRC de faire surveiller la correspondance par poste et télécommunication d'une personne, telle qu'elle est prévue à l'art. 25, al. 1, let. a à d, LRens.

Art. 14, al. 2bis

Le renvoi à la LMSI a été remplacé par un renvoi à la LRens.

Coordination avec la révision totale de la LSCPT

On trouvera ci-après un aperçu des modifications à apporter au projet de révision totale de la LSCPT tel que présenté dans le message du 27 février 2013 (sous réserve des délibérations et des décisions des Chambres fédérales). Les dispositions existantes sont reprises telles quelles du projet de révision totale.

61 RS **780.1**
62 FF **2013** 2483

Préambule

vu les art. 57, al. 2, 92, al. 1, et 123, al. 1, de la Constitution[63],
vu le message du Conseil fédéral du 27 février 2013[64],

Art. 1, al. 1, let. e

[1] La présente loi s'applique à la surveillance de la correspondance par poste et télécommunication qui est ordonnée et mise en œuvre:

e. dans le cadre de l'exécution de la loi du … sur le renseignement (LRens)[65].

Art. 5, al. 1

[1] Le DFJP peut mettre en place un organe consultatif composé de représentants du DFJP, du service, des cantons, des autorités de poursuite pénale, du Service de renseignement de la Confédération (SRC) et des fournisseurs de services postaux et de télécommunication.

Art. 10, al. 2bis

[2bis] Le droit d'accès aux données collectées lors de l'exécution de la LRens est régi par la LRens.

Art. 11, al. 3bis

[3bis] Les données collectées lors de l'exécution de la LRens sont conservées dans le système de traitement aussi longtemps que le but poursuivi l'exige, mais trente ans au plus depuis la fin de la surveillance.

Art. 14a Interface avec le système d'information du SRC

[1] Une copie des données contenues dans le système de traitement peut être transférée en ligne dans le système d'information visé à l'art. 56 LRens, pour autant:

a. que le droit applicable autorise le traitement des données dans ce système, et

b. qu'il soit garanti que seules les personnes en charge de la mesure concernée puissent accéder aux données.

[2] Le transfert ne peut être effectué que par une personne qui a le droit d'accéder au système de traitement au sens de la présente loi et au système d'information considéré au sens de la LRens.

Art. 15, al. 1, let. d et al. 2, let. a

[1] Le service fournit des renseignements sur les données mentionnées aux art. 21 et 22 exclusivement aux autorités et aux fins suivantes lorsque ces autorités le demandent:

b. au SRC, afin d'accomplir les tâches qui lui sont confiées par la LRens.

63 RS **101**
64 FF **2013** 2379
65 RS …

[2] Le service fournit des renseignements sur les données mentionnées à l'art. 21 exclusivement aux autorités et aux fins suivantes lorsque ces autorités le demandent:

a. au SRC, pour l'exécution de la LRens;

Art. 22a Renseignements visant à identifier des personnes en cas de menace pour la sûreté intérieure ou extérieure

Lorsqu'il existe suffisamment d'indices laissant supposer la commission, présente ou passée, par Internet d'une menace pour la sûreté intérieure ou extérieure, les fournisseurs de services de télécommunication fournissent au service toute indication permettant d'identifier son auteur ou sa provenance.

Par ailleurs, l'art. 24 LRens devrait renvoyer à l'art. 15 LSCPT (avec la date de la révision totale) pour les informations sur les raccordements de télécommunication.

Dans la révision totale de la LSCPT, les mesures de surveillance ne sont plus présentées de la même manière que dans la loi actuelle. La présentation de la LRens devrait donc être adaptée comme suit à celle de la LSCPT et du code de procédure pénale (les commentaires relatifs aux différentes dispositions correspondent à ceux du message relatif à la révision totale de la LSCPT):

Art. 25, al. 1, let. a et a^{bis} (LRens)

[1] Les mesures suivantes sont soumises à autorisation:

a. faire surveiller la correspondance par poste et la correspondance par télécommunication et demander des données secondaires du trafic postal et de télécommunication conformément à la loi fédérale du … sur la surveillance de la correspondance par poste et télécommunication[66];

a^{bis}. utiliser des appareils techniques particuliers pour surveiller la correspondance par télécommunication, saisir des transmissions ou identifier une personne, un objet ou le lieu où ils se trouvent lorsque la surveillance en vertu de la let. a est restée vaine, n'aurait aucune chance d'aboutir ou serait excessivement difficile et que les autorisations en vertu du droit des télécommunications pour la mise en œuvre d'appareils techniques particuliers ont été données;

Loi du 30 avril 1997 sur les télécommunications[67]

Art. 34, al. 1ter et 1^{quater}

Le SRC est désormais également mentionné à l'al. 1ter. Cette modification découle de l'art. 7, al. 1, let. d, LRens.

Remarque globale sur les lois modifiées aux ch. 14 à 20

Les actes législatifs concernés n'ont subi que des adaptations formelles dans les articles se rapportant à la communication de données. À chaque fois, le renvoi à la

66 RS **780.1**
67 RS **784.10**

LMSI est remplacé par un renvoi à la LRens, sans aucune autre modification matérielle.

Dans quelques lois, le renvoi introduit par la LMSI II à la communication de données au SRC «dans des cas d'espèce et sur demande écrite et motivée» est supprimé. Ce renvoi s'est avéré inutile, car la communication de données au SRC est déjà prévue dans une autre disposition des lois concernées. Il s'agit dès lors d'une simple correction d'une erreur du législateur, et non d'une modification de la situation juridique.

Loi fédérale du 19 juin 1992 sur l'assurance militaire[68]

Art. 1a, al. 1, let. q

Cette disposition fait pendant à l'art. 35, al. 6, LRens, qui prévoit que les collaborateurs du SRC engagés à l'étranger sont soumis à l'assurance militaire. Elle doit aussi être inscrite dans la loi fédérale sur l'assurance militaire.

Art. 95a, al. 1, let. hbis et i, ch. 8

Le renvoi à la LMSI est remplacé par un renvoi à la LRens (cf. remarque globale ci-avant).

3 Conséquences

3.1 Conséquences pour la Confédération

3.1.1 Conséquences financières

Les conséquences financières dépendent très largement des modalités d'application de la réalisation des différentes mesures et de leur fréquence. Au vu de l'état actuel de la menace, le Conseil fédéral estime qu'une dizaine de cas nécessiteront des mesures au titre de la LRens chaque année, un cas pouvant toutefois comporter plusieurs mesures.

Les moyens et les systèmes techniques à engager pour la localisation à l'étranger ainsi que les moyens aériens et spatiaux pour l'observation sont connus et établis. Leurs conséquences financières peuvent donc être estimées de manière assez fiable. Les coûts d'acquisition et d'investissements de ces systèmes sont de l'ordre de cinq à sept millions de francs par an, auxquels il faut ajouter des frais récurrents de quelque 800 000 francs pour la maintenance, l'adaptation et le coût des licences. En règle générale ces systèmes sont acquis et financés dans le cadre du programme d'armement.

Pour les mesures de recherche d'informations soumises à autorisation en Suisse, par exemple la localisation, la surveillance de données d'utilisation et de communication de raccordements de téléphonie fixe et mobile ou la surveillance d'accès à Internet, le SRC fera appel au service «Surveillance de la correspondance par poste et télécommunication» (SSCPT) du DFJP, qui est compétent en la matière. Sur la base du

68 RS **833.1**

nombre de cas estimés, les indemnités à verser pour ces mesures devraient s'élever à quelque 500 000 francs par an.

Quelque 800 000 francs doivent être inscrits au budget pour la traduction des communications enregistrées.

Les coûts pour l'indemnisation de l'exploration du réseau câblé (art. 38 ss) sont également estimés, par analogie au montant de l'indemnisation de la surveillance des télécommunications par le SSCPT, à 500 000 francs par an.

Certaines technologies, par exemple pour l'introduction dans des systèmes informatiques hautement sécurisés, ne sont encore que peu développées. Comme le marché pour ces systèmes est relativement limité et volatile et que les développements techniques dans ce domaine sont rapides, leurs coûts ne peuvent pour l'instant que faire l'objet d'estimations.

L'équipement et la formation des nouveaux collaborateurs devraient entraîner des coûts de quelque 720 000 francs, soit 35 000 francs par poste à temps complet.

3.1.2 Conséquence sur l'état du personnel

Les nouvelles mesures de recherche d'informations proposées doivent être réalisées autant que possible dans le cadre des structures en place (SRC, Base d'aide au commandement de l'armée, SSCPT). Il faudra néanmoins créer environ 20,5 postes supplémentaires. Le SRC aura besoin de techniciens opérationnels pour le suivi technique des moyens de recherche soumis à autorisation, d'analystes pour l'évaluation opérationnelle des informations obtenues à l'aide des mesures soumises à autorisation, de juristes pour la préparation des demandes pour ces mesures, leur contrôle et l'élaboration des rapports concernant ces mesures et de divers postes supplémentaires pour la garantie de la qualité des nouveaux systèmes et le suivi de l'exploration du réseau câblé. Le Tribunal administratif fédéral aura lui aussi besoin de postes supplémentaires pour assurer la procédure d'autorisation des mesures de recherche, les Archives fédérales pour l'archivage décentralisé dans les locaux du SRC et le Centre des opérations électroniques de la Base d'aide au commandement de l'armée pour l'essai-pilote de l'exploration du réseau câblé. Ces 20,5 postes devront être pourvus progressivement, à savoir 12 postes de travail prioritaires la première année et 8,5 postes de travail la deuxième année.

L'augmentation des exigences pour la gestion des données peut en grande partie être assumée avec les ressources disponibles.

3.1.3 Autres conséquences

Les prestations de soutien en faveur de tiers ne peuvent, par nature, pas être planifiées. La mise à disposition des ressources financières et de personnel doit être réglée dans chaque cas avec le destinataire ou le mandant de ces prestations. Elle dépend notamment des possibilités du SRC.

Les missions du SRC dans des situations particulières en vue de sauvegarder des intérêts essentiels du pays au sens de l'art. 3 ne sont pas non plus planifiables. Aucun poste ou moyen supplémentaire ne sera cependant demandé: si les moyens,

ressources et connaissances spécifiques dont il dispose s'avèrent insuffisants pour une telle mission, le SRC devra demander séparément ce dont il a besoin.

3.2 Conséquences pour les cantons et les communes, ainsi que pour les centres urbains, les agglomérations et les régions de montagnes

Selon le projet de loi, le SRC assure ses tâches de renseignement en collaboration avec les autorités d'exécution cantonales.

La forme actuelle d'organisation décentralisée et de collaboration étroite entre le SRC et les cantons est maintenue. Comme auparavant, les cantons sont les premiers responsables de la sûreté intérieure sur leur territoire. Dans la mesure où la Constitution et la loi en confient la responsabilité à la Confédération, les cantons lui fournissent assistance administrative et judiciaire. Le SRC travaille en étroite collaboration avec la CCPCS et la CCDJP.

Lors de menaces spécifiques et conformément au principe d'assistance, toutes les autorités et unités administratives des cantons ont l'obligation de fournir des renseignements. Les renseignements peuvent être demandés par le SRC ou par les autorités d'exécution cantonales.

Dans le cadre du champ d'application du projet de loi, les autorités d'exécution des cantons ne gèrent plus de banques de données qui leur sont propres. En revanche, elles disposent d'un droit d'accès aux informations du SRC nécessaires à l'accomplissement de leurs tâches. Pour les autorités d'exécution cantonales, le projet prévoit un droit d'accès en ligne au système INDEX SRC. Grâce à cet accès, ces autorités peuvent notamment consulter les données des enquêtes préliminaires qu'elles ont effectuées et les rapports qu'elles ont établis.

L'organe du DDPS chargé de la surveillance du renseignement peut procéder à des contrôles dans les domaines dans lesquels les autorités d'exécution cantonales appliquent les dispositions du présent projet.

La haute surveillance parlementaire est traitée dans les commentaires concernant l'art. 73.

Le SRC contribuera comme il l'a fait jusqu'à présent au financement des autorités d'exécution cantonales.

3.3 Conséquences économiques et sociales

Les normes que propose le présent projet de loi renforcent la sûreté intérieure et extérieure du pays et apportent ainsi par une meilleure protection à la population. Indirectement, comme on crée un environnement plus sûr et socialement plus stable, on améliore les conditions économiques et renforce la place économique suisse.

3.4 Autres conséquences

Formellement, le projet de loi ne répond à aucune obligation directe sur le plan international. Néanmoins, l'image de notre pays pourrait encore être durablement améliorée en démontrant que la volonté de la Suisse à lutter efficacement contre le terrorisme. Les mesures de recherche d'informations plus étendues qu'auparavant conduiront probablement à une meilleure collaboration internationale.

4 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

4.1 Relation avec le programme de la législature

Le présent projet de loi a été annoncé dans le message du 25 janvier 2012 relatif au programme de la législature 2011–2015[69] et dans l'arrêté fédéral du 15 juin 2012 sur le programme de la législature 2011 à 2015[70].

4.2 Relation avec les stratégies nationales du Conseil fédéral

Le 25 mars 2009, le Conseil fédéral a décidé de fusionner le Service d'analyse et de prévention (SAP) avec le Service de renseignement stratégique (SRS) et d'en faire un nouvel office fédéral. Dans le rapport sur la politique de sécurité, le SRC est défini comme centre de compétences pour tous les domaines relevant du renseignement, tant pour la sûreté intérieure que pour la sûreté extérieure; le Conseil fédéral le qualifie d'instrument de politique sécuritaire. Le présent projet de loi va plus loin dans cette voie: d'une part, les normes déterminantes sont toutes réunies dans un seul acte législatif et, d'autre part, ces normes sont adaptées aux nouvelles exigences.

La stratégie générale du Conseil fédéral pour la protection des infrastructures critiques[71] et la stratégie nationale de protection de la Suisse contre les cyberrisques[72] méritent une attention tout particulière. Les deux stratégies visent en effet un rôle actif du SRC pour déceler à temps et prévenir les attaques contre des infrastructures critiques. La mission du SRC a donc été complétée de manière explicite à l'art. 6. Dans la mesure où les attaques contre des infrastructures critiques sont opérées au moyen de technologies d'informations et de communications, le SRC pourra y parer activement (cf. art. 25, al. 1, let. d).

69 FF **2012** 349 425 478
70 FF **2012** 6667 6671 6672
71 www.bevoelkerungsschutz.admin.ch > Thèmes > Protection des infrastructures critiques > Publication PIC > Stratégie nationale pour la protection des infrastructures critiques
72 www.upic.admin.ch > Thèmes > Cyberrisques SNPC > Stratégie nationale de protection de la Suisse contre les cyberrisques

5 Aspects juridiques

5.1 Constitutionnalité et légalité

Aux termes des dispositions constitutionnelles régissant la répartition des compétences entre la Confédération et les cantons, la Confédération peut légiférer lorsque la Constitution fédérale lui en confère la compétence. Lorsque de telles compétences ne lui sont pas conférées, ce sont les cantons qui sont compétents (art. 3 et 42, al. 1, Cst.).

Cependant, dans le domaine de la sûreté intérieure et extérieure, le texte constitutionnel n'est pas déterminant à lui seul pour déterminer si les normes constitutionnelles donnent à la Confédération le pouvoir de légiférer. En effet, la doctrine reconnaît à la Confédération certaines compétences, dites inhérentes, parce qu'elles sont liées à sa souveraineté, même lorsqu'elles ne figurent pas explicitement dans la Constitution (cf. ATF *117* IA 202, consid. 4a). Ainsi, la Confédération a la compétence inhérente de prendre les mesures nécessaires sur le plan intérieur et à l'étranger pour assurer sa protection et celle de ses organes et de ses institutions; elle se doit de garantir et d'assurer la pérennité de la communauté nationale (autrement dit, l'État) et doit veiller à écarter les dangers qui pourraient menacer cette collectivité dans son existence. Dans le domaine de la sûreté intérieure et extérieure, la compétence inhérente de la Confédération comprend dès lors aussi des compétences législatives.

Dans le domaine de la sûreté extérieure, la Confédération dispose d'une compétence générale comprenant de vastes pouvoirs législatifs. La recherche d'informations sur l'étranger qui pourraient avoir une importance cruciale en vue d'évaluer la situation en matière de politique sécuritaire fait également partie de cette compétence. D'ailleurs, l'art. 54 Cst. est également considéré comme une base constitutionnelle pour édicter des actes législatifs étroitement liés aux affaires étrangères.

La doctrine consacrée à la Constitution fédérale reconnaît l'existence d'un droit constitutionnel non écrit. La Confédération a dès lors un pouvoir législatif tant en matière de protection de l'État pour les affaires intérieures que dans le domaine du renseignement à l'étranger. Selon une nouvelle pratique, les compétences qui découlent de l'existence et de la nature même de la Confédération et que la Constitution ne lui attribue pas explicitement sont déduites de l'art. 173, al. 2, Cst. Il n'est donc pas absolument nécessaire de créer une base constitutionnelle explicite pour le renseignement. Certains participants à la procédure de consultation en avaient demandé la création en se fondant sur les conclusions du rapport donnant suite au postulat Malama. S'inscrivant dans le contexte d'une vaste mise à jour de la répartition de compétences conférées par la Constitution entre la Confédération et les cantons dans le domaine de la sûreté intérieure, ce rapport recommandait certes de créer une base constitutionnelle explicite la protection de l'État exercée par la Confédération. Cependant, les Chambres fédérales ont renoncé à conférer un tel mandat au Conseil fédéral. En présentant le présent projet de loi, le Conseil fédéral ne va en tout état de cause pas au-delà des compétences qui sont conférées à la Confédération en vertu du droit constitutionnel. Le Conseil fédéral se fonde donc sur une base constitutionnelle suffisante.

Protection des droits fondamentaux des personnes résidant en Suisse

Le présent projet de loi peut certes entraîner de graves atteintes aux droits fondamentaux des personnes lorsque des mesures de recherche d'informations soumises à autorisation sont mises en œuvre (notamment des mises sur écoute téléphonique ou des enregistrements visuels et sonores dans des locaux privés). En l'occurrence, ce sont essentiellement les droits fondamentaux relatifs à la protection de la sphère privée qui sont lésés (art. 13 Cst.; art. 8 de la Convention européenne des Droits de l'Homme, CEDH) voire d'autres garanties telles que la liberté personnelle (art. 10, al. 2, Cst.)et la liberté d'opinion et d'information (art. 16 Cst.; art. 10 CEDH). En vertu du présent projet de loi, les mesures de recherche soumises à autorisation peuvent uniquement être effectuées en Suisse.

Les mesures de recherche soumises à autorisation se fondent sur une base légale au sens formel qui satisfait au principe de précision. Les dispositions du projet de loi respectent également le principe de la proportionnalité imposé par la Constitution et répondent à un intérêt public suffisant.

S'agissant de la nature des mesures de recherche d'informations, le présent projet n'en prévoit aucune impliquant des atteintes à l'intégrité corporelle d'une personne, telle que notamment une fouille corporelle ou la contrainte physique. De telles mesures doivent continuer à être réservées aux organes de police, qui sont autorisés à les mettre en œuvre en vertu de la loi du 20 mars 2008 sur l'usage de la contrainte[73].

Enfin, le présent projet de loi (tout comme la LMSI, d'ailleurs) interdit sauf exceptions de collecter en Suisse des informations sur les activités politiques et sur l'exercice de la liberté d'opinion, de réunion et d'association (cf. commentaires concernant l'art. 5, al. 5).

Protection des droits fondamentaux en faveur de personnes se trouvant à l'étranger

La recherche d'informations à l'étranger est des plus délicates, parce qu'elle peut porter atteinte à la souveraineté d'un État étranger et aux droits fondamentaux de personnes qui se trouvent à l'étranger (par ex. protection de la sphère privée).

Elle ne doit par conséquent se faire que lorsqu'il est impossible de collecter les informations nécessaires en Suisse. Cette recherche d'informations sert au premier chef à apprécier les menaces sécuritaires qui pèsent sur notre pays et à pouvoir les écarter (par exemple, en matière de terrorisme ou de prolifération d'armes de destruction massive) et à évaluer les rapports de force politique et les conflits.

Les intérêts sécuritaires de la Suisse s'opposent certes à la protection des droits fondamentaux des personnes à l'étranger, mais il faut toujours tenir compte des droits fondamentaux. Le SRC veille dès lors à ce que l'atteinte aux droits fondamentaux d'une personne ne soit pas disproportionnée par rapport au bénéfice escompté en termes d'informations.

Les garanties de procédure sont moins étendues pour les mesures de recherche à l'étranger que pour les mesures mises en œuvre dans notre pays; ce sont surtout les mesures au sens de l'art. 22 du projet de loi qui sont concernées. En dehors des

73 RS **364**

principes énoncés plus haut, les motifs suivants s'opposent à une procédure d'autorisation similaire à celle qui est prévue pour les mesures en Suisse:

- en raison de la distance qui la sépare du terrain opérationnel, une autorité d'autorisation suisse ne pourrait guère se faire une idée de la situation sur place en temps utile, puis rendre une décision objective;
- l'autorisation donnée par une autorité suisse ne changerait rien à l'illicéité de la mesure par rapport au droit étranger.

En revanche, lorsque des informations sur l'étranger sont collectées en Suisse, la protection des droits fondamentaux s'applique d'office dans notre pays – en particulier pour les mesures de recherche soumises à autorisation. Seule l'introduction dans des systèmes et réseaux informatiques qui se trouvent à l'étranger fait exception (art. 36).

Délimitation avec les activités exercées par la police et par les autorités de poursuite pénale

Les investigations en matière de renseignement servent à déterminer s'il existe ou non des menaces contre la sécurité en Suisse. La menace peut cependant être causée aussi bien par des actes qui s'avèrent non punissables que par des actes punissables. Les destinataires des investigations en matière de renseignement sont au premier chef les décideurs politiques, c'est-à-dire les pouvoirs exécutifs de la Confédération et des cantons, afin qu'ils puissent intervenir à temps dans le respect de leur ordre juridique. Lorsque le SRC découvre des actes punissables concrets, il a le devoir d'informer les autorités de poursuite pénale.

En procédure de poursuite pénale, l'enquête sert à clarifier un soupçon d' infraction ou la culpabilité d'un individu, et cette enquête se focalise sur les éléments constitutifs de l'infraction et non au premier chef sur les aspects sécuritaires. Les autorités de poursuite pénale utilisent ainsi les résultats de leurs enquêtes dans une procédure judiciaire: ils ne les soumettent pas aux autorités politiques. Elles ne défendent pas directement des intérêts de politique sécuritaire, même si une poursuite pénale efficace sert également des intérêts sécuritaires.

Les investigations menées par le SRC se distinguent des enquêtes de droit pénal par l'élément déclencheur (soupçon de menace contre la sécurité de la Suisse ou soupçon d' infraction concrète), par l'objet des investigations (découvrir les intentions, les structures et les réseaux ou fournir la preuve d'un comportement punissable pour les autorités de poursuite pénale) et par l'objectif poursuivi au premier chef (fournir à l'exécutif des bases de décision pour prendre les mesures qui s'imposent ou clarifier un soupçon d'infraction ou la culpabilité d'un individu).

Les recherches de renseignement liées à la sûreté de notre pays peuvent se recouper dans la pratique avec les enquêtes des autorités de poursuite pénale sur un comportement délictueux, parce que le prévenu ou l'infraction présumée fait simultanément l'objet de mesures préventives. En d'autres termes, la même personne ou le même délit peut être soumis à des investigations simultanées, mais sous une perspective fondamentalement différente. C'est pourquoi si ces différentes procédures peuvent certes se compléter, du moins en partie, elles ne sauraient se remplacer. La LRens permet de coordonner ces différentes activités en réglementant les flux d'informations et la concertation entre les autorités concernées.

5.2 Compatibilité avec les obligations internationales

Le droit international ne règle pas vraiment les actes d'espionnage commis entre les États. En effet, selon le droit international coutumier, les activités d'espionnage sont tolérées dans une certaine mesure dans les relations internationales. En règle générale, les États qui sont victimes d'espionnage ne qualifient pas ces actes comme étant contraires au droit international mais comme des actes inamicaux. Parallèlement, la plupart des États se réservent explicitement le droit de pratiquer des activités d'espionnage à l'étranger. L'absence d'interdiction générale de l'espionnage dans le droit international n'empêche toutefois pas les États de prévoir dans leur droit national des sanctions pénales pour ceux qui le pratiquent sur leur territoire. Toute comme la Suisse, la plupart des États ont adopté de telles dispositions pénales. Le droit national prévoit aussi souvent des mesures de contre-espionnage.

Bien que l'espionnage pratiqué entre les États ne soit pas interdit en soi par le droit international, certains sous-domaines du droit international comprennent des normes qui pourraient restreindre les activités d'espionnage exercées à l'étranger. Différents instruments créés pour protéger les droits fondamentaux et les droits de l'homme et la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques[74] contiennent ainsi de telles normes. Aussi les organes d'un État qui agissent à l'étranger sont-ils également soumis à l'obligation de respecter les droits fondamentaux et les droits de l'homme. La Convention de Vienne en particulier est cependant souvent bafouée dans la pratique, soit par l'abus de prérogatives diplomatiques à des fins d'espionnage, soit parce que la protection diplomatique dont bénéficient des personnes et des installations est bafouée pour collecter des renseignements.

Le droit fondamental à la protection de la sphère privée (art. 13 Cst.; art. 8 CEDH; art. 17 du pacte II de l'ONU) est principalement concerné. D'autres garanties peuvent cependant aussi être touchées suivant selon les circonstances, telles que les droits fondamentaux à la liberté d'opinion et d'information (art. 16 Cst.; art. 10 CEDH; art. 19 du pacte II de l'ONU[75]), la liberté des médias (art. 17 Cst.; art. 10 CEDH), la liberté d'association (art. 23 Cst.; art. 11 CEDH; art. 22 du pacte II de l'ONU), la liberté personnelle (art. 10, al. 2, Cst.), la liberté de religion (art. 15 Cst.; art. 9 CEDH; art. 18 du pacte II de l'ONU), la liberté économique (art. 27 Cst.) et l'égalité devant la loi (art. 8 Cst.; art. 2 et 26 du pacte II de l'ONU). Dans le présent contexte, la protection de la sphère privée (art. 13 Cst.; art. 8 CEDH; art. 17 du pacte II de l'ONU) peut être considérée comme droit primaire.

Il convient encore de préciser qu'à partir d'un certain degré d'atteinte aux droits fondamentaux du citoyen, une opération de surveillance impliquant des mesures de recherche est soumise à une procédure d'autorisation judiciaire (Tribunal administratif fédéral) et une procédure d'approbation politique. Au terme de l'opération, la personne concernée doit être informée qu'elle a fait l'objet d'une surveillance. Ces mesures sont également soumises après coup à l'autorité judiciaire (Tribunal administratif fédéral avec possibilité de recours auprès du Tribunal fédéral). Il existe en outre un droit d'accès aux données (en vertu de la loi sur la protection des données ou sur demande auprès du Préposé fédéral à la protection des données et à la transparence ou du Tribunal administratif fédéral pendant la durée d'un intérêt motivé à

74 RS **0.191.01**
75 RS **0.103.2**; pacte international du 16 décembre 1966 relatif aux droits civils et politiques

garder le secret sur cette mesure). Il existe donc bel et bien des mesures efficaces au sens des dispositions de la CEDH contre d'éventuels abus.

Les activités du SRC prévues dans le projet de loi sont dès lors conformes au droit international.

Lorsqu'on ne collecte pas uniquement des informations relevant du renseignement mais que l'on prend aussi des mesures pour s'introduire dans des systèmes et réseaux informatiques en vue de perturber, d'empêcher ou de ralentir l'accès à des informations en réaction à des attaques informatiques provenant de l'étranger d'autres questions se posent du point de vue de droit international. Le Conseil fédéral devra procéder dans chaque cas à une évaluation complète de telles opérations du point de vue du droit international avant de les autoriser.

5.3 Forme de l'acte à adopter

Aux termes de l'art. 164, al. 1 Cst., toutes les dispositions importantes qui fixent des règles de droit, en particulier celles qui touchent les droits constitutionnels, doivent être édictées sous la forme d'une loi fédérale. Le présent projet respecte cette règle.

5.4 Frein aux dépenses

En vertu de l'art. 159 de la Constitution, les dispositions relatives aux subventions, ainsi que les crédits d'engagement et les plafonds de dépenses, doivent être adoptés à la majorité des membres de chaque conseil (Conseil national et Conseil des États) s'ils entraînent de nouvelles dépenses uniques de plus de 20 millions de francs ou de nouvelles dépenses périodiques de plus de deux millions de francs. Le présent projet de loi reprend une disposition prévoyant une subvention annuelle de 8,4 millions de francs. À l'époque, cette subvention n'avait pas été soumise au frein aux dépenses. Le présent projet permet d'y remédier. L'art. 81, al. 5, est donc soumis au frein aux dépenses.

5.5 Conformité à la loi sur les subventions

Lors de la procédure de consultation, les cantons ont tous exigé le remboursement intégral des frais découlant des tâches de protection de l'État accomplies pour le compte de la Confédération, ce qui constitue une dérogation au principe voulant que les cantons assument eux-mêmes les frais de l'exécution du droit fédéral. Le projet de loi prévoit donc à l'art. 81, al. 5, que la Confédération indemnise les cantons, dans les limites des crédits approuvés, pour les prestations qu'ils fournissent en exécution de la présente loi. Le Conseil fédéral fixe une indemnité forfaitaire sur la base du nombre de personnes qui se consacrent de manière prépondérante aux tâches de la Confédération. Cette réglementation, qui ne couvre que partiellement les charges des cantons, est identique à la disposition en vigueur (cf. art. 28, al. 1, LMSI). Il convient de poursuivre cette pratique qui se justifie par la situation particulière en matière d'exécution:

«La non-prise en charge des frais de collaboration au traitement des informations pourrait s'avérer catastrophique: l'exécution d'un mandat portant sur la recherche d'un lieu de séjour ou sur l'observation d'une personne peut avoir des répercussions financières totalement différentes. Si la Confédération ne participait pas aux frais, il faudrait s'attendre à de nombreuses réponses négatives, car certains cantons renonceraient à mettre à disposition du personnel spécialement formé pour un engagement approprié à la menace. […] La Confédération a donc intérêt à ce que les cantons disposent de spécialistes compétents et aptes à fournir les résultats souhaités grâce à de bonnes connaissances des conditions locales et avec des moyens raisonnables. Du personnel engagé par la Confédération coûterait certainement plus cher; de plus, une telle solution n'est pas souhaitable pour des considérations fédéralistes. De ce fait, un remboursement adéquat des frais dépend du nombre des personnes qui, dans un canton déterminé, travaillent essentiellement pour le compte de la Confédération[76]».

Ces réflexions sont toujours de mise, à plus forte raison le présent projet ne va vraisemblablement pas réduire le coût de l'exécution cantonale. L'indemnisation accordée aux cantons est actuellement de 8,4 millions de francs au total. Elle devrait aussi se situer dans cet ordre de grandeur après l'entrée en vigueur du présent projet.

5.6 Délégation de compétences législatives

Le projet contient des normes de délégation pour édicter des ordonnances lorsque le Conseil fédéral est habilité à le faire par la loi. Cette délégation de pouvoirs législatifs est nécessaire, parce qu'elle concerne des règles d'application concrètes dépassant le cadre de la loi. Les lignes directrices figurant dans les divers articles de la loi concrétisent suffisamment cette délégation.

Dans le détail, le Conseil fédéral pourra désormais édicter les dispositions suivantes, en sus de ses compétences actuelles:

- déterminer les catégories de collaborateurs du SRC autorisés à porter une arme et régler leur formation (art. 8, al. 3);
- régler la collaboration et l'échange d'informations entre le SRC et les services compétents du Service de renseignement de l'armée et régler la répartition des tâches entre le SRC et les organes assurant le service de sécurité militaire pendant un service de promotion de la paix, un service d'appui ou un service actif (art. 11, al. 3);
- déterminer les événements et constatations que certaines autorités déterminées doivent communiquer spontanément au SRC; définir l'étendue de l'obligation et régler la procédure de communication (art. 20, al. 4);
- régler les domaines d'exploration, l'organisation et les procédures de l'exploration radio et déterminer la durée de conservation maximale des communications enregistrées par le service chargé de l'exploration (art. 37, al. 3);

76 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», commentaires concernant l'art. 26, FF **1994** II 1123 1193

– régler les domaines d'exploration, l'organisation du service chargé de l'exploration du réseau câblé et la procédure qui lui est applicable; déterminer la durée maximale de conservation des données relatives au contenu et des données relatives au trafic par le service chargé de l'exploration du réseau câblé (art. 38, al. 4);

– régler l'indemnisation des exploitants de réseaux câblés et des opérateurs de télécommunications (art. 42, al. 4);

– régler la transmission par les autorités d'exécution cantonales d'appréciations de la situation et des données qu'elles obtiennent du SRC (art. 45, al. 3);

– régler les modalités du traitement des données dans les différents systèmes d'information (art. 46, al. 2);

– déterminer les catégories de personnes à identifier dans le système d'information Quattro P (art. 54, al. 4);

– régler les droits d'accès aux données, la durée de conservation des données, et la sécurité des données provenant de mesures de recherche soumises à autorisation (art. 57, al. 4);

– assurer la conduite politique du SRC en assumant les tâches suivantes: confier une mission de base; approuver la liste d'observation; déterminer les groupements entrant dans la catégorie des extrémistes violents; apprécier la menace, etc. (art. 69);

– charger le SRC dans des circonstances particulières de sauvegarder des intérêts essentiels de la Suisse au sens de l'art. 3; déterminer dans chaque cas la durée, le but, le type et l'ampleur de la mesure (art. 70);

– établir la liste d'observation (art. 71, al. 4);

– régler la composition et l'organisation de l'organe de contrôle indépendant pour l'exploration radio (art. 75, al. 4);

– régler la surveillance financière des domaines d'activités du SRC qui doivent tout particulièrement rester secrets; fixer les exigences minimales auxquelles les contrôles menés dans les cantons doivent répondre et les compétences des organes de surveillance de la Confédération et des cantons à cet égard (art. 76, al. 3);

– régler dans le domaine de la surveillance cantonale: le recours à des organes de contrôle par les autorités cantonales pour exercer la surveillance cantonale; régler l'accès aux informations sur l'existence et le contenu des mandats exécutés pour le compte de la Confédération et sur la manière dont les autorités d'exécution cantonales les exécutent; régler la séparation entre les données traitées de manière indépendante par les autorités d'exécution cantonales et celles qu'elles traitent à la demande du SRC ou en vertu de la liste d'observation (art. 78, al. 3);

– régler l'indemnisation des cantons pour les prestations qu'ils fournissent en exécution de la présente loi (art. 81, al. 5).

5.7 Conformité à la législation sur la protection des données

La LRens doit permettre au SRC d'aménager une vaste base d'information provenant de sources multiples en vue de déceler à temps et d'apprécier des menaces pour la sûreté intérieure ou extérieure de la Suisse. Les droits fondamentaux des personnes sur lesquelles des données sont collectées doivent cependant être être sauvegardés autant que possible. Ce grand écart entre la sécurité et la liberté conduit à régler de manière différente la saisie et la gestion des données. Suivant la thématique, la source et la sensibilité des données, celles-ci sont versées dans les différents systèmes d'information, ces systèmes étant à leur tour soumis à différentes réglementations. Les données relatives à l'extrémisme violent figurant dans le système IASA-EXTR sont soumises aux conditions de traitement de données les plus sévères. Les données et le traitement dans le domaine de l'extrémisme violent se sont en effet révélés les plus sensibles tant sur le plan politique que sur pour le droit de la protection des données. Le traitement des données relatives au contre-espionnage, des données relevant du domaine de la non-prolifération d'armes de destruction massive ou des données relatives à la protection d'infrastructures critiques n'a en revanche guère suscité de critiques par le passé.

La loi réglemente le but, le contenu et le cercle des utilisateurs pour chaque système d'information. Dans la mesure où un accès en ligne externe est prévu, la loi le précise expressément.

Par rapport au droit en vigueur, les prescriptions relatives à la gestion des données et aux normes de qualité des données sont encore plus sévères. Désormais, un contrôle sans faille à l'entrée des informations et un triage sont exigés. Pour pouvoir être enregistrées, les données doivent par ailleurs être suffisamment liées aux tâches du SRC. Le personnel du SRC devra également contrôle la pertinence et à l'exactitude de ces données. Un contrôle analogue doit également avoir lieu lorsque le SRC transmet des données personnelles à des tiers (par exemple, dans un rapport d'analyse, dans une annonce à une autorité ou dans une appréciation de la situation). Désormais, le SRC sera tenu de vérifier périodiquement si toutes les données qu'il a saisies dans ses systèmes d'information sont encore nécessaires pour accomplir les tâches qui lui sont confiées. Les données dont il n'a plus besoin ou les données ayant atteint le délai maximum de conservation prévu par la loi seront détruites.

La loi prévoit aussi désormais une large centralisation à l'échelon de la Confédération des prescriptions relatives à la protection des données. La Confédération met en effet à la disposition des services de renseignement cantonaux les systèmes d'information dont ils ont besoin et gère donc les données qui sont désormais totalement soumises aux dispositions de la Confédération.

Par ailleurs, la loi confirme le principe inscrit dans la LMSI selon lequel il est en principe interdit de collecter en Suisse des informations sur les activités politiques et sur l'exercice de la liberté d'opinion, de réunion et d'association.

Précisons enfin que, sauf disposition contraire figurant dans une loi spéciale, les principes et les prescriptions de la loi fédérale sur la protection des données s'appliquent également au SRC.