# Loi sur le renseignement (LRens)

## Rapport sur l'avant-projet

**8 mars 2013**

## Aperçu

*Le présent projet de loi a pour but de créer une base légale formelle uniforme pour le Service de renseignement civil de la Suisse (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 afin de leur fournir les informations dont ils ont besoin pour pouvoir accomplir leurs tâches de conduite en temps utile et en fonction de la situation.*

*Comme l'armée, la politique étrangère et la police, le SRC fait partie des instruments de la politique de sécurité de la Confédération.*

Le principal objectif de la nouvelle loi est de régler par voie légale les activités, le mandat et le contrôle du Service de renseignement. Le SRC doit ainsi pouvoir fournir, à titre préventif, une contribution substantielle pour la sécurité de la Suisse et de sa population.

### *Historique*

Pour ainsi dire simultanément à l'approbation de la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC), le Conseil fédéral a décidé, dans un premier temps, de transférer au DDPS les unités de renseignement du Service d'analyse et de prévention (SAP) au 1er janvier 2009. Dans un deuxième temps, il a décidé en mars 2009 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, le Conseil fédéral a chargé le DDPS de lui présenter, d'ici fin 2013, un message portant sur le projet d'une nouvelle loi globale sur le Service de renseignement (ACF du 27 novembre 2009).

*Selon la volonté du Conseil fédéral, la nouvelle loi doit établir les bases légales des tâches, des obligations, des droits et des systèmes d'information du service de renseignement civil. Son but n'est pas de développer les bases légales en vigueur, mais de fixer une nouvelle codification globale tenant compte, autant que faire se peut, des critiques et des réserves qu'ont suscité les activités déployées dans le passé par les services de renseignement dans notre pays (en particulier en ce qui concerne la collecte d'informations personnelles) et de mieux tenir compte des changements intervenus au niveau des risques et des menaces.*

***Le présent projet comporte pour l'essentiel les nouveautés suivantes:***

- *Base légale globale pour le SRC: l'actuelle subdivision entre la loi fédérale sur le renseignement civil (LFRC) et la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) devient caduque.*
- *Nouvelle orientation de la recherche d'informations: une distinction n'est plus faite en priorité entre les menaces émanant de l'intérieur et de l'étranger, mais entre l'extrémisme violent en lien avec la Suisse, d'une part, et les autres champs de menaces et tâches, d'autre part.*
- *Introduction de nouvelles mesures de recherche d'informations dans les domaines du terrorisme, de l'espionnage, de la prolifération, d'attaques contre des infrastructures critiques ou pour la sauvegarde d'autres intérêts essentiels de la Suisse: les moyens spéciaux de recherche d'informations refusés par le Parlement dans le projet d'origine de la LMSI II, tels que la surveillance du trafic par poste et télécommunications, l'engagement d'appareils de surveillance dans la sphère privée, etc. ont été remaniés. Ils sont présentés sous une nouvelle forme et complétés. De l'avis du Conseil fédéral, ces nouvelles mesures de recherche d'informations sont nécessaires, car les instruments à disposition aujourd'hui ne permettent plus au SRC d'assurer ses tâches de prévention face aux protagonistes de plus en plus agressifs qui menacent la sûreté intérieure et extérieure de la Suisse et faces aux formes de plus en plus complexes des menaces. Une instance judiciaire (le Tribunal administratif fédéral) et une instance politique (le chef du DDPS) doivent décider de cas en cas de la mise en œuvre de ces mesures.*
- *Gestion et saisie différenciées des données: le projet de loi prévoit que les renseignements recherchés ou communiqués au SRC soient enregistrés dans des systèmes d'informations intégrés 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 partenaire, une appréciation de la situation), elles doivent être examinées quant à leur exactitude et leur pertinence. Les données communiquées au SRC dans le cadre d'une mesure de recherche soumise à autorisation ou à la suite de contrôles à la frontière sont traitées séparément. Seuls les spécialistes au sein du SRC ont accès à ces données.*
- *Régimes de contrôles: les activités du SRC sont soumises à un triple contrôle, respectivement surveillance: par le département auquel il est subordonné, par le Conseil fédéral et par la Délégation des Commissions de gestion du Parlement (DélCdG). L'exploration radio fait l'objet d'un contrôle supplémentaire par l'Autorité de contrôle indépendante (ACI). Les nouvelles mesures de recherche soumises à autorisation qui sont proposées et l'exploration du réseau câblé ne sont mises en œuvre que si le Tribunal administratif fédéral, puis le chef du DDPS, ont autorisé, respectivement avalisé l'exécution de la mesure concernée. Ces mécanismes doivent garantir la légitimité et la proportionnalité des activités du SRC.*

## Sommaire

# Rapport sur le projet de loi

## 1 Partie générale

### 1.1 Introduction

Le présent projet de loi a pour but de créer une base légale formelle uniforme pour le Service de renseignement de la Confédération (SRC). Ce service procède à la recherche d'informations à l'aide de moyens du renseignement, les analyse, les évalue et les transmet aux décideurs à tous les échelons afin de leur fournir les informations dont ils ont besoin pour pouvoir accomplir leurs tâches de conduite en temps utile et en fonction de la situation.

Le SRC fait partie 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 la protection civile. Il fait partie du dispositif mis en place pour veiller à la sûreté de la Suisse.

Le rapport du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse, du 23 juin 2010[1] (ci-après: Rapport sur la politique de sécurité du Conseil fédéral) 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. »

Par cette définition, le Conseil fédéral a simultanément délimité le cadre que la Constitution prévoit pour les tâches du SRC.

Le principal objectif de la nouvelle loi est de régler par voie légale les activités, le mandat et le contrôle du Service de renseignement. Le SRC doit ainsi pouvoir fournir, à titre préventif, une contribution substantielle pour la sécurité de la Suisse et de sa population.

### 1.2 Historique et mandat du Conseil fédéral

Dans son rapport du 29 février 2008[2] sur l'initiative parlementaire « Transfert des tâches des services de renseignement civils à un département », la Commission de gestion du Conseil des Etats 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*

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

*SRS et du SAP 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, 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. A cet effet, le Conseil fédéral a décidé de créer de soi-disant 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'Etat, 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. A 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[3](LFRC), édictée à la suite de l'initiative parlementaire, a été approuvée par les Chambres fédérales le 3 octobre 2008 et elle 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 au 1er janvier 2009. Dans un deuxième temps, en mars 2009, il a décidé de regrouper au 1er janvier 2010 le SRS et le SAP au sein du SRC nouvellement créé.

[3] RS **121**

Dans un troisième temps, le Conseil fédéral a chargé le DDPS de lui présenter d'ici fin 2013 un message portant sur un projet de loi globale sur le service de renseignement (ACF du 27 novembre 2009):

*« Le Conseil fédéral charge le DDPS*

*…de présenter, d'ici fin 2013 au plus tard, un message avec un projet pour une nouvelle loi sur le service de renseignement créant la base légale pour 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 ainsi que les dispositions en vigueur doivent nouvellement être réglés dans le projet de loi. »*

*Echelonnement des travaux selon l'ACF du 27 novembre 2009*

Au printemps 2009, le Conseil national et le Conseil des Etats ont renvoyé au Conseil fédéral le projet LMSI II du 15 juin 2007 (Moyens spéciaux de recherche d'informations; « LMSI II ») pour le remettre sur le métier sans qu'une discussion sur le contenu des différents articles de la loi n'ait eu lieu, les débats du Parlement s'étant limités à la question de l'entrée en matière. Par conséquent, on ne peut se référer à certains éléments précis du projet qui avaient, à l'époque, été acceptés par les milieux politiques.

Le Conseil fédéral a par la suite décidé d'échelonner les travaux législatifs (ACF du 27 novembre 2009): dans un premier projet, il s'agissait de fixer les règles majoritairement non contestées et prêtes à être concrétisées. Cette partie a depuis été réalisée par le message complémentaire « LMSI II réduite », approuvé par le Parlement le 23 décembre 2011. La LMSI révisée est entrée en vigueur le 16 juillet 2012.

Le deuxième projet, comme mentionné, devait avoir pour objet la nouvelle loi sur le renseignement.

## 1.3 Elaboration du projet de loi

Le SRC a confié à un groupe de travail interdépartemental (GTID) la tâche de préparer la nouvelle loi. Ce groupe était composé de représentants du DDPS, du DFAE, de l'OFJ, de fedpol, du Préposé fédéral à la protection des données et à la transparence, de la Chancellerie fédérale, des cantons et du SRC.

Le GTID a débuté ses travaux fin octobre 2010 et jusqu'en juillet 2011, il a élaboré une stratégie et une esquisse de l'acte normatif. Se fondant sur les travaux préliminaires du GTID, le SRC s'est ensuite chargé de rédiger le présent projet. Les différentes versions du projet ont été soumises au GTID pour avis.

Les règlementations de la LMSI et de la LFRC qui ont fait leurs preuves ainsi que de nouvelles règles issues de la révision de la LMSI II réduite[4] ont été reprises dans le projet de loi pour autant que cela ait été jugé opportun. C'est ainsi, par exemple, que l'obligation de renseigner et de communiquer des renseignements, ainsi que l'inter-

[4] 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 » ; FF **2010** 7147)

diction d'exercer une activité, répondent aux principes des dispositions respectives du message relatif à 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 fixer une nouvelle codification globale tenant compte, autant que faire se peut, des critiques et des réserves qu'ont suscité les activités déployées dans le passé par les services de renseignement dans notre pays et de mieux tenir compte des changements intervenus au niveau des risques et des menaces.

*Eléments controversés*

L'introduction de moyens spéciaux pour la recherche d'informations a été de loin la mesure la plus controversée, et ceci aussi bien dans le cadre de la procédure de consultation du projet de 2007 qu'au niveau des débats politiques et des articles dans les médias.

C'est pourquoi, dans son message complémentaire du 27 octobre 2010 relatif à la modification de la LMSI (LMSI II réduite), le Conseil fédéral a pour l'essentiel renoncé aux moyens suivants de recherche d'informations soumis à autorisation:

- surveillance de la correspondance par poste et télécommunication;
- observation de lieux qui ne sont pas librement accessibles au public, notamment au moyen d'appareils techniques de surveillance;
- intrusion dans des systèmes informatiques.

Ces éléments sont repris dans le présent projet de loi.

## 1.4 Objectifs de la nouvelle loi sur le service de renseignement

*Contribution substantielle pour la sûreté de la Suisse*

La Suisse est tributaire d'un service de renseignement efficace pour pouvoir défendre ses intérêts et assurer la protection de sa population. Simultanément, il s'agit de 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 extérieur de la Suisse en respectant les libertés constitutionnelles de ses citoyens. Ils doivent, avec des moyens et des méthodes du renseignement, rechercher les informations nécessaires (en utilisant des sources d'informations publiques, non accessibles au public et des informateurs), les traiter, les analyser et les transmettre sous une forme appropriée aux décideurs de l'Etat à tous les échelons (Confédération et cantons). A cet effet, il est indispensable que le SRC puisse procéder à une appréciation globale de la situation 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 sources accessibles au public, les demandes de renseignement et l'observation dans des lieux publics librement accessibles (art. 14 LMSI), le SRC ne peut que partiellement accomplir son mandat. C'est pourquoi le présent projet de loi 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 des cantons et des autorités d'exécution cantonales.

Le SRC fournit aux bénéficiaires de ses prestations de manière ciblée et dans les meilleurs délais des informations et des appréciations qu'ils ne peuvent obtenir par d'autres moyens.

*Contexte international*

Au XXIe siècle aussi, l'organisation des services de renseignement relève essentiellement des Etats et ces services sont par conséquent un instrument de la conduite politique d'un pays. Cela est particulièrement le cas pour la Suisse. En tant qu'Etat indépendant et neutre, la Suisse doit, à plusieurs égards, faire ses propres choix et ne peut donc compter que sur elle-même. La majorité de nos partenaires en Europe sont membres de l'OTAN et/ou de l'UE. La création de nouveaux organismes, tels que le G20, où d'importantes décisions qui concernent aussi la Suisse sont prises 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 au niveau de l'information. Leur statut de membre les fait bénéficier d'une vue d'ensemble de la situation très large et actualisée en permanence. Par ses contacts avec les services de renseignement d'Etats partenaires et les informations qu'il obtient grâce à ses contacts, le SRC soutient aussi la politique extérieure de la Suisse.

*Acte de codification globale*

Le présent projet de loi répond à l'ACF du 27 novembre 2009 et représente une codification globale pour le SRC. Les dispositions sur la recherche d'informations en Suisse et à l'étranger, contenues jusqu'à présent dans deux lois distinctes, sont réunies en une seule loi.

Dans son concept, le projet de loi ne fait plus en priorité de distinction entre les menaces à l'intérieur de la Suisse et celles émanant de l'étranger, mais entre l'extrémisme violent en lien avec la Suisse, d'une part, et les autres champs de menaces et tâches, d'autre part. 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 des dispositions qui requièrent une base légale formelle pour des raisons de droit constitutionnel. Dans la nouvelle loi, le Conseil fédéral précise en détail les domaines d'activité du SRC par un mandat de base qui se fonde sur des intérêts spécifiques de la Suisse et sur le développement de la situation de la menace.

Est également pris en compte le fait que les activités de renseignement, tant nationales qu'internationales, sont soumises à des conditions particulières (maintien du secret sur les méthodes utilisées, sur les informations, les processus et moyens techniques ainsi que sur les sources, les collaborateurs et les informateurs). Il s'agit en particulier aussi de régler avec précision les ingérences inévitables dans les droits fondamentaux.

*Elimination 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 la soi-disant « affaire des fiches », dont l'impact publique et politique se ressent encore à l'heure actuelle.

En fixant dans la LMSI le principe de n'autoriser le traitement d'informations avant une poursuite pénale que dans certaines limites très strictes, le législateur a sciemment accepté d'assumer un certain risque au niveau de la sécurité. Ce risque devait toutefois être minimisé par un suivi attentif des développements et une nouvelle appréciation périodique de la situation. La recherche, le traitement et la transmission de données particulièrement dignes d'être protégées ont été réglés et limités par des dispositions détaillées. La LMSI répondait ainsi aux exigences strictes de la loi du 19 juin 1992 sur la protection des données[5] (LPD). Peu après l'entrée en vigueur de la LMSI, les attentats terroristes du 11 septembre 2001 ont fondamentalement modifié la situation de la menace. Plusieurs interventions parlementaires ont par la suite réclamé un renforcement du rôle des organes de protection de l'Etat et des services de renseignement, une augmentation des moyens et des instruments à leur disposition ainsi que des rapports détaillés sur la situation de la sécurité. En novembre 2001, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) de lui soumettre un rapport et des propositions pour l'amélioration des mesures visant à lutter contre le terrorisme. En juin 2002, le Conseil fédéral a approuvé le rapport « Analyse de la situation et des menaces pour la Suisse après les attentats du 11 septembre 2001 » et prit simultanément connaissance du projet législatif qui avait pour but, notamment par une révision de la LMSI, de combler les lacunes au niveau des instruments permettant de détecter et d'identifier les menaces.

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

Comme déjà mentionné, au printemps 2009, le Parlement a renvoyé au Conseil fédéral, le projet LMSI II pour révision. Depuis, les principales lacunes et faiblesses de la LMSI n'ont de ce fait été ni comblées ni corrigées.

C'est ainsi que selon le droit en vigueur, la correspondance par poste et télécommunication ne peut de manière générale faire l'objet de recherches menées en vertu de la LMSI. Là où cette source d'informations fait défaut, les autorités du renseignement doivent essayer d'obtenir des informations sur les groupes et les personnes visés à l'aide de contacts camouflés, 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 sont par exemple discutées des actions terroristes, mais ces mesures sont interdites, car ces domaines sont assimilés à la sphère privée. En résultent des lacunes de connaissances au niveau de la détection précoce et de la collaboration internationale.

Selon le droit en vigueur, lorsqu'il s'agit de rechercher des informations relatives à des activités d'espionnage, les lieux qui ne sont pas librement accessibles (par ex. les chambres d'hôtel) échappent en général à toute possibilité d'exploration. Les es-

[5] RS **235.1**

pions utilisent cette lacune à dessein; ils bénéficient souvent de l'immunité diplomatique et sont formés pour collecter des informations sous couverture. A cela s'ajoutent les recherches d'informations par des bureaux d'investigation internationaux, qui agissent parfois (de manière camouflée) sur mandat d'un Etat. La législation actuelle limite par conséquent aussi les activités de contre-espionnage, qui se terminent en principe au seuil de la sphère privée. D'importantes lacunes se créent ainsi dans le dispositif de prévention.

Les tentatives de se procurer des armes de destruction massive sont organisées par le biais de réseaux internationaux extrêmement complexes. Dans ce domaine, la Suisse reçoit par exemple des indications de tiers sur l'implication d'entreprises et d'instituts financiers. Comme dans les domaines du terrorisme et de l'espionnage, le SRC n'est pas en mesure d'étayer avec succès des présomptions d'activités de prolifération sans la possibilité d'une surveillance ciblée de la sphère secrète et de la sphère privée.

Les lacunes et les faiblesses du droit en vigueur ont aussi été thématisées depuis dans 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 Viola, Renforcement de la surveillance sur Internet; 11.3471 – Interpellation Malama Peter, 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 Corinna, Réglementation future de l'activité de protection de l'Etat; 11.4059 – Interpellation, Geissbühler Andrea Martina, 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'Etat de droit; 09.4146 – Interpellation Wehrli Reto, Place financière suisse. Stratégie).

## 1.5 Principaux éléments du projet de loi

*Nouvelle orientation de la recherche d'informations*

Concernant la recherche d'informations, le projet de loi comporte une nouveauté dans la mesure où il ne distingue plus en priorité entre les menaces émanant de l'intérieur du pays et celles de l'étranger, mais entre l'extrémisme violent en lien avec la Suisse et les autres champs de menaces et tâches. Ce concept a pour conséquence que les mesures de recherche d'informations soumises à autorisation ne sont pas applicables à l'extrémisme violent. L'intention est de mettre un terme définitif à l'affaire dite «des fiches » en procédant à une séparation claire entre le terrorisme à proprement parler et l'extrémisme violent. Comme pour la gestion des données s'y rapportant, la recherche d'informations dans le domaine de l'extrémisme violent, qui présentent des liens avec la Suisse, respectivement avec des acteurs suisses, doit être soumise à des conditions plus strictes en ce qui concerne les ingérences dans les droits fondamentaux. Conformément à l'art. 61, al. 1, let. c, le Conseil fédéral établit

chaque année sur une liste les groupements entrant dans la catégorie des groupements d'extrémistes violents.

*Introduction de nouvelles mesures de recherche d'informations dans les domaines du terrorisme, de l'espionnage, de la prolifération, d'attaques contre des infrastructures critiques et pour la sauvegarde d'autres intérêts essentiels de la Suisse.*

Les moyens spéciaux de recherche d'informations dans le projet d'origine de la LMSI II[6], renvoyé par le Parlement pour examen, ont été expertisés quant à leur conformité constitutionnelle et au regard du droit international (expertise du professeur Giovanni Biaggini de juin 2009[7]). Dans le présent projet, le catalogue des moyens spéciaux de recherche d'informations contenu dans la LMSI II a été révisé et complété. Le Conseil fédéral demande que les mesures suivantes soient introduites en Suisse pour la recherche d'informations soumises à autorisation:

- surveillance de la correspondance par poste et de la correspondance par télécommunication d'une personne;
- surveillance des raccordements et des communications par poste ou télécommunication de personnes surveillées;
- renseignements sur la position et la direction d'émission d'antennes auxquelles le téléphone mobile d'une personne surveillée est momentanément 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 propos non publics et pour observer ou enregistrer des événements se produisant dans des lieux non-publics ou dans des lieux qui ne sont pas librement accessibles;
- introduction dans des systèmes et des réseaux informatiques pour la recherche d'informations qu'ils contiennent ou qui ont été transmises par ces systèmes ou pour perturber, empêcher ou ralentir l'accès à des informations;
- procéder à des fouilles de locaux, de véhicules ou de conteneurs emportés par des personnes.

Ces mesures ne peuvent être réalisées que lorsqu'elles ont été approuvées au préalable par le Tribunal administratif fédéral, puis avalisées par le chef du DDPS.

Ces nouvelles mesures de recherche d'informations sont proposées car les instruments actuellement à disposition du SRC (art. 14 LMSI) ne lui permettent plus, au vu des formes de menaces de plus en plus agressives et complexes, d'assurer ses tâches de prévention dans le domaine de la sûreté intérieure. Concernant ces mesures, nous renvoyons aux explications des art. 22 ss (Mesures de recherche soumises à autorisation).

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

Les mesures de recherche non soumises à autorisation (art. 11 ss) ont également été élargies. Dans ce domaine, des possibilités techniques (par ex. l'engagement de

[6] Message du 15 juin 2007 relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI; FF **2007** 4773)
[7] VPB 4/2009 (p. 238-330). Ce document n'est disponible qu'en allemand.

drones) doivent être mises à profit. Jusqu'à présent, de tels moyens ne pouvaient pas être engagés en Suisse en raison de l'absence de bases légales formelles.

*Traitement différencié des données*

Le projet de loi prévoit que les renseignements recherchés ou communiqués au SRC soient enregistrés dans des systèmes d'informations intégrés 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 partenaire, une appréciation de la situation), elles doivent être examinées quant à leur exactitude et leur pertinence. Les données communiquées au SRC dans le cadre d'une mesure de recherche soumise à autorisation ou à la suite de contrôles à la frontière sont traitées séparément. Seuls les spécialistes au sein du SRC ont accès à ces données.

## 1.6 Droit comparé et droit international

Le tableau de *l'annexe II* compare divers systèmes de services de renseignement de l'entourage européen de la Suisse par rapport à certains points spécifiques. Les 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 et, dans ces deux pays, il présente des similitudes avec le SRC.
- L'Autriche et la Belgique sont des pays qui ont une superficie comparable à celle de la Suisse.

## 1.7 Conséquences du projet de loi au niveau des finances, du personnel et de l'économie

*Conséquences financières*

Les conséquences financières dépendent très largement des modalités d'application des différentes mesures et de leur fréquence. Au vu de la situation actuelle de la menace, le Conseil fédéral estime qu'une dizaine de cas environ nécessiteront de telles mesures 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 année ainsi que des frais récurrents d'environ 800 000 francs pour leur maintenance et leur adaptation et des coûts de licences. Ces systèmes doivent être acquis et financés dans le cadre des procédures 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 » du DFJP, qui est compétent en la matière. Conformément au nombre de cas estimés, les indemnités à verser pour ces mesures devraient s'élever à environ 500 000 francs par année.

Pour les travaux de traduction des communications enregistrées, 800 000 francs doivent être prévus au budget.

Par analogie au montant de l'indemnisation de la surveillance des télécommunications par le service « Surveillance de la correspondance par poste et télécommunication » (SCPPT) les coûts pour l'indemnisation de l'exploration du réseau câblé (art. 34 ss) sont également estimés à 500 000 francs par année.

Certaines technologies, par exemple pour l'introduction dans des systèmes informatiques particulièrement 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.

*Conséquences au niveau de l'effectif du personnel*

Les nouvelles mesures de recherche d'informations proposées doivent autant que faire se peut être réalisées dans le cadre des structures en place (SRC, Base d'aide au commandement de l'armée (BAC), Service de surveillance de la correspondance par poste et télécommunication). Il faut néanmoins s'attendre à devoir créer environ 16 postes de travail supplémentaires. Ces derniers se répartissent comme suit: au SRC, des techniciens opérationnels pour le suivi technique des moyens de recherche soumis à autorisation, des analystes pour l'évaluation opérationnelle des informations obtenues à l'aide des mesures soumises à autorisation, des juristes pour la préparation des demandes pour ces mesures, leur contrôle ainsi que les rapports concernant les méthodes de recherche soumises à autorisation ainsi que des postes supplémentaires pour la garantie de la qualité des nouveaux systèmes et le suivi de l'exploration du réseau câblé. D'autres postes sont nécessaires pour le Tribunal administratif fédéral en rapport avec la procédure d'autorisation des mesures de recherche, les Archives fédérales pour l'archivage décentralisé dans les locaux du SRC et pour le Centre des opérations électroniques (COE) de la BAC pour l'essai-pilote de l'exploration du réseau câblé.

L'augmentation des exigences pour la gestion des données par rapport aux conditions actuelles peut en grande partie être assumée avec les ressources à disposition aujourd'hui.

*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 en personnel doit être réglée de cas en cas avec le destinataire ou le mandant de ces prestations. Elle dépend entre autre des possibilités du SRC.

## 1.8 Conséquences du projet de loi sur la collaboration avec les cantons

Selon le concept du projet de loi, le SRC assure ses tâches de renseignement en collaboration avec les autorités d'exécution cantonales.

La forme actuelle de l'organisation décentralisée et la collaboration étroite entre le SRC et les cantons est donc maintenue. Comme auparavant, la compétence pour assurer la sûreté intérieure sur leur territoire relève en premier lieu des cantons. 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 Conférence des commandants des polices cantonales de Suisse (CCPCS) et la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP).

Lors de menaces concrètes et conformément au principe d'assistance, toutes les autorités et unités administratives des cantons ont l'obligation de renseigner. Les informations peuvent être demandées par le SRC ou par les autorités d'exécution cantonales.

Dans le cadre du champ d'application du projet de loi, et c'est nouveau, les autorités d'exécution des cantons ne gèrent plus de banques de données qui leur soient propres. En revanche, elles disposent d'un droit d'accès aux informations automatisées 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. Ces autorités peuvent, entre autres, y consulter les données d'enquêtes préliminaires qu'ils ont effectuées et les rapports qu'ils ont établis.

L'organe du département chargé de la surveillance du service de renseignement peut procéder à des contrôles dans les domaines dans lesquels les autorités d'exécution cantonales appliquent les dispositions du présent projet.

Quant à la haute surveillance parlementaire, nous renvoyons aux commentaires concernant l'art. 69.

Comme il l'a fait jusqu'à présent, le SRC contribue au financement des autorités d'exécution cantonales.

## 1.9 Aspects juridiques

*Base constitutionnelle*

La base constitutionnelle pour la recherche d'informations importantes en matière de politique de sécurité sur l'étranger, respectivement la compétence de la Confédération de légiférer dans ce domaine, se fonde pour l'essentiel sur l'art. 54 de la Constitution[8] (Cst.) (Affaires étrangères):

L'art. 54, al. 1, Cst., donne à la Confédération la compétence de régler les affaires étrangères. En fait partie la compétence de rechercher des informations qui peuvent être importantes pour l'appréciation de la situation en matière de politique de sécurité.

[8] RS **101**

Selon l'interprétation coutumière et la doctrine, la compétence de la Confédération pour légiférer dans le domaine de la sécurité intérieure se fonde sur l'art. 57, Cst. (Sécurité). Cet article ne stipule pas explicitement la compétence de la Confédération d'agir et de légiférer dans le domaine de la sécurité intérieure, mais il le fait de façon inhérente. A ce sujet, nous renvoyons aux commentaires concernant l'art. 73.

*Protection des droits fondamentaux des personnes résidant en Suisse*

Dans le cadre du présent projet, des atteintes graves aux droits fondamentaux peuvent intervenir lors de l'application des mesures soumises à autorisation (art. 22 ss, par ex. écoutes téléphoniques ou enregistrements visuels ou sonores dans des lieux privés). Sont notamment touchés le droit fondamental de la protection de la sphère privée (art. 13, Cst.; art. 8, CEDH) et, selon les cas, d'autres garanties, telles que la liberté personnelle (art. 10, al. 2, Cst.) et les libertés d'opinion et d'information (art. 16, Cst.; art. 10, CEDH). Conformément au projet, les mesures de recherche d'informations soumises à autorisation sont exclusivement mises en œuvre en Suisse et le principe de la protection des droits fondamentaux établi à l'art. 22 ss ne concerne de ce fait que les personnes résidant en Suisse.

Les mesures soumises à autorisation prévues dans le projet tiennent compte des exigences d'une base légale formelle précise et détaillée. Le concept proposé tient également compte du principe de la proportionnalité et de la présence d'un intérêt public suffisant.

S'agissant de la nature des mesures de recherche d'informations, le projet n'en contient aucune impliquant une atteinte à l'intégrité physique (fouille corporelle ou contrainte physique). Ce type de mesure est réservé aux autorités de police, qui peuvent faire usage de contrainte policière ou de mesures policières pour accomplir leurs tâches (voir la loi sur l'usage de la contrainte[9]).

Le projet de loi comporte (comme la LMSI) l'interdiction de rechercher en Suisse et de traiter des informations relatives aux activités politiques et à l'exercice de la liberté d'opinion, d'association ou de réunion. Voir à ce sujet les explications concernant les art. 3 à 5.

*Protection des droits fondamentaux des personnes à l'étranger*

La recherche d'informations à l'étranger est délicate car elle peut toucher la souveraineté d'Etats étrangers et les droits fondamentaux de citoyens étrangers (par ex. la sauvegarde de la sphère privée).

De ce fait, il ne faut procéder à une recherche d'informations à l'étranger que si les informations nécessaires pour lutter contre un danger ne peuvent être obtenues en Suisse. Cette recherche est destinée à lutter contre les dangers émanant pour la Suisse d'événements importants à l'étranger en matière de politique de sécurité, par exemple dans les domaines du terrorisme, de la prolifération et de l'évolution des rapports de force politiques.

Dans le champ de tension entre les intérêts de sécurité de la Suisse et la protection des droits fondamentaux de citoyens étrangers, respectivement de personnes à l'étranger, le concept du présent projet privilégie les intérêts de la sécurité. De ce fait, la prise en compte de la protection des droits fondamentaux de personnes à l'étranger doit être moins globale que celle de personnes en Suisse.

[9] RS **364**

Dans tous les cas, le principe de la proportionnalité doit être respecté: l'ingérence dans les droits fondamentaux et le gain d'informations qui en est attendu doivent être conformes à ce principe.

Par rapport aux prescriptions qui régissent la protection des droits fondamentaux en Suisse, la restriction proposée concerne en particulier les mesures au sens de l'art. 22. Les raisons qui militent contre une obligation d'autorisation analogue à celle de la Suisse – hormis les principes essentiels indiqués ci-devant – sont les suivantes:

- Pour une instance suisse chargée d'autoriser une telle mesure, il serait difficile ou même impossible, vu la distance, de se faire rapidement une idée de la situation sur place et de prendre une décision qui en tienne compte dans de brefs délais.
- L'autorisation de l'instance suisse ne changerait rien à l'illicéité de la mesure par rapport au droit étranger.

Si par contre des informations sur *l'étranger* sont recherchées *en Suisse,* ce sont les prescriptions de la protection des droits fondamentaux en vigueur en Suisse qui sont applicables, en particulier pour les mesures de recherche d'informations soumises à autorisation, à l'exception de l'introduction dans des systèmes informatiques et des réseaux informatiques qui se trouvent à l'étranger (art. 32, al. 2).

Délimitation par rapport aux activités des autorités de poursuite pénale

Contrairement aux autorités de poursuite pénale, dont les activités consistent à confondre l'auteur d'un acte répréhensible (but répressif), le SRC est chargé de tâches de prévention. Le projet souligne à l'art. 1 (Objet et but) le caractère préventif des mesures prises par le SRC (recherche d'informations, appréciation globale de la situation de la menace). La détection précoce des menaces pour la sûreté intérieure et extérieure de la Suisse et la préservation des fondements démocratiques et de l'Etat de droit sont donc les objectifs de ces mesures.

Lorsque le SRC découvre des actes répréhensibles dans le cadre de ses activités ou qu'il soupçonne de tels actes, il en informe les autorités de poursuite pénale.

## 2 Commentaires concernant le projet de loi

*Remarques préliminaires*

*Concernant le terme de « menace »:*

Selon la définition du Conseil fédéral dans son 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)[10].

Le projet de loi utilise donc 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 qu'ils peuvent comporter une chance d'empêcher ou de détourner une menace.

[10] FF **2010** 4681

*Articles éloquents:*

Les articles et alinéas éloquents qui ne jouent pas de rôle central dans le texte de loi ne font pas l'objet de commentaires dans le projet mis en consultation afin de ne pas trop le charger. Si les résultats de la consultation devaient révéler des malentendus, ils pourront être commentés ultérieurement dans le message.

Préambule:

Se fondant sur la récente pratique en matière de législation, le préambule renonce à mentionner la compétence constitutionnelle inhérente de la Confédération pour le maintien de la sûreté intérieure et extérieure de la Suisse. Selon la doctrine actuelle, cette compétence est contenue dans l'art. 173, al. 2, Cst. (L'Assemblée fédérale traite en outre tous les objets qui relèvent de la compétence de la Confédération et qui ne ressortissent pas à une autre autorité fédérale).

De cette compétence découle, entre autre, 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. Nous renvoyons à ce sujet aux commentaires concernant l'art. 7 (Autorités d'exécution cantonales) et l'art. 73 (Exécution par les cantons).

## Chapitre 1: Dispositions générales et principes applicables à la recherche d'informations

*Art. 1* Objet et but

Compte tenu de l'importance du présent projet de codification globale pour le Service de renseignement de la Confédération, il est justifié qu'un article figure dans la loi en précisant l'objet et le but.

Alors que *l'al. 1* ne fait que résumer le contenu du texte de loi, *l'al. 2* reprend des éléments de la LMSI. Il a de ce fait un caractère programmatoire. Il définit les objectifs sur lesquels doivent se concentrer les activités du renseignement. *L'al. 2* ne fixe pas de compétences, mais fait office de ligne directrice pour l'exécution de la loi.

*L'al. 3* doit permettre au Conseil fédéral, lors de situation 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 ordinaire. Conformément à l'art. 62, un arrêté spécial du Conseil fédéral est requis à ce sujet. Le SRC n'est donc pas autorisé à prendre des mesures de son propre chef. L'arrêté du Conseil fédéral ne donne pas au SRC de compétences particulières allant au-delà de celles qui lui sont conférées. Pour les activités de recherche d'informations, ce sont par conséquent les dispositions légales qui sont en vigueur, en particulier pour la mise en œuvre des mesures soumises à autorisation (art. 22 ss), qui doivent être demandées par la voie de la procédure ordinaire et qui doivent être justifiées. Dans son arrêté, le Conseil fédéral peut, par contre, fixer des conditions pour les activités du SRC, en limitant par exemple à l'étranger l'activité d'exploration ou en excluant certaines mesures de recherche d'informations (par ex. celles soumises à autorisation).

Lorsque sont invoqués d'autres intérêts essentiels de la Suisse, non inclus dans le mandat ordinaire du SRC, il s'agit en règle générale de recherches d'informations à l'étranger.

Cet alinéa 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. 7a à 7d de la loi sur l'organisation du gouvernement et de l'administration, RS 172.010).

*Art. 3* Principes applicables à la recherche d'informations

La tâche principale du SRC est de rechercher et d'analyser des informations et de les transmettre sous forme de produits du renseignement aux destinataires concernés ou de mettre à profit les connaissances acquises pour des prestations opérationnelles de prévention en vue de réduire les menaces pour la sûreté de la Suisse. C'est pourquoi l'art. 3 du projet définit des principes pour la recherche d'informations également valables pour toutes les autres dispositions. Ces principes doivent être appliqués par le SRC en tant qu'autorité d'exécution de la Confédération, et également par les autorités cantonales chargées de l'exécution de la LRens ou accomplissant des activités sur mandat du SRC.

Les objectifs des divers alinéas sont en partie réglés 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. A ce sujet, il est important de bien connaître les sources réputées publiques (voir art. 11) afin de pouvoir déterminer les informations qui doivent y être recherchées et qui peuvent, par la suite, être confirmées ou infirmées à l'aide de moyens du renseignement.

*L'al. 2* renvoie au système des mesures de recherche soumises à autorisation ou non présentées en détail au chap. 3. Leur mise en œuvre est réglée dans ce chapitre. Les mesures qui ne sont pas soumises à autorisation (art. 11 ss) sont utilisées par le SRC sous sa propre responsabilité et ne doivent pas être avalisées (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. 22 ss) ne peuvent être mises en œuvre que dans les cas prévus par la loi. Elles doivent être approuvées par le Tribunal fédéral administratif puis avalisées par le chef du DDPS.

*L'al. 3* se réfère à l'application par le SRC du principe général de proportionnalité: l'idée maîtresse de ce principe est d'assurer que l'ingérence nécessaire dans les droits fondamentaux est en adéquation avec le but visé. Cette disposition prescrit au SRC, pour accomplir son mandat, de toujours opter pour la mesure qui, selon toute vraisemblance sera la moins intrusive dans les droits fondamentaux de la personne concernée. Lorsqu'il est possible d'obtenir une information nécessaire avec une mesure non soumise à autorisation, la préférence sera donnée à une telle mesure.

*L'al. 4* est nécessaire pour déroger au principe général de protection des données stipulant 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). La règle de l'al. 4 correspond à l'art. 5, al. 1, LFRC, et à l'art. 14, al. 1, LMSI. Une recherche et un traitement reconnaissables par la personne concernée déjouerait en règle générale le but du traitement des données. La personne concernée dispose par contre d'un droit d'être informée, qui est réglé à l'art. 58.

Les *al. 5 à 8* reprennent en substance les principes ainsi que les exceptions définis dans la LMSI qui ont fait leurs preuves et qui interdisent la surveillance des activités politiques à des fins de renseignement. La LRens garantit ainsi la même protection

que la LMSI pour des activités 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 selon l'al. 6 concernant 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 d'y 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. Dans ce cas, la recherche et le traitement des informations concernent cette personne, et pas 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 apparemment à des fins culturelles. Une soirée folklorique avec la participation de musiciens n'est pas conforme au but annoncé, mais 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 plus détaillées de l'art. 3 LMSI, entrées en vigueur en 2012. Lorsque des données doivent être effacées, le SRC à l'obligation de les proposer aux Archives fédérales. Les données qui ne sont pas dignes d'être archivées sont définitivement détruites.

*L'al. 8* précise que toutes les informations sur des organisations et des groupements inscrits sur la liste d'observation visée à l'art. 63 peuvent être recherchées et traitées lorsqu'elles se prêtent à une appréciation de la menace. Cette disposition, dont l'application comportait quelques ambiguïtés, était jusqu'à présent contenue dans les réglementations de la LMSI concernant la liste d'observation. Avec sa nouvelle intégration dans la systématique, ces ambiguïtés sont évitées.

## Chapitre 2: Tâches et collaboration du SRC

### Section 1: Tâches, mesures de protection et de sécurité et port d'armes

*Remarques liminaires*

Le SRC contribue en priorité à la sécurité de la Suisse par des activités de prévention. Mais il peut aussi, à l'aide de ses moyens spéciaux, soutenir d'autres services de la Confédération dans l'accomplissement de leurs tâches (voir art. 60).

L'activité de prévention du SRC doit être clairement délimitée par rapport aux activités de répression des autorités de poursuite pénale. Le premier but du SRC est de déceler à temps et prévenir 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 procédures pénales (par ex. enquêtes, arrestations, etc.). Les activités du SRC et des autorités de poursuite pénale sont complémentaires; elles ne sont pas préparatoires les unes 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 réciproque d'informations entre le SRC et les autorités de poursuite doit de ce fait obéir à des règles précises.

*Art. 4* 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. 73). Leur contenu correspond aux domaines de compétences fixés dans la LMSI. Ils sont complétés par la mention explicite d'attaques contre des infrastructures d'information, 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 jusqu'à présent, des tâches définies aux ch. 1 et 2. Un tel lien ne se révélant souvent qu'à la suite d'investigations approfondies, il est nécessaire, pour que le SRC puisse assumer son rôle dans le cadre de la stratégie de protection des infrastructures critiques de la Confédération, qu'il puisse participer aux recherches sur de tels événements dès le début. Les réseaux des infrastructures d'information doivent être protégés contre les attaques des cyber-pirates. Dans ce domaine, le SRC doit continuer à rechercher les informations nécessaires sur les menaces d'attaques ou les attaques qui se sont produites pour les services chargés de s'en occuper 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'événements importants 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 d'Etat de droit, de lui infliger de graves dommages en matière de politique de sécurité ou autres ou d'entraver la capacité d'agir de ses autorités.

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

Est aussi nouvellement introduite la notion de « sauvegarde d'autres intérêts essentiels de la Suisse » (voir les commentaires relatifs à l'art. 1, al. 3).

La recherche et le traitement de données selon *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'alertes relèvent de la compétence d'autres services (par ex. de 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 WEF ou de grandes conférences internationales, telles que le Sommet de la francophonie), le SRC, pour assurer les tâches stipulées aux al. 2 et 3, met sur pied un Réseau national de renseignement. Ce dernier coordonne la recherche et la diffusion d'informations et permet aux services habilités à participer à ce réseau de suivre en permanence l'évolution de la situation par le biais de la Présentation électronique de la situation (PES, voir art. 48).

La fonction du SRC en tant d'autorité responsable pour les contacts en matière de renseignement avec l'étranger, telle que fixée aujourd'hui à l'art. 8 LMSI, est stipulée à *l'al. 4*. Les doublons et les contradictions dans les échanges avec des services partenaires étrangers doivent ainsi être évités. Cette fonction est décrite plus en détail à l'art. 10.

L'*al. 5* est consacré aux tâches de prévention relevant de l'unité opérationnelle et 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 aujourd'hui déjà à l'alerte précoce d'un cercle défini d'exploitants d'infrastructures critiques. Cette fonction importante va au-delà d'un traitement exclusif d'informa-tions selon l'al. 1, let. a, ch. 5, raison pour laquelle elle est expressément réglée ici.

*L'al. 7* revêt une importance particulière pour la sécurité du SRC, de ses collaborateurs, de ses installations, de ses sources et des données qu'il traite. L'art. 5 contient des règles plus précises à ce sujet. Parallèlement à la LRens, la Confédération élabore aussi une base légale pour la sécurité des informations et des objets. Le cas échéant, elle réglera certains besoins spécifiques du SRC dans ce domaine sous une forme générale pour l'ensemble de l'administration fédérale. Pour l'instant, c'est la LRens qui doit assurer que le SRC soit chargé de garantir 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 à l'art. 60.

*Art. 5* Mesures de protection et de sécurité

Les mesures de protection et de sécurité stipulées 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. Ces mesures sont destinées à l'application des prescriptions relatives au secret de fonction et augmentent de ce fait la sécurité et la crédibilité du SRC concernant le traitement de données classifiées.

Pour garantir la sécurité, les mesures consacrées à la formation et à la sensibilisation ont priorité sur d'autres mesures. Dans ce contexte, la prise de mesures techniques et de contrôle du respect des prescriptions font 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 ainsi que le personnel engagé temporairement au SRC, tels que des stagiaires ou des membres de l'armée par exemple. Peuvent également être contrôlés les collaborateurs des entreprises qui fournissent des prestations dans les locaux du SRC. Ne font pas l'objet de contrôles les membres des organes de surveillance et les visiteurs, qui sont accompagnés en permanence lorsqu'ils se trouvent dans les locaux du SRC.

*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 classifiées et/ou particulièrement dignes d'être protégées ainsi que dans les entrepôts de biens de valeur.

*Let. d:* Les locaux dans lesquels ont lieu des discussions portant sur des contenus très sensibles et hautement classifiés sont si possible équipés de systèmes de protection passive (bouclier d'assourdissement et isolation acoustique) qui interdisent que des informations parviennent 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 téléphones mobiles. Dans ces cas, il sera veillé 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 contenus sensibles ou classifiés secrets. Les installations de brouillage doivent être conformes aux prescriptions de l'OFCOM et aux normes en vigueur.

*L'al. 2* constitue la base légale pour le réseau informatique hautement sécurisé que le SRC exploite aujourd'hui 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.

*Art. 6* Port d'armes

Lors de la recherche d'informations dans le domaine du terrorisme, de l'espionnage, de l'extrémisme violent, du trafic d'armes et du commerce illégal d'armes chimiques, biologiques et nucléaires de destruction massive, les collaborateurs qui en sont chargés 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 eux-mêmes 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 la police qui ont recours aux services de personnes de confiance.

L'arme ne peut être utilisée qu'en cas de légitime défense (art. 15f du Code pénal[11]) ou en état de nécessité licite (art. 17, CP). L'usage de l'arme à feu doit en particulier respecter le principe de la proportionnalité (al. 2).

Cette disposition correspond dans ses grandes lignes à l'art. 5a LMSI en vigueur aujourd'hui. En plus des dispositions d'exécution du Conseil fédéral, le SRC réglera dans des directives, comme c'est le cas aujourd'hui, les détails pour le port d'une arme de service (entre autres des directives pour justifier d'une formation suffisante, de l'autorisation de porter une arme et des entraînements obligatoires de tir).

**Section 2: Collaboration**

[11] RS **311.0**

*Art. 7* Autorités d'exécution cantonales

Le présent projet prévoit que les tâches de renseignement soient exécutées en commun par la Confédération et les cantons (voir art. 73). Les autorités d'exécution cantonales recherchent sur leur territoire les informations qu'elles doivent se procurer directement en fonction de la LRens ou d'un mandat particulier du SRC. A cet effet, comme cela a été le cas jusqu'à présent, les cantons désignent un service spécialisé pour accomplir ces tâches. En règle générale, ce service fait partie du corps de police.

D'autres prescriptions en lien avec les cantons se trouvent au chap. 4 (concernant le traitement des données) et au chap. 5 (concernant le contrôle et la surveillance).

*Art. 8* Information des cantons

La nouvelle loi doit aussi accorder toute son importance à l'étroite collaboration entre la Confédération et les cantons. Comme elle l'a fait jusqu'à présent, la Confédération est chargée d'informer les autorités cantonales compétentes des événements particuliers survenant dans le domaine d'activité du SRC et de la situation 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 directrices et 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 en accord avec les besoins de la Confédération.

*Art. 9* 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 assurant le service de sécurité militaire, telle qu'elle existe depuis la création du SRC, doit être maintenue.

Ces deux services travaillent dans des domaines thématiques apparentés pour l'appréciation de la menace et de la sécurité pour les besoins de l'armée. L'art. 9 règle l'obligation du SRC d'informer les services compétents de l'armée d'événements importants susceptibles d'avoir une incidence sur l'exécution de leurs tâches. L'obligation de ces services d'informer le SRC est réglée à l'art. 17 (Obligation de renseigner en cas de menace concrète) et à l'art. 18 (Obligation spécifique de fournir et de communiquer des renseignements). Les détails de la collaboration doivent être fixés (en principe selon le modèle actuel) dans l'ordonnance d'exécution du présent projet de loi.

*L'al. 2* doit permettre au SRC, dans certains cas, de charger les attachés de défense de l'armée de rechercher pour lui des informations et d'assurer le suivi des contacts avec des services partenaires étrangers. 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 personnes de liaison du SRC annoncées auprès des services de renseignement concernés des Etats où ils sont accrédités. Cette manière de procéder a fait ses preuves, par exemple lors de cas d'enlèvements ou de l'observation des développements du « printemps arabe ».

*Art. 10* Collaboration avec l'étranger

En guise d'introduction, il faut indiquer que le Conseil fédéral a explicitement renoncé à mentionner 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). Ce principe est déjà appliqué conformément à la disposition de l'art. 56, al. 3, Cst. L'exécution par les cantons ne s'en trouve donc en rien modifiée.

Concernant *l'al. 1,* il est à noter que dans le domaine du renseignement, la Suisse n'est pas liée par des contrats de droit international, mais qu'elle conclut tout au plus des « arrangements » (agreements), ou, le cas échéant, des « déclarations d'intention » (Memorandums of Understanding, MoU), qui ne sont pas contraignants. La raison de cette pratique est due au fait 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, ce qui est le cas aujourd'hui pour la Suisse avec un grand nombre de pays, par exemple dans les domaines de la défense contre le terrorisme, l'espionnage, l'extrémisme violent ou des questions militaires ou relatives aux rapports de force politiques. Les Etats veulent rester libres d'adapter leurs intérêts en matière de renseignement à leurs besoins, et ceci sans être liés par des contrats. Il en va de même pour la Suisse.

A l'avenir, une exception pourrait intervenir dans cette pratique 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 renseignement européens, mais ils n'ont pas encore pu être globalement réalisés car dans la plupart des Etats, les bases légales nationales nécessaires pour des systèmes communs font encore défaut et qu'il n'existe pas non plus d'accords internationaux à ce sujet. Le Conseil fédéral propose de fixer dans la LRens le principe que le SRC peut participer à des systèmes d'informations automatisées si de tels systèmes sont créés. Etant donné qu'il s'agit d'une forme particulière de collaboration internationale, elle devrait, pour des raisons de protection des données, être réglée dans le cadre d'un accord technique. Dans ce cas, la compétence pour la conclusion d'un tel accord relèverait du Conseil fédéral (art. 61, al. 3).

A l'avenir, conformément à *l'al. 2* et de façon analogue aux attachés de migration, de défense et de police, le SRC doit pouvoir détacher des collaborateurs de liaison dans les représentations suisses à l'étranger si cela s'avère nécessaire pour la collaboration internationale. L'engagement de telles personnes n'intervient qu'en accord avec le DFAE. Dans ces cas, les collaborateurs du SRC sont en mission officielle. Ils sont annoncés conformément aux règles établies auprès des services compétents du pays d'accueil, des éventuels Etats tiers lors d'accréditations collatérales et ils travaillent exclusivement comme agents officiels de liaison avec les services compétents. Leur mission n'est pas de collecter secrètement des informations et ils ne violent pas le droit des Etats hôtes.

*L'al. 3* doit garantir que les contacts de la Suisse avec d'autres pays dans le domaine du renseignement soient exclusivement menés en conformité avec les réglementations de la LRens. Le même principe est déjà fixé sous une forme similaire à l'art. 8 LMSI et il est précisé plus en détail aux art. 11, al. 1 et 2 de l'ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération[12] (OSRC). La

[12] RS **121.1**

tâche du SRC en tant qu'« office leader » ne concerne cependant que les contacts avec des services de renseignement et avec d'autres autorités étrangères lorsqu'il s'agit de contenus du renseignement, et ceci particulièrement dans le cas de contacts avec des autorités étrangères qui assument plusieurs fonctions (par ex. police judiciaire et service de renseignement intérieur). Dans ces cas, les contacts ayant un contenu à caractère policier (police judiciaire) relèvent de la compétence des autorités suisses de police.

**Chapitre 3: Recherche d'informations**

Conformément à la définition globale de la notion de traitement des données de la LPD, leur recherche fait aussi partie de leur traitement (voir art. 3, let. e, LPD). 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 être liée à des ingérences significatives dans les droits fondamentaux, il est justifié que des règles concernant leur recherche et leur traitement ultérieur fassent l'objet de chapitres séparés.

Les dispositions du chap. 3 ne citent que le SRC comme service de recherche d'informations. Dans le cadre de leurs mandats d'exécution (art. 7 et 73), ces dispositions sont aussi valables pour les autorités d'exécution cantonales.

**Section 1: Mesures de recherche non soumises à autorisation**

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 du fait que leur ingérence dans les droits fondamentaux est relativement faible. Elles correspondent très largement aux possibilités de recherche actuelles fixées à l'art. 14, al. 2, LMSI. Ce chapitre contient tous les moyens classiques de recherche d'informations d'un service de renseignement, de l'observation dans des lieux publics et des lieux librement accessibles (art. 12), d'enregistrements visuels et sonores (art. 12, al. 2), des informateurs (art. 13) à l'exploration radio (art. 24 et 33 ss). Selon l'importance de leur ingérence dans les droits fondamentaux, la loi fixe des règles particulières pour l'utilisation de ces mesures.

*Art.11* Sources d'informations publiques

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

Ce type de recherche est le plus faible au niveau de l'ingérence dans les droits fondamentaux puisqu'il s'agit d'informations pratiquement accessibles à tout un chacun. Le fait que certaines informations soient proposées contre paiement ne change en rien leur caractère public. Les banques de données électroniques ne doivent pas ici être traitées différemment que les médias classiques, tels que des journaux ou des ublications spécialisées, qui, en règle générale, sont aussi proposés contre paiement.

La qualité des informations provenant de sources publiques 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 le portail ROSO (art. 49). En cas de besoin, elles peuvent ensuite être évaluées et transférées dans d'autres systèmes pour être utilisées pour des produits du renseignement.

*Art. 12* Observations dans des lieux publics et dans des lieux librement accessibles

*L'al. 1* reprend les règles en vigueur de l'art. 14, al. 2, let. f, LMSI. L'observation et la documentation d'événements dans des lieux publics et dans des lieux en général 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 en général librement accessibles au public.

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

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

*L'al. 2* 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 pouvoir faire appel à des moyens aériens adéquats, tels que des drones, des avions ou des hélicoptères. Des moyens spatiaux, par exemple des satellites, peuvent également être appropriés pour l'exploration d'images (par ex. lors de cas d'enlèvements de citoyens suisses à l'étranger). Des photos satellite permettent aussi d'observer les progrès de programmes étrangers d'armes de destruction massive. Le SRC ne dispose pas lui-même de tels moyens, mais peut en demander l'engagement auprès de tiers. Le Service de renseignement militaire dispose d'un centre IMINT (Imagery Intelligence) pour l'obtention et l'évaluation de ce type d'informations. Des photos satellite sont essentiellement fournies par des entreprises commerciales, la Suisse ne disposant pas non plus de ses propres moyens dans ce domaine.

Ces observations sont indispensables pour une évaluation indépendante et autonome d'événements importants du point de vue de la politique de sécurité. Les appréciations du SRC soutiennent directement la politique étrangère de la Suisse, par exemple en fournissant au DFAE des pronostics sur le temps encore à disposition pour des négociations avec un Etat pratiquant la prolifération.

Les événements sur terre ne font pas partie de l'espace public lorsqu'ils se déroulent par exemple dans un appartement ou sur un terrain privé. Si de tels événements doivent être observés de manière ciblée, la recherche d'informations doit faire l'objet d'une demande de mesure soumise à autorisation (art. 22 ss). Dans les autres cas, les données doivent être détruites si l'espace privé n'a pas déjà pu être écarté lors de l'observation. La situation est comparable à celle d'un avion de ligne survolant une zone habitée. On ne peut empêcher que des passagers observent ou photo-

graphient par les hublots des événements qui se déroulent à terre dans l'espace privé. L'utilisation de telles images serait toutefois susceptible d'être attaquée en justice.

Une règle analogue doit être ancrée dans la loi du 3 février 1995 sur l'armée[13] (art. 99, al. 1$^{quater}$, voir Abrogation et modification du droit en vigueur).

*Art. 13* Informateurs

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

Lorsque un groupement terroriste en Suisse ou à l'étranger planifie par exemple des attentats en Suisse contre des citoyens ou contre des intérêts suisses à l'étranger, ces informations ne peuvent en général être obtenues que par des personnes qui ont un accès direct ou indirect à ce groupe. Pour des raisons de sécurité, les planifications et les activités du groupe ne font que très rarement l'objet de documents ou d'échanges écrits et les informations internes ne sont transmises 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 sur la base d'un décompte de frais et/ou pour le paiement d'informations déterminantes pour l'accomplissement des tâches confiées au SRC. Des informateurs, résidant en particulier à l'étranger, demandent souvent de l'argent pour communiquer leurs informations. Leur indemnisation, si elle devient notoire, peut représenter pour les informateurs un risque important tant dans leur pays d'origine que pour leur entourage. Un soupçon de revenus provenant d'activités et de relations liées au renseignement peut causer à un informateur un préjudice professionnel, ruiner sa réputation et, selon le pays et l'entourage, représenter un danger pour son intégrité corporelle et pour sa vie. C'est pour ces raisons que dans la plupart des cas, les indemnités versées aux informateurs ne peuvent être ni déclarées ni imposées ou assujetties aux assurances sociales habituelles. 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 parfois être officialisés par le biais de structures de couverture.

*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. Cela est particulièrement le cas dans l'entourage de cellules terroristes, de 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 courir un danger très important dans leur pays

[13] RS **510.10**

d'origine. Leur découverte, en dernière conséquence, peut signifier pour eux une condamnation à mort:

- Des scientifiques nucléaires de pays asiatiques 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 aux régimes installés en Suisse faisaient régulièrement l'objet d'une observation ou de molestations de la part de personnes fidèles au régime en provenance de leurs pays. Si une éventuelle collaboration avec le SRC d'informateurs dans l'entourage de ces opposants était découverte, cela pourrait non seulement mettre en danger 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 de ses informateurs avec tous les moyens dont il dispose. Dans le cadre de la gestion de ses informateurs, le SRC veille en permanence à assurer leur protection maximale. Les mesures qui peuvent être prises afin d'assurer cette protection comportent aussi, dans certains cas exceptionnels, des permis de séjour en Suisse pour un informateur et les membres de sa famille ou l'attribution d'une couverture ou d'une identité d'emprunt. Pendant l'engagement actif d'un informateur, conformément aux art. 15 et 16, le SRC peut le doter d'une couverture ou d'une identité d'emprunt si cela est nécessaire à sa protection.

Au terme de son activité pour le SRC, le danger pour l'intégrité corporelle et la vie d'un informateur peut persister. 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 12 mois fixé pour l'examen de cette mesure lors d'un engagement actif n'est plus appliqué. En outre, cette mesure est mise en œuvre aussi longtemps que le danger persiste pour l'informateur et éventuellement pour ses proches. Comme dans ces cas le SRC n'a en règle plus de contacts réguliers avec l'informateur, il est prévu que le chef du DDPS autorise l'attribution d'une couverture ou d'une identité d'emprunt pour que les risques politiques puissent aussi être évalués dans ces cas.

*Art. 14* Signalements pour la recherche du lieu de séjour de personnes et la localisation de véhicules

Les *al. 1 et 2* doivent introduire une réglementation similaire à celle que prévoit la nouvelle loi sur les tâches de police de la Confédération (Chap. 3: Mesures visant à prévenir les infractions). Mais contrairement à cette loi, le présent projet n'est 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. Une menace concrète pour la sûreté intérieure et extérieure, respectivement un arrêté du Conseil fédéral pour la sauvegarde d'autres intérêts essentiels de la Suisse (voir l'art. 1, al. 3, en relation avec l'art. 62) est donc une condition pour le signalement de personnes et de véhicules par le SRC (voir l'al, 2, let. a).

Le présent projet fixe ainsi dans la loi la possibilité de pouvoir déterminer, comme cela est déjà le cas aujourd'hui, le lieu de séjour et les mouvements de personnes

(par ex. de membres de groupements soupçonnés de terrorisme) et de véhicules ciblés par leur signalement dans le Système de recherches informatisées de la police (RIPOL). La législation relative à la police parle dans ce cas de « surveillance discrète », notion qui n'est pas reprise dans la LRens afin d'éviter des malentendus. A l'avenir, cette possibilité de signalement doit aussi être donnée dans la partie nationale du Système d'information Schengen (N-SIS). Lorsque des personnes signalées par le SRC entrent dans un pays membre de Schengen, le quittent ou qu'elles sont contrôlées par la police ou par les organes de la douane à l'intérieur de cet espace, la Suisse, respectivement le SRC, recevra à l'avenir une communication de la part des autorités étrangères compétentes. L'annonce est transmise par l'intermédiaire du bureau suisse de SIRENE (point de contact pour la collaboration SIS entre autorités compétentes des Etats Schengen; voir art. 8 et 9 de l'ordonnance N-SIS ; RS 362.0). Il va de soi que de cas en cas, il s'agit d'examiner si un signalement est nécessaire et approprié. Il n'existe en particulier pas d'automatisme de signalement entre RIPOL et le système Schengen.

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

### Section 2: Couverture et identité d'emprunt

*Remarques liminaires*

Sur la base de l'art. 99 de la loi sur l'armée et l'administration militaire, le Service du renseignement stratégique (SRS) disposait, depuis 1997, 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; FF *2004* 1594). Depuis le regroupement du SAP et du SRS ayant donné lieu à la création du SRC, l'art. 16, al. 1, let e, OSRC, prévoit expressément l'utilisation de papiers d'identité fictifs et d'assertions trompeuses en lien avec la recherche d'informations à l'étranger. Depuis 1997, des identités d'emprunt et des couvertures (fausses qualités) 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 au contrôle du chef du DDPS, de la Délégation du Conseil fédéral pour la sécurité et de la Délégation des Commissions de gestion.

Suite à l'adoption par le Parlement de la révision de la LMSI, le 23 décembre 2011, la possibilité d'utiliser aussi des identités d'emprunt et des couvertures pour la recherche d'informations en Suisse a nouvellement été fixée à l'art. 14c. A la différence du processus d'autorisation interne au SRC pour les identités d'emprunt liées à 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. 14c, al. 1, let. c, LMSI, permet désormais d'attribuer également des identités d'emprunt à des informateurs du SRC dans le cadre d'une mission spécifique de recherche d'informations.

Les art. 15 et 16 font nouvellement une distinction entre la notion de « couverture » et « d'identité d'emprunt » car il s'agit de mesures différentes qui peuvent être prises indépendamment l'une de l'autre.

Dans le présent projet, les différentes réglementations en vigueur aujourd'hui pour les identités d'emprunt sont regroupées et elles sont applicables pour la recherche d'informations en Suisse et à l'étranger. En outre, une attention plus soutenue est accordée à leur objectif de protection. Compte tenu de la nouvelle réglementation introduite par la LMSI, le Conseil fédéral propose de confier au chef du DDPS la compétence pour l'octroi d'identités d'emprunt pour les activités en Suisse et à l'étranger.

La compétence pour l'autorisation de couvertures doit être attribuée au directeur du SRC. Elles ne nécessitent en effet pas de pièces d'identité comportant de faux noms et elles ne permettent pas d'effectuer des actes juridiques sous un faux nom.

*Art. 15* Couverture

Une couverture permet de dissimuler l'appartenance d'une personne au SRC en indiquant par exemple un autre nom d'employeur que ce service et une autre activité professionnelle que celle exercée. Mais la personne garde son vrai nom ainsi que d'autres données la concernant (date de naissance, lieu de naissance, etc.). Une couverture peut être nécessaire pour rendre possible 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 Etats et y être sévèrement puni).

Il n'est pas possible pour un collaborateur du SRC de se rendre à l'étranger pour une mission secrète de recherche d'informations et simultanément d'être clairement identifiable comme un collaborateur du renseignement. Les collaborateurs concernés et les informateurs avec lesquels ils sont en contact pourraient 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 de l'évolution 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 liées au renseignement à l'étranger, il est donc nécessaire de pouvoir établir des couvertures en rapport avec la véritable identité des personnes concernées.

Les couvertures constituent souvent une mesure à long terme et elles ne sont pas liées à certaines opérations en particulier. Selon la protection requise, leur établissement ne peut demander qu'un un délai assez court (par ex. l'achat d'un téléphone prépayé et l'impression de cartes de visite fictives) ou plus long (par ex. trouver/créer un employeur fictif, garantir que la personne est atteignable par téléphone, par courriel, etc.).

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 veut fournir à cette pratique une base légale plus claire.

Si l'établissement de couvertures implique le soutien d'autorités suisses, ces dernières doivent être tenues de collaborer. Cela peut être le cas si certains documents

officiels s'avèrent nécessaires pour la crédibilité de la couverture (par ex. pour rendre crédible une activité commerciale).

La surveillance permanente de ces mesures est assurée par l'obligation d'en faire rapport chaque année au chef du DDPS.

*Art. 16* Identité d'emprunt

Une identité d'emprunt attribue une autre identité à une personne, c'est-à-dire un autre nom et, le cas échéant, d'autres données la concernant (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 également dissimuler le lien avec le SRC, par exemple indiquer un autre employeur que ce dernier. Lorsqu'il ne s'agit toutefois que de protéger un collaborateur en tant que personne et non 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 sont tributaires de pouvoir les munir d'identités d'emprunt et des couvertures qui s'y rapportent. Les recoupements avec la vraie identité des collaborateurs qui procèdent à des recherches d'informations, par exemple dans le domaine du terrorisme ou de l'espionnage, peuvent les exposer et aussi les membres de leurs familles à des tentatives directes de pression, à des menaces, voire à des dangers concrets pour leur intégrité corporelle. Les identités d'emprunt sont de ce fait et en premier lieu une mesure de protection permanente pour le personnel chargé de rechercher des informations.

Outre leur mission 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 le domaine du terrorisme, de l'espionnage ou dans le cadre d'une mission de recherche à l'étranger, tout lien du collaborateur concerné 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 lors du 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 l'établissement 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. L'utilisation des identités d'emprunt est limitée dans le temps et peut au besoin être prolongée (voir l'al. 2). Elle est soumise à des critères bien précis, qui doivent dans tous les cas être respectés selon l'al. 3.

La constitution d'une identité d'emprunt implique aussi le droit d'exécuter des actes juridiques sous ce nom, notamment de créer des structures de couverture qui dissi-

mulent le lien avec le SRC. Contrairement aux couvertures qui utilisent la véritable identité (art. 15), leur mise au point avec des identités d'emprunt demande souvent un effort beaucoup plus conséquent puisqu'elles doivent être en rapport avec une identité fictive, un employeur plausible, un domicile fictif, etc., pour être crédibles. Les personnes dotées d'une identité d'emprunt bénéficient de leur pleine personnalité juridique et peuvent conclure des contrats (par ex. location de locaux et de véhicules, raccordements de télécommunication, création de structures de couverture, 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. Il est ainsi garanti que ces identités 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. 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 limite maximum fixée arbitrairement, sa durée d'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 12 mois.

*L'al. 3* fixe les critères pour l'utilisation d'identités d'emprunt à des fins de recherche d'informations en fonction du principe de la proportionnalité et de la subsidiarité.

*L'al. 4* permet l'établissement de pièces d'identité d'emprunt et d'autres documents: pour ce faire, le SRC est tributaire 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 courrent un danger particulier en leur attribuant une autre identité pendant la période où un tel danger existe. Ce n'est par ailleurs qu'exceptionnellement et avec beaucoup de retenue que des papiers d'identité suisses doivent être mis à disposition d'étrangers. Dans ces cas, l'attribution temporaire de papiers suisses ne leur accorde bien évidemment pas durablement la nationalité suisse.

## Section 3: Droits d'obtenir des renseignements et obligation de fournir des renseignements

### *Art. 17* Obligation de renseigner en cas de menace concrète

Pour accomplir les tâches qui lui sont confiées, le SRC est tributaire d'informations qui lui sont ou qui doivent lui être communiquées par des tiers (services de la Confédération et des cantons, organisations chargés de tâches publiques). Ces informations peuvent être communiquées à la demande du SRC ou spontanément par un service tiers qui constate une menace concrète pour la sûreté de la Suisse.

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 ceux de la sauvegarde de la sphère privée des citoyens. 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 renseigner pour certaines menaces spécifiques, pour autant qu'elles risquent de léser des biens juridiques importants. Les différentes sources d'où peuvent émaner ces menaces sont indiquées de manière exhaustive à l'al. 2. Il s'agit d'activités terroristes, de l'espionnage (services de renseignements politiques, économiques et militaires) de la prolifération NCB, d'attaques contre des infrastructures critiques ainsi que de l'extrémisme violent. Selon les fondements de l'entraide administrative, cette disposition oblige en principe l'ensemble des autorités et unités administratives de la Confédération et des cantons à communiquer toute information ayant trait à de telles menaces.

Si l'obligation de renseigner est justifiée par l'invocation d'autres intérêts essentiels de la Suisse, elle requiert un arrêté correspondant du Conseil fédéral (voir à ce sujet les explications concernant l'art. 1, al. 3, et l'art. 62).

Cet article correspond dans ses grandes lignes au nouvel art. 13a de la LMSI. Mais il ne cite plus explicitement les autorités fiscales. Ces dernières sont également assujetties à l'obligation de renseigner puisqu'elles font partie des services nommés à l'al. 1. Une mention particulière les concernant pourrait donner l'impression que les autorités fiscales fournissent très souvent des informations au SRC, ce qui n'est pas le cas.

Dans les cantons, l'obligation de renseigner s'étend aussi aux services administratifs des communes; ils sont inclus dans le terme « canton ».

Les organisations qui accomplissent des tâches publiques sont également soumises à l'obligation de renseigner. Il s'agit d'organisations ou de personnes de droit public ou privé chargées de tâches administratives selon l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[14] (LOGA) qui ne font pas partie de l'administration fédérale.

La notion « sur demande motivée portant sur un cas particulier » doit souligner que l'obligation des autorités et des organisations de renseigner est permanente, mais qu'elle l'est uniquement dans des cas précis, concrets et uniquement à la demande du SRC (ou des autorités d'exécution cantonales agissant sur mandat du SRC). Comme cette obligation ne concerne que des cas précis et des menaces concrètes, le nombre relativement important des autorités et des services qui y sont assujettis est justifié.

Les informations obtenues par les autorités et les organisations sont transmises au SRC. Sur mandat de la Confédération, les autorités d'exécution cantonales peuvent prendre des mesures et demander directement aux autorités et organisations soumises à l'obligation de renseigner de rechercher des informations pour les mettre à disposition du SRC. Dans tous les cas, la Confédération reste le maître des données.

*L'al. 4* règle le cas d'une autorité qui constate de façon indépendante une menace pour la sûreté intérieure ou extérieure. Elle doit avoir la possibilité de communiquer spontanément ce renseignement au SRC. Lors d'un soupçon d'acte répréhensible, le pendant à cette disposition est l'art. 22a de la loi du 24 mars 2000 sur le personnel de la Confédération[15] (LPers), qui fait obligation aux employés de la Confédération de dénoncer tous les crimes et délits poursuivis d'office.

[14] RS **172.010**
[15] RS **172.220.1**

*Art. 18* Obligation spécifique de fournir et de communiquer des renseignements

Sont nommés à *l'al. 1* 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. 17, dans la mesure où cette obligation spécifique 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. Contrairement à l'art. 17, elle ne concerne par contre que les autorités et organes cités.

N'est pas entendu ici une obligation intégrale de fournir des informations, mais une obligation en rapport avec des organisations et des cas concrets.

*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, LMSI). La plus grande partie des autorités soumises à l'obligation de renseigner sont publiées à l'annexe 1 de l'OSRC. Les obligations de renseigner sur des événements et des constatations qui ne peuvent être publiées pour des raisons de sauvegarde du secret, doivent, comme jusqu'à présent, faire l'objet d'une liste confidentielle. Les services concernés sont informés séparément de leur obligation de renseigner.

*Art. 19* Procédure en cas de divergences de vues

*L'al. 1* règle les cas de divergences de vues entre le SRC et l'administration fédérale. C'est le chef du DDPS qui statue en première instance lors de litiges au sein du département. Le Conseil fédéral, en tant qu'autorité de surveillance commune, statue définitivement sur les divergences avec les services d'autres départements. Cette pratique correspond aux règles générales de l'organisation de l'administration.

*L'al. 2* règle les cas de divergences entre le SRC et une organisation, un organe ou une autorité n'appartenant pas à l'administration fédérale. La compétence relève dans ces cas du Tribunal administratif fédéral. Comme pendant de cette règle, une disposition fixant la compétence du Tribunal administratif fédéral en cas de divergence est ajoutée en annexe du présent projet à la loi fédérale du 17 juin 2005 sur le Tribunal administratif fédéral[16] (voir Abrogation et modification du droit en vigueur).

*Art. 20* Communications et renseignements fournis par des tiers

Les informations fournies au SRC ou aux autorités d'exécution cantonales par des particuliers sont communiquées à titre facultatif. Lors de l'utilisation de couvertures dissimulant l'appartenance au service de renseignement, l'attention de la personne interrogée ne peut toutefois être attirée sur ce caractère facultatif. Lorsqu'une personne qui communique ou qui fournit des informations est soumise au secret professionnel ou à d'autres prescriptions légales concernant le maintien du 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 personnes ou service officiel.

[16] RS **173.32**

*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 ne sont pas obligatoirement liées à une dissimulation de l'appartenance au SRC.

*Art. 21* Obligations spécifiques de fournir des renseignements pour les particuliers

*L'al. 1* reprend la règle de l'art. 13 c ajouté à la LMSI en 2012, qui fixe l'obligation des transporteurs commerciaux de renseigner, et l'élargit aux exploitants privés d'infrastructures de sécurité, telles que les installations de vidéosurveillance. D'importantes informations peuvent aussi être fournies par des systèmes d'accès électroniques. Comme le stipule la LMSI, personne ne peut être assujetti à l'obligation de relever ou de conserver certaines données spécifiques. Cette disposition est uniquement destinée, en cas de menaces concrètes, à permettre l'accès à des données qui existent de toute manière.

De telles informations pourraient par exemple être importantes pour constater des voyages et des déplacements de personnes impliquées dans des activités terroristes, d'extrémisme violent, d'espionnage ou de prolifération. De telles informations peuvent par exemple être fournies par des compagnies aériennes, des agences de voyages et des entreprises de location de véhicules.

*L'al. 2* se réfère à la possibilité, déjà fixée dans la loi du 30 avril 1997 sur les télécommunications[17] (LTC), d'obtenir par l'intermédiaire du SCPPT des informa-tions sur les raccordements de télécommunication d'une personne et sur d'autres éléments d'adressage, respectivement à qu'elle personne sont attribués des éléments d'adressage identifiés (par ex. des numéros de téléphone). La loi sur les télécommunications est modifiée en conséquent (art. 14, al. 2bis, LTC, voir Abrogation et modification du droit en vigueur).

En cas de nécessité, l'obligation spécifique de renseigner pour les particuliers est imposée par une décision susceptible de recours, arrêtée dans le cadre d'une procédure administrative fédérale, si nécessaire avec renvoi à l'art. 292 du Code pénal (Insoumission à une décision de l'autorité).

Conformément à l'art. 71, les décisions du SRC peuvent être attaquées par voie de recours. La recherche d'informations, par exemple sur des personnes soupçonnées d'activités terroristes au détriment de la Suisse, doit souvent être effectuée dans des délais très courts. S'il fallait dans ces cas attendre la conclusion d'une longue procédure de recours, l'information communiquée ensuite par une entreprise de transport pourrait s'avérer inutile. C'est pourquoi le présent projet prévoit qu'un recours n'a pas d'effet suspensif (art. 71, al. 3).

**Section 4: Mesures de recherche soumises à autorisation**

*Remarques liminaires*

Afin de pouvoir s'acquitter de ses tâches, en particulier de détecter précocement et d'évaluer les menaces et les dangers pouvant limiter la capacité de décision et d'action des autorités suisses ou menaçant les fondements démocratiques ainsi que les

[17] RS **784.10**

structures de l'Etat, le SRC a besoin de moyens efficaces pour collecter des informations.

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:

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 à Montauban. L'auteur était un Français d'origine algérienne prétendant appartenir au groupement 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 cas de personnes ayant des liens avec la Suisse pour lesquelles il est possible de tirer des parallèles avec un cas de radicalisation, tel que celui de Toulouse et Montauban. Les personnes en question se sont radicalisées via Internet et ont séjourné dans des camps d'entraînement terroristes à l'étranger. Les auteurs isolés radicalisés, tels que l'assassin de Montauban et Toulouse mènent une vie discrète et, vu de l'extérieur, donnent l'impression d'être bien intégrés dans la société. Souvent, ils ne partagent même 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. Afin de pouvoir se procurer suffisamment tôt des informations pertinentes sur de telles personnes, les autorités sont de plus en plus tributaires de mesures de recherche particulières comme celles proposées dans le présent projet de loi. 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. Nous vivons de plus dans un environnement dans lequel la menace de violence intérieure est également susceptible de s'aggraver.

Dans d'autres domaines d'activités du SRC également, la partie adverse travaille souvent de manière conspirative, par ex. dans celui de l'espionnage, de la prolifération ou des attaques contre des infrastructures critiques. Avec une recherche d'informations limitée aux lieux publics, il est très difficile de collecter des renseignements sur les activités et les intentions de ces milieux.

Avec les moyens de recherche actuels, qui consistent pour l'essentiel dans l'exploitation de sources accessibles au public, demandes de renseignements et observations de faits dans des lieux publics (art. 14, LMSI), le Conseil fédéral estime que le SRC n'est plus que partiellement en mesure de remplir sa mission. De nombreux incidents permettant d'apprécier la menace ne surviennent pas dans des lieux publics et il est rare que des communications à caractère conspiratif puissent être constatées sur 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 prendre 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 mesures de recherche soumises à autorisation devront être prises chaque année, un cas pouvant toutefois en comporter plus d'une (par ex. la surveillance de plusieurs raccordements de télécommunication, la localisation d'un véhicule ainsi que la fouille d'une chambre d'hôtel concernant la même personne). Il s'agit ici de cas comportant un potentiel de menace particulier dans les domaines du terrorisme, de l'espionnage, de la prolifération et d'attaques contre des infrastructures critiques ou

pour la sauvegarde d'autres intérêts essentiels de la Suisse, pour lesquels les autres mesures de recherche ne suffisent pas à obtenir des informations élémentaires pour le maintien de la sûreté de la Suisse.

Les mesures de recherche soumises à autorisation englobent notamment (art. 22):

- la surveillance de la correspondance par poste et la correspondance par télécommunication d'une personne;
- la détermination de l'emplacement de personnes ou d'objets par la localisation d'un téléphone mobile utilisé par la personne ou à l'aide d'appareils de localisation spéciaux (en règle générales 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 y ont été transmises, ou de perturber, d'empêcher ou de ralentir l'accès à des informations lorsque des attaques contre des infrastructures critiques sont commises à partir de ces systèmes; et
- la fouille de locaux, de véhicules ou de conteneurs emportés par des personnes en vue de se procurer des informations qu'ils contiennent ou qu'ils ont transmises, ainsi que des objets. Les locaux, véhicules ou conteneurs peuvent être fouillés secrètement et à l'insu des personnes concernées.

Ces mesures doivent être autorisées par le Tribunal administratif fédéral, et après consultation préalable de la Délégation pour la sécurité, être avalisées par le chef du DDPS avant de pouvoir être mises en œuvre par le SRC. Lorsqu'un danger peut être lié à l'éventuel retard de l'exécution d'une mesure, le directeur du SRC peut ordonner qu'elle soit appliquée immédiatement. La demande d'autorisation correspondante doit alors être adressée au Tribunal administratif fédéral dans les 24 heures (art. 27, al. 2).

Il faut souligner que ces mesures de recherche soumises à autorisation ne concernent que les cas de menaces importantes en matière de politique de sécurité, sans rapport avec des enquêtes pénales. Lorsqu'une menace est liée à une présomption d'acte répréhensible, ce sont les autorités de poursuite pénale qui doivent être informées (voir art. 55). Une éventuelle procédure pénale et des mesures de surveillance ordonnées dans ce cadre sont prioritaires par rapport aux recherches d'informations prévues par la présente loi. Toutes les menaces importantes en lien avec la politique de sécurité ne sont toutefois pas pertinentes du point de vue pénal et souvent, les éléments de présomption ne suffisent pas à entamer une enquête pénale.

*Art. 22* Types de mesures de recherche soumises à autorisation

*L'al. 1, let. a,* permet au SRC d'ordonner la surveillance de la correspondance par poste et la correspondance par télécommunication. Contrairement aux 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 va les ordonner qu'à des fins préventives, l'objectif étant d'identifier suffisamment tôt les menaces pesant sur la sûreté intérieure ou extérieure de la Suisse. Si le SRC, au

cours de ses recherches, constate ou soupçonne des actes répréhensibles, il en informe les autorités de poursuite pénale.

A la différence de la mesure stipulée à la let. a, la disposition de la *let. b* concerne la surveillance d'un raccordement utilisé par des personnes différentes ou dont le propriétaire n'est pas identifié. Il peut par exemple s'agir d'une cabine téléphonique ou d'une carte prépayée anonyme. Dans ces cas, la surveillance sert généralement à identifier la personne qui utilise le raccordement et dont émane la menace.

D'un point de vue technique, la procédure utilisée par le SRC est la même que celle employée dans le cadre des procédures pénales de la Confédération et des cantons, tirée de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[18] (LSCPT). Quant à la surveillance à proprement parler, elle est effectuée par le SSCPT. Le SRC ne procède pas lui-même à ce type de surveillance.

Pour les mesures de surveillance figurant aux let. a à d, le SRC indemnise le SSCPT sur la base des tarifs habituels. L'art. 16 de la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT) règle ces indemnités, qui seront directement applicables au SRC (voir Abrogation et modification du droit en vigueur). Les mandats supplémentaires de surveillance auxquels le SSCPT doit s'attendre de la part du SRC ne représentent qu'un effort additionnel assez faible pour ce service par rapport aux prestations qu'il fournit aujourd'hui déjà pour les autorités de poursuite pénale (2011: 2699 mesures de surveillance en temps réel, 5758 mesures de surveillance rétroactives/données secondaires et 3918 renseignements d'ordre technique et administratif[19]).

La *let. c* permet une surveillance rétroactive des communications par poste ou télécommunication par un relevé des données secondaires ou des communications. Ce relevé est effectué par le SSCPT auprès du fournisseur de services de télécommunication et permet de constater à quelle heure un raccordement donné a été en liaison avec quels autres raccordements. Dans ces cas, le contenu des communications ne peut pas être déterminé.

Exemple: un officier traitant d'un service de renseignement étranger séjournant en Suisse essaie de recruter des informateurs et d'obtenir illégalement de leur part des informations issues de domaines sensibles. Le SRC sait que l'officier utilise des numéros de téléphones mobiles pour leur donner ses consignes. A cet effet, il a acquis quatre abonnements prépayés pour des téléphones mobiles en Suisse. Afin de savoir avec quelles personnes il est en contact par le biais de ces téléphones, le SRC doit pouvoir disposer des relevés des communications ou des données secondaires de ces raccordements.

La *let. d* se fonde sur la législation sur la surveillance de la correspondance par télécommunication qui prévoit déjà, pour les organes de poursuite pénale, la possibilité de localiser des téléphones mobiles en surveillant la position et la direction d'émission de l'antenne avec laquelle l'appareil mobile de la personne surveillée est momentanément relié (voir à cet égard l'art. 16, let. b, de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[20]). L'emplacement approximatif d'une téléphone mobile, ainsi que ses déplacements,

[18] SR **780.1**
[19] Selon une statistique publiée sur Internet, voir https://www.li.admin.ch/de/themes/stats.html
[20] RS **780.11**

peuvent ainsi être déterminés sans qu'une intervention sur l'appareil ou le placement d'un capteur auprès de la personne soient nécessaires. Comme un accès à des données de télécommunication ainsi que la collaboration de fournisseurs de services de télécommunication sont requis à cet effet, cette mesure doit être soumise à une procédure d'autorisation.

La *let. e* règle l'engagement de moyens techniques, tels que des GPS, qui permettent de déterminer la position et les mouvements d'une personne, d'un véhicule ou de tout autre objet mobile. Les signaux transmis par ces instruments permettent de localiser sur une carte 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 techniques sont entre autres destinés à soutenir des mesures d'observation (de manière analogue aux engagements de la police, où l'utilisation de tels moyens fait depuis des années partie de la pratique), notamment lors d'une perte du contact avec l'objectif, les remplacer en partie lorsqu'une observation directe n'est pas nécessaire ou de les préparer en procédant au relevé des habitudes d'une personne à surveiller, ce qui permet ensuite aux équipes de mieux cibler leurs observations.

Le choix des moyens à engager reste ouvert afin de ne pas exclure les futurs développements techniques (par ex. la technique RFID).

La *let. f* permet notamment d'enregistrer les conversations de personnes surveillées dans des locaux privés ou dans des lieux qui ne sont pas librement accessibles, ainsi que de procéder à une surveillance par l'image (technique vidéo). Selon le droit en vigueur, une telle mesure n'est autorisée que dans le cas d'une procédure pénale. Lorsqu'il y a un soupçon pressant de comportement menaçant pour l'Etat de la part d'un groupe donné de personnes, le SRC doit être en mesure d'étendre ses recherches dans des locaux privés également. Les principes généraux pour ordonner une telle mesure sont aussi applicables dans ces cas (art. 23).

L'exemple ci-après illustre une mise en œuvre possible de mesures techniques de surveillance: en présence de petites cellules terroristes (par ex. la cellule tricéphale du Nationalsozialistischer Untergrund [Mouvement clandestin national-socialiste] en Allemagne), les contacts n'ont lieu que dans la clandestinité, sous forme conspirative. En public, ces personnes n'expriment jamais leurs vraies intentions et opinions. Elles n'ont aucun contact avec des externes auxquels elles les confieraient. Dans de tels cercles, il n'est pas possible non plus d'engager des informateurs, puisque les cellules en question n'autorisent aucun accès depuis l'extérieur. Seuls les moyens techniques de surveillance évoqués permettent d'obtenir les informations dont le SRC a besoin pour empêcher que la sûreté soit mise en danger, par exemple par des attentats terroristes. Lorsque le seuil de présomption d'un acte répréhensible est dépassé, le SRC en informe les autorités de poursuite pénale (art. 55).

La *let. g* prend en compte le transfert de plus en plus important de déclarations et d'actions menaçant la sécurité sur des sites sécurisés de l'Internet. Au vu des menaces croissantes qu'elles entraînent pour la sécurité de la Suisse, le SRC a besoin de nouveaux moyens adéquats pour pouvoir, dans le cadre de ses tâches de prévention, explorer des réseaux informatiques et évaluer ces menaces. Il s'agit, 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 contre des infrastructures critiques.

Afin de pouvoir détecter et évaluer des développements qui présentent un danger pour la sûreté de la Suisse, le SRC doit, le cas échéant, pouvoir s'introduire dans des réseaux informatiques particulièrement bien protégés. Les informations ainsi obtenues peuvent par exemple contribuer à identifier et à empêcher des activités planifiées dans le domaine du terrorisme.

Les attaques visant à perturber des infrastructures critiques peuvent menacer gravement la sûreté intérieure et extérieure de la Suisse et comportent un potentiel de dommages très important: par exemple des attaques électroniques visant l'approvisionnement en énergie (centrales nucléaires), les transports (aériens, ferroviaires et 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 un dommage intervenu, aussi partiellement, lors d'une telle attaque. Le principe de subsidiarité est respecté dans la mesure où le SRC ne devient actif qu'en dernier recours. Dans ce contexte, la protection préventive du pays (par ex. d'une contamination radioactive) doit être prioritaire. A souligner que les mesures indiquées sous ch. 2 contre des systèmes en Suisse sont toujours soumises à autorisation, c'est-à-dire qu'elle doivent être approuvées au niveau judiciaire (approbation par le Tribunal administratif fédéral) et au niveau politique (aval du chef du DDPS).

Au DFJP, c'est le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) qui est chargé des aspects de poursuites pénales concernant des activités criminelles sur Internet.

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

*L'al. 2* stipule que les mesures mentionnées ci-devant peuvent être exécutées de manière secrète 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'Etat de droit. La mesure effectuée doit également être communiquée ultérieurement à la personne concernée (art. 29) en lui donnant la possibilité de déposer un recours contre la mesure ordonnée (art. 71).

*Art. 23* Principe

*L'al. 1* fixe que l'engagement de mesures de recherche soumises à autorisation doit répondre à l'une ou l'autre des deux conditions préalables, à savoir soit l'existence d'une menace concrète pesant sur la sûreté intérieure ou extérieure de la Suisse, à l'exception de l'extrémisme violent, soit la sauvegarde d'autres intérêts essentiels de la Suisse sur la base d'un arrêté fédéral. Dans son arrêté, le Conseil fédéral détermine aussi si des mesures soumises à autorisation peuvent être mises en œuvre Dans tous les cas, la procédure d'autorisation selon l'art. 25 et suivants doit être appliquée, c'est-à-dire que l'arrêté du Conseil fédéral ne remplace pas cette procédure, mais qu'il 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 de la restriction définie par la loi.

En présence d'intérêts essentiels et d'une menace concrète pour la sûreté intérieure ou extérieure de la Suisse selon l'art. 17, al. 2, let. a à d (cumulatives), 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; et
- la recherche d'informations effectuée jusque-là est restée vaine ou serait vouée à l'échec ou demanderait des efforts disproportionnés sans avoir recours à ladite mesure.

Il s'agit d'exigences supplémentaires restrictives au principe constitutionnel de la proportionnalité, qui s'inspirent de celles stipulées dans le droit de procédure pénale (voir l'art. 269, al. 1, du Code de procédure pénale[21] du 5 octobre 2007 (CPP)).

Les services tiers chargés selon l'al. 3 d'exécuter ces mesures sont, entre autres, le SSCPT du DFJP pour la surveillance des télécommunications en lien avec ces mesures ou les organes de sécurité des cantons pour l'engagement d'appareils techniques de surveillance ou des fouilles.

*Art. 24* Mesures ordonnées à l'encontre de tiers

Il se peut qu'une personne, pour laquelle les conditions préalables stipulées à l'art. 22, al. 1, soient données pour ordonner 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 réceptionner des informations. Cela peut se produire à l'insu de cette personne. Dans de tels cas, le SRC doit avoir la possibilité de faire surveiller les adresses postales et les raccordements de télécommunication du tiers en question, d'accéder à ses systèmes ou réseaux informatiques 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 faire se peut et elle doit être informée de cette mesure une fois que celle-ci a pris fin (art. 29).

N'est pas autorisée la surveillance d'un tiers qui bénéficie du droit de refuser de témoigner selon les art. 171 à 173 CPP, par exemple des ecclésiastiques, des avocats, des médecins et leurs auxiliaires ou des professionnels des médias. Le projet de loi reprend ici les règles du CPP.

*Art. 25* Procédure d'autorisation

Le mode d'autorisation proposé ici comprend deux phases: dans un premier temps, le SRC doit demander l'approbation d'une instance judiciaire, en l'occurrence le Tribunal administratif fédéral. 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 tribunal en question a approuvé la mesure sur le plan juridique (art. 26) et que le chef de DDPS a au préalable consulté la Délégation du Conseil fédéral pour la sécurité.

[21] **RS 312.0**

Concrètement, la procédure est la suivante:

- Le SRC demande au Tribunal administratif fédéral l'autorisation d'engager une mesure de recherche soumise à autorisation
- Le président de la cour compétente du Tribunal administratif fédéral examine la demande et décide d'approuver ou de rejeter la mesure sollicitée, voire de faire compléter le dossier.
- En cas d'approbation de la mesure, il incombe ensuite au chef du DDPS de l'autoriser ou non.
- Le SRC peut alors exécuter 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 et extérieure de la Suisse, l'exposé de la proportionnalité de la mesure, la désignation de la personne à surveiller, pour autant qu'elle soit déjà identifiée, les moyens à déployer ainsi que les éventuelles mesures de protection visant à préserver les droits de la personne surveillée ou de tiers.

Par analogie avec l'art. 274, al. 5, CPP, l'approbation est octroyée pour une durée maximale de trois mois et peut à chaque fois être prolongée de trois mois au plus. Si une prolongation s'avère nécessaire, le SRC dépose une demande en ce sens tout en prenant soin de fournir les mêmes indications que celles exigées pour l'approbation initiale (al. 5).

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 de traitement particulières vis-à-vis des autorités de poursuites pénales pour éviter qu'elles ne soient utilisées dans des procédures pénales au cours desquelles aucune mesure d'enquête comparable n'aurait été autorisée (voir à ce sujet l'art. 55, al. 3 et 4).

*Art. 26* Aval du chef du DDPS

Le présent article règle l'autorisation par le chef du DDPS, après que ce dernier ait consulté la Délégation du Conseil fédéral pour la sécurité, d'une mesure de recherche autorisée par un juge. 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 seulement envisagée sous l'angle juridique mais également politique. La conduite de la politique de sécurité peut, pour des raisons politiques, refuser de donner son aval pour une telle mesure.

Il faut toutefois souligner que le chef du DDPS ne peut autoriser que des mesures préalablement approuvées sur le plan judiciaire. Il ne peut donc pas autoriser une mesure n'ayant pas reçu l'approbation nécessaire.

*Art. 27* Procédure en cas d'urgence

Au contraire des autorités de poursuites pénales, 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 d'abord obtenir l'approbation du Tribunal administratif fédéral et l'aval du chef du DDPS, ce dernier ayant préalablement consulté la Délégation du Conseil fédéral pour la sécurité, avant d'ordonner des mesures selon les art. 22 et suivants.

En cas de danger imminent, l'art. 27 prévoit la possibilité pour le SRC d'engager une mesure immédiatement. Un tel cas n'intervient que si 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 importante personne 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, implantation d'un appareil de localisation) peuvent selon les circonstances 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 l'exécution d'une mesure ordonnée dans l'urgence:

- il peut mettre un terme immédiat à l'exécution de la mesure dès qu'il en a été informé par le SRC, ou
- il peut décider de ne pas l'autoriser après avoir été informé de l'approbation octroyée par le Tribunal administratif fédéral (voir à cet égard l'art. 29); une telle façon de faire est imaginable lorsqu'il a pris connaissance du contexte global de l'exécution sur la base de la demande écrite, alors que la première information est de nature sommaire.

*Art. 28* Fin de la mesure de recherche

Les règles qui s'appliquent lorsqu'un terme est mis 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, même si elle devait encore être approuvée.

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

*Art. 29* Obligation d'informer les personnes surveillées

L'obligation d'informer à posteriori les personnes visées par des mesures soumises à autorisation découle de la protection de la vie privée d'une personne ainsi que du respect de la sphère privée. Cette garantie s'appuie sur l'art. 8 CEDH et l'art. 13 Cst.

Lorsqu'une opération, c'est-à-dire une procédure concertée de plusieurs mesures de recherche éventuelles relatives à des faits donnés, est terminée, le SRC doit, en principe dans un délai d'un mois, informer les personnes visées par la mesure et les tiers dont les raccordements ont le cas échéant été placés sous surveillance de la

recherche d'information, conformément à l'*al 1*. La loi ne se rattache pas ici à la mesure individuelle, car d'autres mesures de recherche autorisées sont par exemple encore en cours et qu'elles pourraient être mises en péril par la communication d'une mesure déjà terminée (exemple typique: l'acquisition des données secondaires d'anciennes communications téléphoniques selon l'art. 22, 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 aussi qu'au terme de toutes les mesures que l'on peut déterminer si une notification est possible ou si une exception est nécessaire au sens de l'al. 2 (par ex. parce que le cas est transmis aux autorités de poursuites pénales et qu'une procédure juridique est ainsi engagée).

*L'al. 2, let. a*, s'inspire de la jurisprudence de la Cour européenne des droits de l'homme, qui, dans l'arrêt Klass contre la République fédérale d'Allemagne, du 6 septembre 1978, a constaté qu'une notification ultérieure pouvait remettre en question l'objectif à long terme d'une surveillance et qu'il devait être 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'article 8, al.2*[22] *(art. 8-2), 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* s'appuie sur les intérêts publics prépondérants pour préserver la sûreté intérieure ou extérieure, qui sont également respectés par la CEDH. L'objectif ici 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. C'est ainsi qu'un combattant ou commandant Taliban dont le téléphone mobile a été placé sur écoute dans le cadre d'une affaire d'enlèvement ne sera pas informé ultérieurement de la mise sur écoute, et ce pour des raisons évidentes.

*La let. c* reprend quant à elle 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 ou à la dérogation de la communication ultérieure est la même que pour l'injonction de la mesure de recherche soumise à autorisation proprement dite: approbation par le Tribunal administratif fédéral puis autorisation par le chef du DDPS (art. 26).

[22] CEDH

**Section 5: Collaboration et protection des sources**

*Art. 30* Collaboration et mandat en matière de recherche d'informations

Aujourd'hui, les acteurs étatiques et non étatiques qui sont actifs 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 du transfert illicite de technologies le sont à un niveau global et ne respectent ni les frontières ni les conventions interétatiques. Ces acteurs se servent par exemple de la zone de Schengen, libre de visa, afin de se rencontrer dans d'autres pays à des fins de conspiration et d'échapper ainsi aux mesures de surveillance dont ils font l'objet dans leurs propres 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*, est toujours plus importante, avant tout dans les domaines de la transmission des informations, des observations transfrontalières, des opérations communes de recherche et des mesures techniques de surveillance, qui sont exécutées conformément au droit suisse en vigueur. Le SRC ne peut notamment pas 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 privés ayant 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 privés, le SRC ne pourrait que très difficilement acquérir ladite information, 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 l'acquisition devient probable.

Peuvent par exemple faire partie des mesures de recherche stipulées à l'*al. 2* des appareils techniques de surveillance d'une grande complexité qui ne peuvent être exploités que par des entreprises privées spécialisées. Il est également imaginable de faire appel à des spécialistes en informatique privés pour des réseaux de données particulièrement 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 les surveiller dans l'accomplissement de ce dernier aussi étroitement que ses propres collaborateurs.

*Art. 31* 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 en la discrétion du SRC en serait diminuée et la recherche d'informations très fortement pénalisée.

Le droit actuel ne contient qu'une réglementation très rudimentaire relative à la protection des sources dans l'art. 7 LFRC et délègue par ailleurs la protection au Conseil fédéral. Ce dernier est d'avis que la codification complète du service de renseignement doit aussi contenir une réglementation plus détaillée sur la protection des sources. On veut ainsi également éviter les incertitudes entre les ordonnances spécifiques d'exécution et l'éventuel droit commun contradictoire d'autres textes de loi.

*L'al. 1* définit le principe de la protection des sources ainsi que de la légitimité particulière des personnes qui recherchent des informations à l'étranger à être protégées, laquelle figurait déjà dans l'art. 7 LFRC. Cet alinéa englobe également les relations avec des services partenaires étrangers, qu'il s'agit également de protéger, sans quoi la Suisse serait considérée comme un partenaire non fiable. L'absence d'une telle protection pourrait avoir de graves conséquences pour la crédibilité du SRC comme partenaire de coopération. Les personnes condamnées ou recherchées pour des crimes contre l'humanité ne mériteront en revanche aucune protection.

L'*al. 2* limite la protection des informateurs (art. 13) domiciliés en Suisse face auxautorités de poursuites pénales. Ces personnes n'obtiennent aucune protection si elles sont elles-mêmes 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 généralement acceptée de la notion d'infraction grave dans le droit pénal et le droit de procédure pénale. Il n'existe pas non plus de critères globalement valables pour les infractions graves. La qualification d'une infraction dépend bien plus 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 [23] 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* explique en outre quels sont les critères qui doivent encore être utilisés pour la protection des sources. A cet égard, c'est toujours le maintien de la source à des fins d'acquisition d'informations qui prime. Conformément à la réglementation générale sur la promulgation du droit d'application, le Conseil fédéral règle les spécificités dans une ordonnance.

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, laquelle peut acquérir les connaissances techniques correspondantes en matière de renseignement. Il propose par conséquent dans l'*al. 4* d'établir le Tribunal administratif fédéral comme instance de décision pour la protection des sources.

**Section 6: Recherche d'informations sur des événements se produisant à l'étranger**

[23] RS **364.3**

*Art. 32* Dispositions générales

*Remarques liminaires*

La recherche d'informations relatives à des événements se produisant à l'étranger se fonde aujourd'hui sur la réglementation générale, telle qu'elle est formulée à l'art. 1, let. a, LFRC:

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

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'art. 99, al. 1, LAAM. Elle a été formulée de manière très générale dans la LFRC, puisque cette dernière voulait uniquement résumer les bases juridiques existantes relatives au service de renseignement civil, sans mettre en place de nouvelles barrières au niveau du contenu. La LFRC a donc repris la réglementation de la LAAM, qui souhaitait donner une grande marge de manœuvre au service de renseignement en ce qui concerne la recherche d'informations à l'étranger et ne voulait pas dévoiler à l'étranger les méthodes et possibilités en matière de recherche d'informations utilisées par l'ancien Service de renseignement stratégique (SRS).

L'art. 16 OSRC décrit plus précisément les méthodes aujourd'hui autorisées à l'étranger pour rechercher des informations sur le plan du renseignement.

Si la recherche d'informations sur l'étranger se fait en Suisse, ce sont en principe les mêmes règles qui s'appliquent que pour la recherche d'informations relatives à des événements se produisant 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 les mesures de recherche à l'étranger sous sa propre responsabilité, y compris celles qui seraient soumises à autorisation en Suisse (art. 22 ss).

La réglementation différente de la recherche d'informations en Suisse et à l'étranger correspond à une pratique valable pour la plupart des services de renseignement dans le monde et qui 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 sur le plan international. 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'Etat visé comme une atteinte illégale à sa souveraineté de la part des autorités judiciaires et politiques suisses. Il faut par ailleurs également tenir compte du fait que

- la substance des droits fondamentaux doit également être respectée lors de la recherche d'informations à l'étranger (al. 3);
- les activités de recherche relatives à des événements se produisant à l'étranger doivent être documentées de près à l'intention des organes de surveillance et de contrôle (al. 4);
- la recherche d'informations à l'étranger est soumise au contrôle du DDPS, du Conseil fédéral et enfin de la DélCdG (voir à cet égard les art. 66 ss).

L'*al. 1* statue le principe selon lequel les activités de recherche à l'étranger doivent se dérouler en secret. Ce principe est nécessaire car si tel n'était le cas, elles pourraient être empêchées par les Etats ou les acteurs concernés, ce qui pourrait mettre en péril aussi bien les collaborateurs que les sources du SRC.

L'*al. 2* permet à la recherche d'informations sur l'étranger d'être également active en Suisse (par ex. en rencontrant des informateurs) mais veille à ce que le SRC respecte les mêmes règles que pour la recherche d'informations en Suisse. Ce principe s'applique en particulier à l'engagement éventuel de mesures de recherche soumises à autorisation (section 4). L'intrusion dans des systèmes et réseaux informatiques en est exclue (art. 22, al. 1, let. g), dans la mesure où ces systèmes et réseaux se trouvent à l'étranger. Dans un tel cas, une obligation d'autorisation serait incompréhensible, puisque la même attaque cybernétique n'aurait pas besoin d'autorisation si elle était exécutée depuis un emplacement situé de l'autre côté de la frontière.

Le SRC engage 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. 22 et suivants. La raison pour laquelle la solution appliquée pour l'engagement des mesures de recherche diffère de celle utilisée pour la recherche en Suisse réside non seulement dans les raisons susmentionnées mais 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 afin de pouvoir remplir leurs missions.

Le Conseil fédéral propose dès lors de régler les mesures de recherche secrètes autorisées à l'étranger dans une liste exhaustive sans autorisation particulière. Et ceci du fait qu'en règle générale, 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 engageant leur responsabilité. Dans une telle situation, une procédure ordinaire d'autorisation (qui constituerait de toute manière un cas unique à l'échelon international) ne serait pas possible. A cela vient s'ajouter la problématique qu'une des plus hautes juridictions de Suisse devrait au préalable déclarer licites des mesures que les pays dans lesquels elles sont effectuées considèrent souvent comme étant répréhensibles.

Cela ne signifie toutefois pas l'abandon d'un contrôle efficace. Au contraire: *l'al. 4* oblige le SRC de documenter l'ensemble de ses recherches d'informations sur les événements se produisant à l'étranger à l'intention de la surveillance politique du SRC par le Conseil fédéral, le Parlement (Commission de gestion, resp. DélCdG) et le DDPS (Surveillance des services de renseignement).

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. Le Conseil fédéral propose donc dans l'*al. 5* de les soumettre à l'assurance militaire.

Les mesures de protection prévues à *l'al. 6* peuvent prendre la forme d'équipements techniques, mais aussi de couvertures et d'identités d'emprunt ou encore d'un appui opérationnel, par exemple l'engagement de contre-observations visant à identifier rapidement les menaces existantes dans le contexte d'une intervention.

*Art. 33* Exploration radio

Avec l'art. 4*a* de la LFRC, le Parlement a 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 ressortissant au service de renseignement. Cette disposition n'est entrée en vigueur que le 1er novembre 2012, après l'adaptation de l'ordonnance sur la guerre électronique. Le Conseil fédéral l'a donc reprise telle quelle ou presque dans la loi sur le renseignement, avec quelques légères adaptations à l'usage ainsi qu'au champ d'application de la LRens. C'est ainsi que la sauvegarde d'autres intérêts essentiels de la Suisse sur ordre direct du Conseil fédéral (voir l'art. 1, al. 3, et l'art. 62) a été reprise dans les conditions pouvant présider à l'engagement de l'exploration radio, dans l'al. 2.

L'exploration radio est axée sur l'étranger, ce qui veut dire qu'elle n'a le droit d'opérer 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 veille à ce que les émissions radio ne puissent être exploitées que si leur contenu a un lien avec l'étranger. A cette occasion, il est aussi possible que des informations sur des personnes en Suisse soient récoltées, notamment lorsque le partenaire de communication d'une personne ou d'un équipement étranger faisant l'objet d'une exploration utilise un raccordement de télécommunications suisse. Ces informations, le COE ne peut les transmettre au SRC qu'après les avoir rendues anonymes, pour autant qu'elles n'indiquent pas de menace concrète pour la sûreté intérieure (al. 5). La LFRC renvoie ici au traitement ultérieur selon les réglementations de la LMSI. Dans la LRens, les menaces en question sont celles qui figurent à l'art. 4, al. 1, let. a.

L'exploration radio est aujourd'hui déjà contrôlée par un organe autonome. Ici aussi, le Conseil fédéral reprend dans l'art. 66 LRens la réglementation correspondante de la LFRC (art. 4*b*), de manière inchangée ou presque.

La LRens reprend ainsi intégralement la réglementation et la pratique juridiques 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. 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 participation du professeur Biaggini.

**Section 7: Exploration du réseau câblé**

*Art. 34* Dispositions générales

Outre l'exploration radio déjà pratiquée aujourd'hui, en Suisse également, l'exploration du réseau câblé gagne en importance à l'échelle internationale. Le transfert des télécommunications de moyens sans câble (radio) vers des réseaux reliés par des

conduites (désignés comme « câble » par souci d'intelligibilité) s'est intensifié au cours de ces dernières années avec l'élargissement des réseaux très performants de fibre optique. Simultanément, les possibilités d'obtenir des résultats à partir de l'exploration radio diminuent quelque peu. L'avant-projet se fonde dès lors en partie sur une législation similaire édictée par la Suède en 2008 (loi 2008:717 sur l'exploration des signaux au sein du Service de renseignement militaire, qui possède en Suède la fonction du Service de renseignement stratégique) et qui règle également l'exploration du réseau câblé. Il ne sera possible en Suisse de procéder à des examens techniques plus approfondis et à des tests avec l'exploration du réseau câblé que lorsque les bases juridiques nécessaires à cet effet seront entrées en vigueur.

A l'instar de l'exploration radio, l'exploration du réseau câblé sert à rechercher des informations à l'étranger et n'est dès lors pas conçue comme une mesure de recherche soumise à autorisation. Si des objectifs d'exploration similaires ayant trait à la Suisse doivent être atteints, 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 télécommunications, à qui il faut donner un ordre juridiquement valable pour qu'ils puissent transmettre au COE les flux de données correspondants. Etant donné qu'une procédure de recours contradictoire 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. 25). Le traitement des données se fait toutefois différemment en ce sens qu'il n'intervient pas dans des systèmes séparés, mais dans le fichier de données résiduelles et dans IASA SRC (art. 42 ss), comme pour les résultats issus de l'exploration radio.

Dans le cadre de l'exploration du réseau câblé, certains flux de données sont interceptés sur des câbles de télécommunication internationaux et, comme pour l'exploration radio, sont examinés, triés et exploités selon leur contenu. Au contraire de la surveillance des télécommunications en Suisse comme mesure de recherche soumise à autorisation, l'exploration du réseau câblé est un instrument de l'exploration à l'étranger et n'est pas prévue pour enregistrer l'ensemble du trafic de télécommunications de certains raccordements. Sur le plan technique, cela n'est pas possible de la même manière, puisque les objets cibles se trouvent à l'étranger.

La Suisse n'a jusqu'à présent aucune expérience avec cet instrument d'exploration, puisqu'elle ne possède aucune base juridique à cet effet.

Comme pour l'exploration radio, le service chargé de l'exécution d'après l'*al. 1* est le COE, qui dispose des compétences techniques ainsi que des équipements nécessaires à son exécution. Afin de protéger les droits fondamentaux des personnes dont les données de communication sont enregistrées dans le cadre de l'exploration du réseau câblé mais qui ne répondent pas aux critères de recherche dictés par le mandat du SRC, il est indispensable que le triage des données soit effectué non pas par le SRC mais par un organe tiers. Comme c'est le cas 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 quant à une mise en danger de la sûreté intérieure ou extérieure. A quelques détails près, ces critères ainsi que les manières de procéder correspondent à la pratique en vigueur pour l'exploration radio.

L'*al. 2* veille à ce qu'aucune communication purement suisse ne soit enregistrée. Lorsque cela n'est techniquement pas possible (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 immédiatement être détruites, dès que leur origine suisse et leur adresse cible ont été identifiées. Cette contrainte s'applique aussi bien au COE qu'au SRC.

L'*al. 3* définit les prescriptions applicables aux termes de recherche que le SRC établit pour le mandat. Ceux-ci doivent être formulés de manière aussi précise que possible, afin que les atteintes à la sphère privée des personnes concernées qui sont causées par l'enregistrement des données soient aussi faibles que possible. En d'autres termes, il est par exemple plus efficace et précautionneux 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 trivial tel que « Al-Qaïda » ou « attentat à l'explosif ». Il existe à cet effet déjà une pratique éprouvée ainsi que juridiquement correcte et contrôlée issue de l'exploration radio.

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

*Art. 35 et 36* Obligation d'obtenir une autorisation et procédure d'autorisation

Par analogie avec les mesures de recherche soumises à autorisation, ces articles règlent l'approbation des mandats d'exploration du réseau câblé. Etant 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.

Le mandat stipulé à l'*art. 36, al. 1*, englobe également les catégories de termes de recherche d'après lesquelles les données doivent être sélectionnées au profit du SRC. Les expériences faites avec l'exploitation de 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 pour l'exploration du réseau câblé de travailler également avec des catégories de termes de recherche, afin qu'une nouvelle approbation ne doive pas être obtenue pour chaque affinement. 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 personnes ne peuvent être identifiées nommément qu'en cours d'exploration. Les indications se rapportant aux éléments d'adressage relevant de la technique de télécommunications (par ex. numéros de téléphone), les adresses ou les désignations de dossiers et de projets sont par exemple 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 à chaque fois être autorisées que pour une durée de trois mois, l'exploration du réseau câblé doit pouvoir être autorisée pour une durée de six mois lors du premier mandat, conformément à ce qui est stipulé dans l'*al. 3*. Une telle mesure paraît judicieuse, puisque l'enregistrement de la saisie ainsi que la formation et l'intégration du triage dans un mandat nécessite par exemple plus de temps que l'envoi intégral au SRC de toutes les télécommunications surveillées selon l'art. 22, al. 1, let a. S'agissant des prolongations, c'est ensuite le même délai qui s'applique que pour les mesures de recherche soumises à autorisation, soit trois mois.

*Art. 37* Mise en œuvre de l'exploration du réseau câblé

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 de la part des fournisseurs de télécommunications. Les fournisseurs concernés doivent être déterminés au cas par cas en fonction de l'identification des voies de transit à travers la Suisse.

La procédure ultérieure ainsi que les critères dictant le choix des données devant être transmises au SRC se fondent essentiellement sur les réglementations 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 sont les données qu'il dépose dans ses systèmes d'information conformément aux bases légales pour y être traitées (voir le chap. 4). Comme c'était le cas jusqu'à présent, le COE peut aussi assortir les données transmises d'explications techniques ou de fond, de résumés ou de traductions au profit du SRC.

*Art. 38* Obligations des exploitants de réseaux câbles et des opérateurs de télécommunications

Etant donné, comme il a été expliqué plus haut, que l'exploration du réseau câblé ne peut être effectuée qu'avec la participation des fournisseurs de prestations de service de télécommunication et des exploitants de réseaux tributaires d'éléments conducteurs, l'art. 38 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 sont toutefois soumis à cette obligation. Les renseignements techniques sont notamment aussi nécessaires afin de pouvoir 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 approuvé et autorisé. En règle générale, les questions techniques devront être clarifiées entre le COE et les fournisseurs. Afin de pouvoir 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.

Une participation du SSCPT, rattaché au DFJP, n'est pas nécessaire à cet égard, puisque l'exploration du réseau câblé n'est pas un type de surveillance conforme à la LSCPT qui est proposé par ce dernier. Les modalités techniques doivent bien plus être clarifiées au cas par cas directement entre le SRC, le COE et les exploitants.

A 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 sont les flux de données pertinents sur le plan du renseignement qui transitent aujourd'hui et transiteront demain à travers la Suisse. Ces informations ne pourront être recensées que lorsque les bases juridiques respectives seront entrées en vigueur.

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 deux entités. Ces postes seront demandés dans les planifications ordinaires du personnel.

## Chapitre 4: Traitement des données et archivage

### Section 1: Principes et traitement par les cantons

*Remarques liminaires*

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

Les attentats terroristes, activités d'espionnage, actions extrémistes violentes, etc. sont typiquement préparés en secret et le restent aussi longtemps que possible. Comme ils peuvent toutefois conduire à des dommages considérables, leur détection précoce et leur prévention 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 quant à la préparation ou à l'existence d'une infraction. Ces menaces, le SRC doit avant tout 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 à ce que cette distinction ne puisse plus jouer de rôle déterminant lors du traitement des données par le SRC.

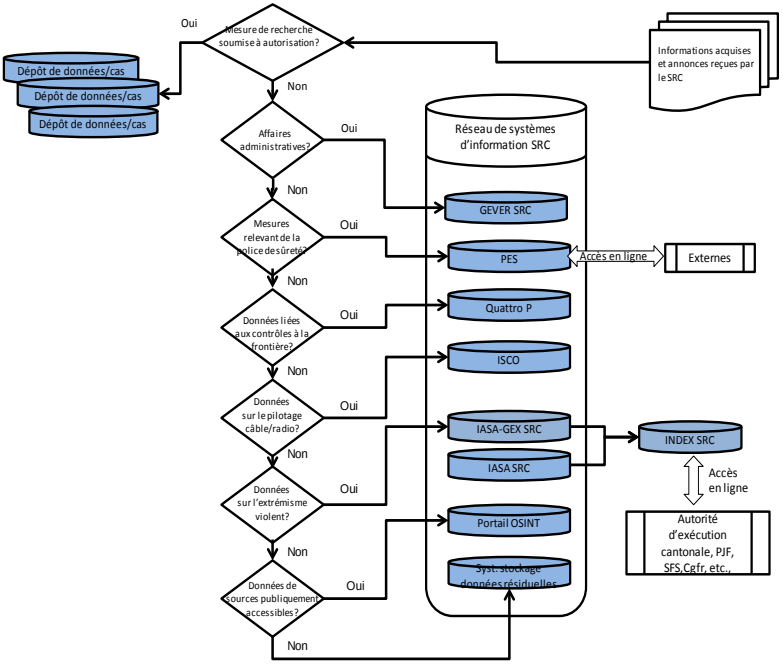
Le service de renseignement fusionné est bien plus tributaire d'une réglementation uniforme de la saisie, de la conservation et de l'exploitation des données, afin que le gain en efficacité visé à travers la fusion et l'exploitation intégrale exigée des données relevant du renseignement puissent se réaliser. A cet égard, il y a lieu de tenir adéquatement compte des points qui ont fait leur preuve dans la longue pratique avec les bases légales actuelles que sont la LMSI et la LFRC.

Le présent projet de loi prévoit que les informations recherchées par le SRC ou qui lui sont communiquées soient saisies dans des systèmes d'information intégrés selon la thématique, la source et la sensibilité des données. Le SRC ne peut pas collecter et conserver des données au hasard. Pour ce faire, il faut toujours qu'il y ait un lien suffisant avec les tâches qui lui sont dévolues par la présente loi. Il faut de plus tenir compte du respect des restrictions de traitement des données relatives à l'exercice des droits politiques (art. 3, al. 5 à 8). Enfin, il faut veiller à ce que les données soient vérifiées avant leur enregistrement dans les systèmes d'information afin de s'assurer qu'elles soient pertinentes et exactes. Cette vérification intervient également avant que des données personnelles n'aient un impact vers l'extérieur, c'est-à-dire qu'elles soient utilisées dans le cadre d'un produit du SRC (par ex. rapport d'analyse, annonce à un service partenaire, appréciation de la situation).

Les données que le SRC reçoit par le biais d'une mesure de recherche soumise à autorisation ou faisant suite à des contrôles à la frontière bénéficient d'un traitement spécial 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 du droit lié à la protection des

données. Les servitudes 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 rapprochées). Les servitudes s'appliquant aux annonces issues de sources publiquement accessibles sont en revanche moins strictes (rythme de vérification plus lent, durée de conservation allongée, cercle plus large de personnes bénéficiant d'une autorisation d'accès), puisque de telles données pourraient en règle générale également être recoupées à partir des sources d'origine, même si elles sont structurées différemment et que leur disponibilité est moins garantie.




*Art. 39* Principes

Les principes prévus à l'art. 39 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 des données personnelles sont enregistrées. Les systèmes peuvent recevoir des données sous la forme de textes, de supports sonores, d'images ou d'autres formats appropriés.

Pour s'acquitter de ses tâches, le SRC reste tributaire du traitement de données personnelles particulièrement dignes d'être protégées, telles que l'appartenance religieuse pour les terroristes à motivation fondamentaliste, l'exécution de peines d'emprisonnement par des condamnés ou l'état de santé de figures d'identification ou de politiciens étrangers. Il établit et traite des profils de personnalité, par exemple dans le but d'évaluer la menace constituée par des extrémistes violents agissant seuls

ou en groupes. L'*al. 2* crée la base juridique formelle nécessaire à ces traitements de données.

Contrairement aux servitudes habituelles en matière de protection des données, le SRC doit aussi pouvoir conserver les données reconnues comme inexactes et exploitées comme telles, conformément à l'*al. 2*. En ce qui concerne l'appréciation d'informations relevant du renseignement, il s'agit également toujours d'identifier la désinformation et les fausses informations. De telles informations permettent de déterminer les intentions des producteurs ainsi que des fournisseurs d'informations. Une fois reconnue comme telle, une désinformation ou une fausse information doit rester disponible à l'avenir aussi, afin de ne pas provoquer d'erreurs d'interprétation ultérieures. De même, il doit être possible d'accéder aux fausses informations identifiées dans le cadre de la collaboration internationale, afin d'apprécier correctement le colportage ultérieur 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 partenaire.

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. Son travail d'analyse, il ne pourra l'exécuter et l'étayer dans le système d'information IASA SRC prévu à cet effet que lorsqu'il aura 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 complète est souvent nécessaire pour l'établissement d'un produit donné, l'annonce en question doit systématiquement rester dans le système original, où elle est à la disposition d'autres utilisateurs et où on vérifie régulièrement qu'elle soit pertinente et exacte (voir à cet égard l'art. 40, Contrôle de qualité). Les données peuvent ainsi être copiées d'un système à l'autre et sont soumises aux consignes respectives des différents systèmes d'information.

La mise en réseau des données dans les systèmes, déjà pratiquée aujourd'hui 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. C'est ainsi qu'il est par exemple possible de saisir et représenter efficacement les relations entre les personnes et avec des événements. L'*al. 5* crée donc la base juridique expresse pour de telles mises en réseau et l'usage de programmes automatisés de recherche et d'exploitation.

*Art. 40* Contrôle de qualité

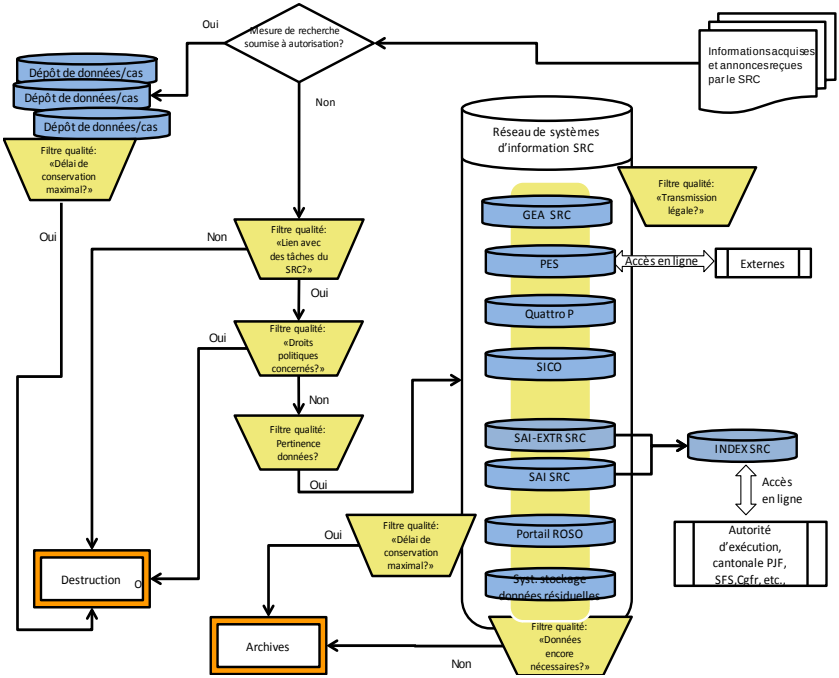
Divers rapports d'organes de surveillance ont démontré à quel point un contrôle de qualité fiable et exploitable est important pour la qualité des données du SRC. La mise en place d'un organe de contrôle de qualité interne au SRC a fait ses preuves et doit à présent également être ancré dans la loi. 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 dans le domaine de l'extrémisme violent (al. 5, let. a) ainsi que 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 ou du terrorisme il s'agit le plus souvent d'observer des développements sur plusieurs années, il faut s'attendre à des cycles de qualité des données beaucoup plus courts dans le domaine de l'extrémisme violent. Le risque d'avoir des données dans le système qui sont dans l'intervalle devenues inutiles doit ici être considéré comme beaucoup plus élevé et exige donc des cycles de contrôle plus courts. Quant aux contraintes actuellement très strictes applicables aux banques de données LMSI cantonales, elles 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, par le biais notamment de cours de formation, de prescriptions et de 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 des traitements de données. Ces critères s'inspirent de ceux des organes de surveillance (art. 65 ss). Quant aux enseignements qui en sont tirés, ils profitent systématiquement aux cours de formation destinés aux collaborateurs. S'agissant du système de stockage des données résiduelles, un contrôle périodique des annonces s'assure que seules les annonces qui répondraient aussi aux exigences liées à un nouvel enregistrement restent enregistrées dans le système. On ne vérifie toutefois pas l'ensemble des données personnelles dans le détail mais on s'assure que l'annonce dans sa globalité soit pertinente et exacte.
- S'agissant du système de stockage des données résiduelles, un contrôle périodique des annonces s'assure que seules les annonces qui répondraient aussi aux exigences liées à un nouvel enregistrement restent enregistrées dans le système. On ne vérifie toutefois pas l'ensemble des données personnelles dans le détail mais on s'assure que l'annonce dans sa globalité soit pertinente et exacte.

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 toutes les données quant à leur exactitude et à leur pertinence;
- contrôle périodique: les données enregistrées dans les systèmes d'information du SRC sont régulièrement contrôlées pour savoir si elles sont encore nécessaires pour l'accomplissement des tâches prévues dans la présente loi;

- triage de sortie: les données personnelles ne peuvent avoir un impact vers l'extérieur que si le traitement des données est légal (voir l'art. 54);
- 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 liminaire effectuée par le SRC avant chaque saisie de données dans un système d'information.

L'élément déterminant selon *l'al.1* est que les données en question soient pertinentes et exactes. Dans le système de stockage des données résiduelles, qui n'est pas ordon-

né selon des objets ou des personnes, l'appréciation ne s'effectue pas pour les données personnelles individuelles d'une annonce mais pour 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. 4, al. 1). Lors du contrôle d'entrée et avant de les saisir dans un système d'information, le SRC doit concrètement s'assurer que les renseignements et les annonces présentent un lien avec l'extrémisme violent, le terrorisme, l'espionnage, la prolifération, des attaques contre 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 activités politiques (art. 3, al. 5 à 8).

Conformément à l'*al.* 4, le SRC veille à ce que les données personnelles enregistrées dans tous ses systèmes d'information soient régulièrement contrôlées. Les données dont il n'a plus besoin pour l'exécution de ses tâches sont éliminées de ses systèmes pour être archivées conformément aux prescriptions des Archives fédérales (art. 59).

*Art. 41* Traitement des données par les cantons

*L'al. 1* se fonde sur le concept suivant: tant que les autorités cantonales d'exécution sont actives dans le domaine d'application du présent texte de loi, elles travaillent exclusivement avec les systèmes d'information que la Confédération met à leur disposition. C'est ainsi que l'INDEX SRC permet par exemple aux cantons de saisir des enquêtes préalables sur des rapports adressés à la Confédération, de gérer les mandats et d'archiver leurs rapports (voir à cet égard l'art. 46). Les données sont exclusivement administrées par la Confédération, par le truchement du SRC, et sont soumises au droit de la protection des données de la Confédération. Cette dernière est le seul maître des données dans le domaine d'application du présent texte de loi.

Les données stipulées à l'*al. 2* sont traitées par les cantons soit dans le cadre de la propre activité cantonale 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. C'est ainsi que les cantons traitent par exemple les données liées aux demandes d'autorisation pour des manifestations de leur propre chef. Et si des débordements extrémistes violents sont à craindre dans ce contexte, le SRC les traite également de ce point de vue. Si la manifestation se déroule effectivement dans la violence, le SRC traite ces informations du point de vue de l'extrémisme violent d'après la présente loi alors que les autorités cantonales s'intéressent de leur propre chef aux infractions, telles que les déprédations matérielles, les violations de l'ordre public ou les lésions corporelles. En raison des diverses réglementations applicables au devoir de renseignement pour ces traitements de données, il faut éviter qu'une banque de données contienne des indices 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 traitement bilatéral, par exemple en cas d'éventuelles réserves lors d'interrogations.

**Section 2: Systèmes d'information en matière de renseignement**

*Art. 42* Systèmes d'information du SRC

L'art. 42 définit le réseau de systèmes d'information que le SRC exploite afin de s'acquitter de ses tâches. Le réseau est comparable à celui des systèmes d'information de police, tel qu'il est réglé à l'art. 2 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[24].

L'article donne un aperçu de tous les systèmes d'information du SRC qui s'appuient sur la présente loi sur le plan juridique formel. Chaque système d'information est traité ci-après dans un article séparé.

L'*al. 2* charge le Conseil fédéral de déterminer les spécificités du traitement des données pour chaque système d'information, dont les délais pour les contrôles périodiques et la durée de conservation maximale. La délégation de ces réglementations détaillées 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)[25] fixe aujourd'hui par exemple les délais maximaux de conservation, qui sont de 30 ans après le dernier traitement pour les données concernant l'exploration à l'étranger, mais de 45 ans au maximum. Pour ce qui est des données suisses, selon la provenance des données, ces délais se situent entre cinq (données issues des contrôles de sécurité relatifs aux personnes) et 45 ans (données issues de sources publiquement accessibles). 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 stipule à cet effet que le Conseil fédéral doit tenir compte des spécificités des données ainsi que des besoins inhérents aux différents domaines d'activités lorsqu'il fixe les délais en question. Cela doit permettre, comme auparavant, de trouver des solutions différenciées pour les divers systèmes et catégories de données.

De plus, le SRC va édicter des règlements d'utilisation pour tous les systèmes d'information en se fondant sur les consignes générales applicables en matière de droit de la protection des données et des informations, règlements qui décrivent notamment l'organisation interne ainsi que les procédures de traitement de données et de contrôle et qui contiennent la documentation sur la planification, la réalisation et l'exploitation de la banque de données ainsi que des moyens informatiques.

*Art. 43* Versement des données dans les systèmes d'information

Les données qui parviennent au SRC sont dans un premier temps examinées quant à leur pertinence pour l'exécution de la mission et quant à 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, d'analyser et de documenter les données et enseignements nécessaires à la production. L'INDEX SRC contient du côté du SRC avant tout les données d'identification de personnes, d'organisations, d'objets et d'événements qui sont copiées à partir des systèmes SAI SRC et SAI-EXTR SRC dans l'INDEX SRC.

[24] RS **361**
[25] RS **121.2**

*Art. 44* SAI SRC

L'art. 44 ancre formellement le système SAI SRC (système d'analyse intégrale du SRC) sur le plan juridique, un système qui permet d'effectuer une analyse relevant du renseignement pour 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 SAI-EXTRSRC (art. 45). A quelques détails près, SAI SRC remplace les systèmes actuels que sont ISIS et ISAS.

La saisie et le contrôle périodique des données enregistrées dans IASA incombent aux analystes du SRC dans leurs spécialisations respectives. L'organe interne de contrôle de la qualité effectue de plus régulièrement des contrôles par sondage, afin de s'assurer que les données soient traitées conformément à l'esprit de la loi (art. 40).

*Art. 45* SAI-EXTR SRC

Les données liées à l'extrémisme violent ont souvent des liens plus prononcés exclusivement liés à 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 et soustraites à la recherche ainsi qu'au traitement des informations conformément à l'art. 3, al. 5, LRens. Elles sont par conséquent saisies dans un système d'information particulier, à savoir SAI-EXTR SRC (système d'analyse intégrale de l'extrémisme violent), qui sert à saisir, traiter et analyser de manière centralisée toutes les données se rapportant à ce domaine. Elles y 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. 40, al. 5, let. a).

Conformément à l'art. 61, al. 1, let. c, le Conseil fédéral détermine chaque année les groupements qui doivent être catégorisés comme extrémistes violents.

*Art. 46* INDEX SRC

L'INDEX SRC (système d'indexation des données) 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 SAI SRC et SAI-EXTR SRC peuvent y être consultées. Concrètement, ce sont les principales données d'identification pour les personnes qui y sont saisies, telles que le nom, la date de naissance, la nationalité, etc. Ont également accès à l'index les organes autorisés qui ne sont pas raccordés au réseau hautement sécurisé du SRC.

L'INDEX SRC sert ainsi à coordonner les activités relevant du renseignement de la Confédération et des cantons mais aussi à coordonner les activités ressortissant au renseignement avec celles relevant de la police de sûreté et de la police criminelle. Aujourd'hui, une telle coordination est possible en ce sens 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 des autorités d'exécution cantonales 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. 54 ss).

L'INDEX SRC est nécessaire à ces fins comme système particulier, puisque SAI SRC et SAI-EXTR SRC doivent être exploités dans le réseau hautement sécurisé du SRC pour des raisons de sécurité, lequel n'autorise aucun accès de services exté-

rieurs au SRC. L'INDEX SRC permet aux services tiers autorisés de demander rapidement les 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 d'exécution cantonales. Elles y traitent les données en amont d'un rapport destiné au SRC. L'index leur permet en outre d'avoir une vue d'ensemble des mandats de la Confédération et de les archiver. Grâce à cette centralisation à l'échelon fédéral de tous les traitements de données intervenant dans le cadre du présent texte de loi, il est possible de garantir une réglementation et un contrôle uniformes.

*Art. 47* GEA SRC

Le système GEA SRC (système de gestion des affaires du SRC) consiste en une administration standardisée des affaires, comme elle est utilisée dans d'autres secteurs de l'administration fédérale également. Toutefois, le SRC traite typiquement des affaires qui relèvent avant tout du renseignement, telles que des rapports d'analyse, des appréciations de situation écrites ou orales ou encore des réponses à des demandes individuelles. Celles-ci 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 GEA 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 GEA SRC dans son réseau particulièrement protégé, auquel aucun service tiers n'a accès.

*Art. 48* PES

L'art. 48 reprend de l'art. 10*a* LMSI le fondement juridique formel pour la PES, le système du SRC pour la présentation électronique de la situation. La réglementation 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 cela est absolument nécessaire pour la présentation et l'appréciation de la situation.

En ce qui concerne l'*al. 3*, l'accès exceptionnel de privés 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: jusqu'à présent, aucun accès de la sorte n'a été autorisé, car aucune situation correspondante ne s'est présentée. 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 démontré que lors de manifestations d'envergure avec un potentiel de risque accru, il peut être nécessaire de donner immédiatement accès à certaines données du système PES SRC à des organisations privées ou à des partenaires étrangers également. 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 donne un accès qu'aux données qui sont nécessaires pour la lutte contre cette menace en particulier.

*Art. 49* Portail ROSO

L'art. 49 constitue la base juridique formelle sur laquelle s'appuie le portail d'accès aux renseignements de source ouverte (ROSO), système servant aux collaborateurs du SRC à compiler des données provenant de sources accessibles au public. L'enregistrement de données web est par exemple indispensable à une analyse ciblée, faute de quoi il faudrait à chaque fois recommencer les recherches dans l'ensemble du web, tout en sachant que la disponibilité des données autrefois existantes sur Internet n'est nullement garantie.

Etant donné qu'il s'agit de données qui sont en principe accessibles à tout le monde, elles doivent être traitées de manière moins restrictive au sein du SRC que les données issues d'autres sources. Il est par conséquent inutile, dans *l'al. 3,* d'en limiter l'accès à certains domaines du SRC.

*Art. 50* Quattro P

Le SRC fait aujourd'hui déjà saisir par les organes aéroportuaires suisses de contrôle à la frontière les données d'entrée dans le pays de personnes provenant de certains pays à des fins de détection précoce des activités d'espionnage et de prolifération. Ces données, il doit les traiter dans un système d'information séparé portant le nom de Quattro P (« Programme préventif de contrôle des passeports », jusqu'à présent dans le module informatique P4 selon l'art. 25, al. 1, let. h, OSI-SRC).

Conformément à l'*al. 3,* seul un petit cercle de personnes au sein du SRC y a accès, celles qui sont chargées de saisir, de rechercher et d'analyser ces données (moins de dix personnes à l'heure actuelle).

Le Conseil fédéral détermine selon l'*al. 4* annuellement la portée des contrôles, 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. 18, al. 4, pour la détermination des incidents ainsi que des observations devant spontanément être annoncés au SRC. S'agissant des données du système Quattro P, la durée maximale de conservation est aujourd'hui de cinq ans (art. 33, al. 1, let. i, OSI-SRC).

*Art. 51* SICO

Le système 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 à cet effet les art. 33 ss). Les mandats en question contiennent l'ordre d'exploration, les informations relatives aux objets concrets devant être explorés, les résultats attendus ainsi que d'autres conditions-cadre applicables au développement du mandat. Font également partie de SICO les résultats des contrôles périodiques internes au SRC quant à la légalité, l'utilité et l'efficacité des mesures d'exploration. Les données de SICO servent de base pour les activités des organes de surveillance (en particulier l'organe de contrôle autonome prévu à l'art. 67).

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 ainsi que 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. 52).

*Art. 52* Système de stockage des données résiduelles

Sont enregistrées dans le système de stockage des données résiduelles toutes les informations qui n'ont pas pu être directement versées dans un autre système lors du triage effectué après le contrôle d'entrée. Il s'agit avant tout des annonces provenant d'autorités étrangères de sûreté, de données issues de l'exploration radio ainsi que de l'exploration du réseau câblé, provenant d'informateurs et d'informations qui ne sont pas activement acquises 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 le système SAI-EXTR SRC.

Les informations issues du système de stockage des données résiduelles sont transférées dans le système SAI-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 actuelles contenues dans le système de stockage des données résiduelles soient pertinentes (lien avec un domaine d'activité du SRC, respect des limites de traitement fixées aux al. 5 à 8 de l'art. 3 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 s'effectue sur la base de l'annonce dans sa globalité, c'est-à-dire qu'aucune déclaration individuelle émanant d'un document plus important n'est examinée.

**Section 3: Données provenant de mesures de recherches soumises à autorisation**

*Art. 53*

Les données qui sont acquises par le biais de mesures de recherche soumises à autorisation nécessitant l'engagement de moyens technologiques (comme par ex. une surveillance de communications) peuvent d'une part être très volumineuses et contenir d'autre part de nombreuses informations n'ayant aucun rapport avec le but de la recherche, parce qu'elles sont par exemple de nature strictement privée. Il faut également tenir compte de la protection de la personnalité des tiers qui utilisent par exemple le raccordement de télécommunication de la personne surveillée. Souvent, il n'est pas possible de déterminer de prime abord si des communications données sont pertinentes ou non, parce que le réseau de contact de la personne surveillée doit par exemple encore être identifié ou que celle-ci utilise des éléments de conspiration dans ses communications pour les protéger. Les informations ne peuvent donc pas être immédiatement identifiées comme nécessaires ou non.

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

L'art. 53 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. Le SRC ne reprend que les données nécessaires aux fins du mandat selon l'*al. 2* pour les analyser ultérieurement dans les systèmes d'information correspondants du réseau, en règle générale dans SIA SRC.

L'*al. 3* restreint par conséquent 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.

**Section 4: Dispositions particulières relatives à la protection des données**

*Art.54* Vérification avant la transmission de données

Sont tenus d'évaluer la qualité des données avant transmission non seulement les organes du SRC chargés plus particulièrement du contrôle de qualité mais aussi chaque personne qui participe à une transmission d'informations du SRC. Ils sont tenus de veiller à ce que le cadre juridique préalable nécessaire à la transmission soit respecté et que les données personnelles soient traitées correctement.

*Art. 55* Transmission de données personnelles à des autorités suisses

Afin que le SRC puisse s'acquitter de sa mission, il doit pouvoir transmettre des données personnelles à des autorités politiques, des autorités de poursuites pénales, des autorités judiciaires ou des autorités de sûreté. A quelques détails près, la réglementation correspond au droit en vigueur dans l'art. 17 LMSI. Elle a toutefois été précisée et différenciée dans la LRens.

La transmission de données issues de mesures de recherche soumises à autorisation exige notamment d'autres mesures de protection. On veut ainsi éviter que de petits délits qui ont par exemple été constatés lors de surveillances de télécommunications soient annoncés aux autorités de poursuites pénales. Le droit de procédure pénale contient une réglementation similaire pour de telles découvertes dites fortuites (art. 278 CPP). La LRens reprend dès lors dans l'*al. 3* le principe selon lequel seules peuvent être utilisées les données d'observations se rapportant à des infractions pour la poursuite desquelles la mesure de surveillance correspondante ressortissant au droit de procédure pénale aurait pu être ordonnée.

*Art.56* Transmission de données personnelles à des autorités étrangères

A quelques détails près, cet article reprend les dispositions de l'art. 17 LMSI. Le droit en matière de protection des données prévoit en règle générale que des données personnelles ne peuvent être transmises qu'aux Etats qui garantissent un niveau de protection des données comparable à celui de la Suisse (art. 6, al. 1, LPD). Une telle disposition exclurait la plupart des pays non européens de la collaboration avec le SRC si les exceptions restrictives prévues à l'art. 6, al. 2, LPD ne pouvaient pas s'appliquer au cas par cas, ce qui priverait le SRC d'importantes sources d'information dans les régions en crise.

C'est pourquoi la LMSI établit déjà des réglementations particulières pour la collaboration en matière de renseignement et l'échange de données personnelles avec

l'étranger, que la LRens reprend ici. Il existe à cet effet une longue pratique, qui est 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).

L'*al. 2, let. d*, concerne les demandes de conformité ou les clearings déjà mentionnés à l'art. 10, al. 1, let. d, au profit de personnes (généralement suisses) qui doivent avoir accès à l'étranger à des projets, informations, installations, etc. classifiés. De tels renseignements sont en règle générale dans l'intérêt de la personne concernée, qui ne pourrait sinon pas débuter à une place de travail ou commencer une activité commerciale.

*Art. 57* Transmission de données personnelles à des tiers

Jusqu'à présent, pour qu'une activité en matière de renseignement soit possible, il était également nécessaire de pouvoir transmettre des données à des privés. Le cas pratique le plus fréquent consiste à motiver une propre demande de renseignement. En d'autres termes, lorsqu'il recherche des renseignements sur des personnes physiques ou morales, le SRC doit naturellement pouvoir dire à la personne interrogée sur qui il a besoin d'un renseignement et dans quel contexte. Cette disposition correspond à l'actuel art. 17, al. 3, LMSI.

*Art. 58* Droit d'accès

S'agissant du droit d'accès d'une personne aux données saisies la concernant, le projet de loi reprend la solution adoptée par le Parlement dans le cadre de la révision LMSI du 23 décembre 2011 (« LMSI II réduite »), qui s'inspire de la LSIP. A quelques détails près, la LRens reprend à cet égard l'art. 18 LMSI dans sa nouvelle version, entrée en vigueur le 16 juillet 2012.

Dans le cadre de la consultation relative à la LMSI II, le Conseil fédéral avait encore demandé lors de la discussion portant sur le réaménagement de ce droit d'accès à ce que la LPD soit intégralement appliquée. Or, comme le Parlement a sciemment opté pour la solution inspirée de la LSIP, le Conseil fédéral considère qu'il n'est pas judicieux de soumettre une nouvelle fois une réglementation différente en la matière.

La procédure prévoit que le SRC examine d'abord l'opportunité de donner un renseignement mais retarde l'échéance au cas où des intérêts visant à préserver un secret ou des personnes non répertoriées entrent en jeu. La personne concernée peut ensuite s'adresser au Préposé fédéral à la protection des données et à la transparence (PFPDT), qui applique ensuite en substance l'ancienne procédure du renseignement indirect.

En guise de seul écart par rapport à la réglementation actuelle de la LMSI le Conseil fédéral propose de revenir dans l'*al. 9* à la formulation originelle dans la LSIP, qui prévoit que des renseignements peuvent exceptionnellement être donnés sur recommandation du PFPDT en cas de report de la réponse (en raison d'intérêts liés au maintien du secret ou en présence de personnes non répertoriées), pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure de la Suisse et qu'une personne peut expliquer de façon convaincante que le report de la réponse la lèserait gravement et de manière irréparable.

Dans la LMSI, la charge de la preuve a été inversée, en ce sens que le SRC doit donner un renseignement sur recommandation du PFPDT dans la mesure où cela ne

constitue pas une menace pour la sûreté intérieure ou extérieure du pays. S'agissant des personnes non répertoriées, le SRC ne peut en règle générale pas apporter cette preuve, puisqu'il ne dispose précisément d'aucune information sur elles. La règle stipulée à l'al. 2, let. c, qui dit que la réponse est différée pour les personnes non répertoriées, devient donc caduque. Le Conseil fédéral considère dès lors qu'il est techniquement plus juste de revenir à la procédure prévue dans la LSIP.

**Section 5: Archivage**

*Art. 59*

Les données et dossiers du SRC sont globalement soumis à la loi fédérale du 26 juin 1998 sur l'archivage[26] (LAr). A l'expiration de leur délai de conservation, ils sont transférés dans des locaux (en partie spécialement sécurisés) des Archives fédérales et gérés selon les principes de l'archivage. Une exception existe déjà aujourd'hui en ce qui concerne les données et les dossiers provenant de relations directes avec des services de sécurité étrangers. Leur transmission et leur archivage sont soumis à la règle internationale habituelle de l'approbation explicite du maître des données étranger. C'est pourquoi le Conseil fédéral doit régler dans une ordonnance la conservation et la destruction de ces données et de ces dossiers dans l'esprit de la base légale actuelle (art. 28, al. 2, OSRC).

**Chapitre 5: Prestations**

*Art. 60*

A l'instar de chaque autre service officiel, le SRC est globalement autorisé et tenu de fournir une assistance administrative dans les domaines où il est à la fois compétent et en mesure de le faire, tant sur le plan du personnel que technique. Le SRC peut ici mettre à disposition des moyens et des méthodes de type opérationnel particuliers, par exemple des prestations de transmission, de transport et de conseil, dont les autres services ne disposent pas.

C'est ainsi que des moyens de communication sécurisés du SRC sont 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 sécurité d'écoute et de la protection des informations. Le SRC conseille les organes d'acquisition de la Confédération pour ce qui est des coffres-forts et des techniques de fermeture. Les services partenaires étrangers sont notamment soutenus par le SRC par le biais de transports spéciaux.

[26] SR **152.1**

Lors d'un cas d'enlèvement à l'issue heureuse, le SRC a participé à l'effort de gestion de la crise en fournissant les prestations suivantes:

- Il a mis à disposition des moyens de communication sécurisés pour assurer la liaison entre le centre de gestion des crises du DFAE ainsi que la représentation de ce dernier sur place et a fourni le support technique.
- Il a mis à disposition 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 en permanence mis à la disposition de l'ambassadeur suisse un collaborateur pour assurer la liaison avec le service de renseignement local ainsi que 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 d'autres services de renseignement étrangers et de la collaboration avec d'autres services suisses.
- Il a servi de base de négociation et de communication avec le service de renseignement étranger concerné.

Le Conseil fédéral considère qu'il est juste de créer une base légale explicite pour ces prestations de soutien.

## Chapitre 6: Pilotage politique, contrôle ainsi que voies de droit

### Section 1: Pilotage politique et interdiction d'exercer une activité

*Art. 61* Pilotage politique par le Conseil fédéral

Le SRC est un instrument qui sert dans une mesure particulière les intérêts du pays et du gouvernement. Le rôle du Conseil fédéral sur le plan du pilotage politique et de l'orientation des activités du SRC ne doit dès lors pas seulement être repris des bases juridiques actuelles mais explicité et renforcé. L'art. 61 reprend donc différents éléments de la législation actuelle et les réunit dans une disposition centrale sur le pilotage politique.

La *let. a* approfondit le système déjà existant aujourd'hui, selon lequel le Conseil fédéral donne au SRC une mission 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, notamment dans le domaine de l'étranger, de couvrir de la même manière l'ensemble des régions et des évolutions ressortissant à la politique de sécurité. La mission de base du Conseil fédéral lui dicte donc l'orientation nécessaire. De plus, des événements et des développements à court terme peuvent bien évidemment influer sur l'activité du SRC à l'intérieur du cadre légal. Lorsque de tels développements ont un impact à long terme, la mission de base doit, le cas échéant, déjà être adaptée hors de la période ordinaire de contrôle de quatre ans. S'agissant du pilotage politique, il faut toutefois globalement viser la continuité.

A l'heure actuelle, 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 dans l'art. 63 et que l'on connaît déjà du droit en vigueur (art. 11, al. 3 à 7, LMSI).

La *let. c* s'inspire du nouveau concept de traitement des données, avec la distinction et le traitement plus strict des données liées à l'extrémisme violent. Afin que le SRC puisse faire cette distinction de manière univoque, le Conseil fédéral désigne chaque année les groupements ressortissant à ce dernier. Aucune mesure soumise à autorisation selon les art. 22 et suivants ne peut par exemple être prise contre de tels groupements. De plus, les données concernant les groupements extrémistes violents sont versées dans le système d'information spécial SIA-EXTR SRC dans le cadre du traitement des donnés du SRC (art. 45). Parallèlement, le SRC l'informe 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. Le Conseil fédéral obtient ainsi une image d'ensemble de l'extrémisme violent en Suisse.

Comme c'était déjà le cas avec le droit en vigueur, le Conseil fédéral approuve la collaboration du SRC avec les organes de sûreté d'autres Etats, conformément à la *let f*. Sont avant tout concernés ici 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.

La collaboration avec des autorités étrangères dans le domaine du renseignement, qui doit être autorisée par le Conseil fédéral, n'est classiquement pas réglée de façon formelle, par exemple par le biais de traités internationaux. Le plus souvent, il s'agit d'accords informels non contraignants (déclarations d’intention) ou de conventions administratives.

Le rattachement du SRC à une banque de données commune qui serait exploitée en réseau avec des partenaires étrangers du SRC devrait en revanche être réglé dans un accord de droit public conclu par le Conseil fédéral conformément à l'*al. 2*. A l'heure actuelle, il n'existe ni de banques de données de la sorte ni d'accords correspondants, même si des réflexions sont fréquemment émises sur le plan international visant à améliorer la collaboration à l'aide de tels instruments. Le Conseil fédéral considère dès lors qu'il est judicieux, en cas de nouvelle codification du service de renseignement, de procéder aux travaux préparatoires nécessaires afin que la Suisse, puisse à l'avenir éventuellement participer à de tels développements.

*Art. 62* Sauvegarde d'autres intérêts essentiels de la Suisse

Cet article s'inspire de l'art. 1, al. 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 ne sont pas supprimées. L'attribution formelle d'un mandat constitue bien plus une condition préalable pour que le SRC puisse tout simplement agir.

*Art. 63* Liste d'observation

Déjà connue de la LMSI, la liste d'observation est un instrument de conduite du Conseil fédéral. La liste est établie par le DDPS et doit être approuvée chaque année par ce dernier (art. 60, al. 1, let. b). Depuis le 11 septembre 2001, la communauté internationale a intensifié ses efforts de lutte contre le terrorisme. En raison de la prise en compte des listes internationales (révision LMSI II réduite du 23 décembre 2011), le lien vers les listes internationales de terroristes a été pris comme étalon pour la liste d'observation. A la différence de la LMSI, qui charge le Conseil fédéral de désigner les organisations et communautés internationales importantes, 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.

Lorsqu'une organisation ou un groupement est placé sur la liste suisse d'observation, aucune sanction (par ex. interdiction de l'organisation) n'est prévue, au contraire de ce qui se passe pour le système de liste utilisé par le Conseil de sécurité de l'ONU à l'appui de la résolution 1267. Contrairement à la liste de ce dernier, on ne retrouvera pas non plus d'individus sur la liste d'observation. Finalement, grâce à la procédure annuelle de ratification par le Conseil fédéral, il lui est toujours possible d'éliminer un groupement de la liste. L'enregistrement d'une organisation, d'un groupement (ou d'une personne) sur une liste internationale n'entraîne donc pas automatiquement son inscription obligatoire sur la liste d'observation suisse.

La restriction quant au traitement imposée par l'art. 3, al. 5 (activités politiques et exercice de droits fondamentaux) ne s'applique pas à la liste d'observation (voir à cet égard l'art. 3, al. 8). Le SRC peut acquérir et traiter toutes les informations disponibles sur les organisations et groupements figurant sur la liste, lorsque celles-ci peuvent aider à évaluer la menace émanant de ces associations.

*Art. 64* Interdiction d'exercer une activité

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

La disposition règle la compétence juridique du Conseil fédéral dans les cas prévus par la LRens, sans toutefois restreindre sa compétence globale en matière de promulgation d'ordonnances et d'arrêtés sur la base de l'art. 185, al. 3, Cst. lors d'autres perturbations graves de l'ordre public ou de la sûreté intérieure et extérieure. Cette compétence du Conseil fédéral subsiste en parallèle dans les cas qui ne sont pas régis par la loi.

La disposition proposée prévoit la possibilité pour le Conseil fédéral de prononcer une interdiction d'exercer une activité dans le domaine de la sûreté intérieure ou extérieure pour une durée maximale de cinq ans et de pouvoir la prolonger à chaque fois de cinq ans, pour autant que les conditions préalables nécessaires à cet effet 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, il existe actuellement une ordonnance de l'Assemblée fédérale interdisant Al-Qaïda en tant qu'organisation et qui expire à fin 2014. Il conviendra d'examiner s'il vaut mieux, à l'avenir, édicter des interdictions d'exercer une activité selon l'art. 9 LMSI, voire selon la LRens, ou si le Parlement prononce et prolonge des interdictions d'organisation sur la base de sa compétence en matière d'ordonnances.

A l'appui des expériences faites par le passé, on peut partir du principe 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 identifiée distinctement, puisqu'elle se meut dans le cadre des affaires politiques courantes.

L'*al. 1* donne au Conseil fédéral la compétence de décréter une interdiction de droit administratif contre les activités induisant une menace concrète pour la sûreté intérieure ou extérieure de la Suisse. Contrairement à la réglementation actuellement consignée dans la LMSI, tous les départements doivent toutefois pouvoir déposer des demandes dans ce sens.

La portée et le contenu des activités interdites doivent être décrits aussi précisément que possible dans l'arrêté, afin que l'interdiction puisse être appliquée et contrôlée de manière efficace. Elles dépendent toutefois des activités individuelles des personnes concernées et ne doivent donc pas être décrites de manière exhaustive dans la loi.

Les interdictions prononcées selon l'*al. 1* pouvant entraver les personnes visées dans l'exercice de leurs droits fondamentaux, elles doivent être limitées dans le temps. Les autorités sont ainsi tenues, au terme de la durée de validité de l'interdiction, de réexaminer si les conditions ayant présidé à cette dernière sont encore remplies ou si elles sont devenues caduques.

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

Les interdictions d'exercer une activité prononcées sur la base de cet article peuvent, conformément à l'art. 71, être attaquées devant le Tribunal administratif fédéral et ensuite déférées au Tribunal fédéral.

## Section 2: Contrôle et surveillance du Service de renseignement

*Remarques liminaires*

Les art. 65 à 69 contiennent par ordre croissant la cascade des prescriptions en matière de surveillance et de contrôle:

1. Auto-contrôle du SRC
2. Surveillance par le département
3. Organe de contrôle indépendant pour l'exploration radio
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 autonome (OCA, art. 67) veille à la légalité de l'exploration radio à l'étranger, conformément à l'art. 33.

*Art. 66* Surveillance par le département

L'organe de contrôle du renseignement interne au département (aujourd'hui appelé « Surveillance des services de renseignement SSR ») est désormais réglé à l'échelon de la loi (al. 2), car des compétences élargies doivent lui être octroyées. Son activité de contrôle auprès des autorités cantonales d'exécution doit aussi être ancrée dans la loi (al. 3). Cette procédure s'applique aux domaines au sein desquels les cantons recherchent des informations sur la base du droit fédéral (voir l'art. 73). De cette manière, la tâche de contrôle et de pilotage du DDPS est complétée selon l'al. 1.

*Art. 67* Organe de contrôle indépendant pour l'exploration radio

Comme celle applicable à l'exploration radio (art. 33), la réglementation sur l'organe de contrôle autonome (OCA) correspond à la réglementation entrée en vigueur le 1er novembre 2012, que le Parlement a directement ancré dans la LFRC (art. 4b). Il s'agit aujourd'hui d'une commission interne à l'administration. L'activité de contrôle de l'OCA était auparavant déjà réglée de manière similaire dans l'ordonnance sur la guerre électronique et a fait ses preuves au cours des années écoulées. Elle répond à un besoin dans un domaine sensible de l'exploration à l'étranger. S'agissant de l'exploration du réseau câblé, des dispositions similaires s'appliquent. En revanche, une autorisation judiciaire et politique similaire à la procédure applicable aux mesures de recherche soumises à autorisation est prévue, car l'exécution de la recherche requiert la collaboration de fournisseurs privés de télécommunications en Suisse, ce qui n'est pas le cas pour 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'OCA brouillerait en revanche les domaines de compétences des parties prenantes (Tribunal administratif fédéral et chef du DDPS d'un côté et OCA de l'autre) et n'est donc pas indiqué.

La seule différence par rapport à l'art. 4*b* LFRC réside dans l'emplacement de la durée de mandat de l'OCA, qui ne figure pas à l'al. 1, mais à l'al. 4, puisqu'il s'agit plutôt d'une spécificité de l'exécution.

*Art. 68* Surveillance et contrôle par le Conseil fédéral

Le présent article reprend le principe du contrôle des activités quant à leur légitimité, utilité et efficacité, déjà ancré dans l'art. 26 LMSI et déclaré valable pour l'ensemble du service de renseignement par le biais de l'art. 8 LFRC. La LRens maintient ici le standard existant en matière de surveillance et de contrôle. L'information régulière du Conseil fédéral sur les observations des organes de surveillance du DDPS ainsi que de la Délégation des Commissions de gestion en fait également partie.

*Art. 69* Haute surveillance parlementaire

Le principe de la réglementation actuelle selon l'art. 25 LMSI est repris et simultanément précisé: la haute surveillance parlementaire de l'exécution du présent projet de loi est exclusivement du ressort de la Délégation des Commissions de gestion des Chambres fédérales. Ce contrôle englobe aussi bien les activités du SRC que celles des autorités d'exécution cantonales. Une bipartition de la haute surveillance entre les parlements cantonaux, d'une part, et le Parlement fédéral, d'autre part, n'est pas prévue dans le présent projet de loi.

Le Conseil fédéral est d'avis que le législateur fédéral a réglé la haute surveillance parlementaire de manière conclusive en créant la Délégation des Commissions de gestion pour la surveillance des activités dans le domaine du renseignement et en lui octroyant des compétences particulières par le biais de l'art. 53 de la loi fédérale du 13 décembre 2002 sur l'Assemblée fédérale[27]. Si le législateur fédéral octroyait en parallèle aux cantons des compétences à l'échelon cantonal sans les assortir de servitudes particulières, cela relèverait de l'inconséquence. Les organes cantonaux de sûreté interviennent toujours dans l'exécution directe de la loi au profit des organes fédéraux et non dans l'intérêt exécutif originel des cantons.

Les parlements cantonaux restent, bien sûr, autonomes dans les domaines où les autorités cantonales sont responsables de la sûreté intérieure de leur territoire hors du présent projet de loi.

Art. 70 *Surveillance cantonale*

Il est proposé un partage de la surveillance des autorités d'exécution cantonales entre la Confédération et les cantons.

*Surveillance par la Confédération*

La haute surveillance sur l'exécution matériellement correcte de la présente loi et donc sur l'activité des autorités d'exécution cantonales incombe à la Délégation des Commissions de gestion des Chambres fédérales. Par ailleurs, l'instance de surveil-

[27] RS **171.10**

lance interne au DDPS peut effectuer des contrôles auprès des autorités cantonales d'exécution (art. 66, al. 3).

*Surveillance par les cantons*

La surveillance des cantons consiste pour l'essentiel en la surveillance des services par les instances supérieures des autorités d'exécution cantonales. La surveillance cantonale des services vérifie:

- que les procédures administratives cantonales correspondent aux prescriptions légales déterminantes,
- que l'autorité cantonale d'exécution traite les données fédérales séparément des 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 acquiert 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 fait ses preuves dans la pratique. Elle doit dès lors être conservée.

Les dispositions sur la surveillance cantonale prévoient également le soutien de la surveillance cantonale des services par les organes de surveillance de la Confédération (par ex. à travers un organe de surveillance similaire à l'actuelle Surveillance des services de renseignement) et l'accès aux informations utiles par la surveillance cantonale des services (al. 3).

Dans le cadre de l'évaluation d'une solution appropriée pour la surveillance sur les autorités d'exécution cantonales, les alternatives suivantes ont été examinées:

a. Une solution exclusivement fédérale: celle-ci signifierait que la surveillance entière sur les autorités d'exécution cantonales serait confiée à la Confédération, par le truchement du SRC. Cette solution unitaire engloberait 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 du canton seraient transférés dans l'administration fédérale.

b. Une solution exclusivement cantonale: à l'inverse de la solution actuelle, une telle solution 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 également. Dans le domaine de la surveillance de la protection des données, la surveillance cantonale devrait être habilitée à consulter intégralement les données qui sont traitées par l'autorité cantonale d'exécution.

La *solution fédérale* aurait l'avantage de mettre en place une réglementation uniforme de la surveillance des autorités d'exécution cantonales. Elle contredirait toutefois le concept fédéral de sûreté intérieure, selon lequel 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 uniquement fédérale irait à l'encontre de la structure fédéraliste de notre Etat et ne bénéficierait pas du profond ancrage local auprès des autorités de sûreté. Elle doit dès lors être abandonnée.

Une *solution purement cantonale* pour la surveillance des autorités d'exécution cantonales aurait également l'avantage de constituer une réglementation uniforme pour tous les cantons. La bipartition entre la Confédération et les cantons au niveau de la surveillance tomberait. Le canton serait seul responsable de la surveillance. Cette solution aurait toutefois l'inconvénient que les parlements cantonaux, à qui incomberait désormais la haute surveillance sur les activités des autorités d'exécution cantonales, pourraient développer des pratiques différentes. De plus, en cas de solution purement cantonale, les organes cantonaux de surveillance devraient avoir 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 plus, des questions difficiles de délimitation concernant la surveillance des missions confiées par l'organe fédéral se poseraient. Le SRC pourrait en partie aussi devoir rendre des comptes aux organes cantonaux de surveillance, ce qui irait à l'encontre du système. Par conséquent, dans l'ensemble, 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 l'actuelle 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 de celui du droit du service. Si elle mène toutefois des enquêtes sur ordre des autorités judiciaires, elle se retrouve sous la surveillance spécialisée de ces dernières.

L'*al. 2* doit préciser clairement que la haute surveillance parlementaire sur l'exécution de la présente loi se trouve entre les mains de la Délégation des Commissions de gestion des Chambres fédérales et pas simultanément (entièrement ou partiellement) auprès d'une autorité cantonale.

**Section 3: Voies de droit**

*Art. 71*

La LRens définit des mesures et des décisions parfois radicales, pour lesquelles il faut garantir des voies de droit appropriées. La LRens prévoit ici dans l'*al. 1* la voie juridique ordinaire vers le Tribunal administratif fédéral puis le Tribunal fédéral. Elles ne tombent dès lors clairement pas sous le coup de la réglementation d'exception selon l'art. 83, let. a, de la loi fédérale du 17 juin 2005 sur le Tribunal fédéral[28], qui exclut les décisions touchant à la sûreté intérieure ou extérieure du pays du champ des recours pour les affaires relevant du droit public.

[28] RS **173.110**

L'*al. 3* empêche que la remise au SRC de renseignements nécessaires pour la sûreté du pays ne puisse être retardée par des recours jusqu'à ce qu'il soit trop tard pour écarter la menace.

Etant 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. 4* fixe le début du délai de recours à la date de réception de la communication.

## Chapitre 7: Dispositions finales

*Art. 72* Dispositions d'exécution

Conformément à l'art. 7 de la loi sur l'organisation du gouvernement et de l'administration, le Conseil fédéral édicte les ordonnances, dans la mesure où la constitution ou la législation l'y autorise (voir à cet égard aussi l'art. 182, al. 1, Cst.). De plus, l'art. 72 charge le Conseil fédéral d'édicter des prescriptions générales en matière d'exécution pour les délégations spéciales prévues par la loi.

*Art. 73* Exécution par les cantons

*L'al. 1* statue 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. Sur le principe, il y a lieu de faire les remarques suivantes 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 vraies responsabilités fédérales (mesures pour sa propre protection, pour la protection de ses institutions et 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[29]). Selon ce dernier, les cantons sont libres de développer des activités propres et d'édicter des dispositions juridiques dans le domaine du renseignement, pour autant qu'il ne s'agisse pas de domaines au sein desquels la compétence de réglementation incombe à la Confédération (compétence originelle ou inhérente). La compétence de réglementation de la Confédération concernant la sauvegarde de la sûreté intérieure est concrétisée dans le présent projet de loi.

Le « rapport Malama » du Conseil fédéral dit ceci au sujet de la responsabilité des cantons (voir les pages 4181/4182):

*«…..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*

[29] FF **2012** 4161

*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 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 dans les *al. 1 et 2* (recherche d'informations, de manière autonome ou sur la base d'un mandat du SRC, annonce spontanée au SRC) ont été repris du droit en vigueur (art. 12 LMSI). Ils ont fait leur preuve dans la pratique et doivent être conservés.

Le soutien technique et opérationnel mutuel, tel qu'il est stipulé aux *al. 3 et 4* existe depuis des années et permet une utilisation efficace des moyens en personnel et des moyens techniques de la Confédération et des cantons.

L'indemnisation des cantons selon l'*al. 5* pour des 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, et ne pas la considérer comme acquittée à la suite de la péréquation financière globale entre la Confédération et les cantons.

**Abrogation et modification du droit en vigueur**

**I Abrogation du droit en vigueur**

Le présent projet de loi ne reprend pas les dispositions relevant du droit policier de la LMSI (protection de personnes et de bâtiments, mesures contre la violence lors de manifestations sportives, saisie de propagande violente). Les dispositions à caractère de droit policier seront reprises dans la future loi sur les tâches de police, également en préparation.

Dans le cas où la loi sur le renseignement peut entrer en vigueur avant la loi sur les tâches de police, le Conseil fédéral veillerait à ce qu'aucune lacune juridique ne surgisse en se servant de la mise en vigueur et de l'abrogation partielles.

La même remarque s'applique au domaine des contrôles de sécurité relatifs aux personnes (CSP), où une nouvelle base juridique est également en préparation (loi sur la sécurité de l'information), qui reprendra cette partie de la LMSI. Les dispositions relatives aux CSP ne figurent dès lors plus dans le présent projet de loi.

La LFRC est en revanche intégralement reprise par la LRens et peut par conséquent être purement et simplement abrogée.

## II Modification du droit en vigueur

### 1. Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile[30]

*Art. 9, al. 1, let. c et l (nouvelle)*

Les autorités fédérales responsables de la sûreté intérieure sont aujourd'hui mentionnées à l'art. 9, al. 1, let. c, LDEA (accès en ligne), mais cet accès en ligne au système d'information de l'Office fédéral des migrations (ODM) est limité pour le SRC à l'examen de mesures d'éloignement, ce qui ne correspond pas au spectre global 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 potentiels pour la sûreté intérieure ou extérieure. Nous proposons dès lors d'expliciter les conditions préalables nécessaires à l'accès en ligne conformément aux tâches légales du SRC et de les régler simultanément dans une lettre séparée de l'art. 9, al. 1. Les réserves émises par rapport aux dangers pour la sûreté intérieure ou extérieure sont contenues dans de nombreuses dispositions de la loi fédérale du 16 décembre 2005 sur les étrangers[31] ainsi que de la loi fédérale du 26 juin 1998 sur l'asile[32], ce qui permet au présent texte de loi de renoncer à certaines mentions individuelles.

### 2. Loi fédérale du 26 juin 1998 sur l'archivage[33]

*Art. 14, al. 2, let. a$^{bis}$ (nouvelle)*

30 RS **142.51**
31 RS **142.20**
32 RS **142.31**
33 RS **152.1**

Ce complément doit combler une lacune dans l'actuel droit sur l'archivage. Les tiers ont certes en partie la possibilité de consulter des dossiers archivés en lien avec la sûreté intérieure et extérieure, mais pas l'organe de livraison, à savoir ici le service de renseignement, lorsqu'il s'agit de procéder à une nouvelle appréciation de menaces pour laquelle les dossiers archivés pourraient être utiles. La LAr doit dès lors être complétée de sorte à ce qu'elle tienne compte de cet aspect lié à la sauvegarde de la sûreté intérieure et extérieure.

### 3. Loi fédérale du 17 décembre 2004 sur la transparence[34]

Les expériences faites par le SRC depuis sa création avec les demandes de consultation fondées sur la LTrans ont démontré que le besoin de protection particulier lié aux informations ressortissant au renseignement n'est qu'insuffisamment conciliable avec l'esprit de transparence préconisé par la LTrans.

Les demandes d'accès déposées jusqu'à présent concernaient toujours des documents et des dossiers sur la recherche d'informations par le SRC ou sur des actions exécutées par le SRC (ou ses prédécesseurs). Ponctuellement, l'accès a également été demandé à d'autres documents, concernant par exemple les échanges avec les services partenaires étrangers.

Eu égard aux personnes ou aux services partenaires impliqués, le SRC a toujours dû refuser l'accès aux dossiers de recherche et du service partenaire. Les demandes ont en partie engendré une charge de travail conséquente, car les documents souhaités ont dû être réunis et analysés. Or, certains de ces documents étaient très volumineux et contenaient plusieurs centaines de pages.

On s'est dès lors posé la question de savoir s'il était nécessaire d'exclure intégralement le SRC du champ d'application de la LTrans. Etant donné toutefois que le SRC s'occupe aussi d'affaires purement administratives, pour lesquelles il est tout à fait possible de renseigner conformément aux principes de la LTrans, le Conseil fédéral ne propose qu'une exception matérielle pour les documents concernant la recherche d'informations relevant du renseignement.

### 4. Loi du 17 juin 2005 sur le Tribunal administratif fédéral[35]

*Art. 23, al. 2, let. b* et *art. 36b Autorisation de mesures de recherche d'informations du Service de renseignement*

La let. b est ajoutée à l'art. 23, al. 2 pour fixer la compétence du président de la cour compétente du Tribunal administratif fédéral dans le domaine de la procédure d'autorisation des mesures de recherche d'informations soumises à autorisation ainsi que de l'exploration du réseau câblé.

L'art. 36b 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 (nouveau)*

[34] RS **152.3**
[35] RS **173.32**

Le recours contre les décisions du Conseil fédéral liées à l'interdiction d'exercer une activité (art. 31) doit explicitement être prévu, car il ne figure pour l'heure pas dans l'énumération exhaustive stipulée à l'art. 33, let.b, LTAF.

## 5. Code civil[36]

*Art. 43a, al. 4, ch. 5 (nouveau)*

Grâce au complément apporté à l'art. 43a, al. 4, ch. 5, CC, le SRC a désormais accès au système Infostar (registre de l'état civil) afin d'identifier des personnes ainsi que leur lieu de séjour actuel, voire passé. Etant donné que le CC ne mentionne aucune affectation obligatoire pour les autres services autorisés d'accès, il n'y en a pas non plus pour le SRC. 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.

## 6. Code pénal[37]

*Art. 317$^{bis}$, al. 1 et 2*

Le renvoi vers la LMSI est remplacé par celui vers la loi sur le renseignement.

*Art. 365, al. 2, let. r, s, t et u (nouvelles)*

Sont désormais mentionnées ici les tâches du SRC pour l'exécution desquelles le SRC a besoin d'un accès au casier judiciaire informatisé (VOSTRA). Ces accès existent aujourd'hui déjà dans le cadre des tâches actuelles stipulées à l'art. 365, al. 2. Ils ne couvrent toutefois l'éventail des tâches du SRC que de manière rudimentaire. Il est donc justifié de compléter cette énumération dans la nouvelle législation sur le service de renseignement. On citera notamment la mention du contrôle de l'innocuité des personnes qui collaborent à des projets étrangers classifiés ou doivent avoir accès à des informations, matériaux ou installations classifiés de l'étranger (voir à cet égard l'art. 10, al. 1, let. d).

*Art. 367, al. 2, let. m (nouvelle) et al. 4*

Pour pouvoir s'acquitter des tâches qui lui sont confiées par la loi, le SRC doit avoir connaissance non seulement des condamnations prononcées mais également d'éventuelles procédures pénales en cours. D'une part, cela sert non seulement à empêcher que des activités ressortissant au renseignement se recoupent avec celles des organes de poursuites pénales mais aussi à donner des renseignements corrects lors de clarifications d'innocuité selon l'art. 10, al. 1, let. d, LRens, pour des autorités étrangères de sûreté. S'agissant de l'entente sur la transmission de renseignements se rapportant à des procédures pénales en cours, le SRC va comme auparavant se mettre en

[36] RS **210**
[37] RS **311.0**

contact avec l'autorité de poursuites pénales compétente, afin d'éviter tout impact négatif sur les enquêtes en cours.

### 7. Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[38]

Dans le domaine des accès aux systèmes d'information policiers, la LRens ne fait qu'actualiser les bases juridiques pour les accès déjà existants aujourd'hui ( art. 15 LSIP, système de recherches informatisées de police ) et ancre les possibilités de signalements pour la recherche du lieu de séjour conformément à l'art. 14 LRens.

L'accès aux données ne sera pas autorisé 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.

### 8. Loi fédérale du 3 février 1995 sur l'armée[39]

*Art. 99, al. 1$^{bis}$, 1$^{quater}$ (nouveau) et 3$^{bis}$(nouveau)*

La nouvelle disposition légale pour l'exploration radio effectuée par le service de renseignements de l'armée est ancrée dans l'art. 99, al. 1$^{bis}$. Jusqu'à présent, le renvoi correspondant dans l'art. 99, al. 1$^{bis}$, se rapportait à l'art. 4a LFRC.

L'al. 1$^{quater}$ met à la disposition du service de renseignements de l'armée les mêmes moyens d'observation depuis les airs que pour le SRC (art. 12) et reprend également ses mesures visant à protéger la sphère privée.

L'al. 3$^{bis}$ correspond à la disposition idoine de l'art. 60, al. 2, LRens.

### 9. Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[40]

*Art. 16, al. 1, let. h (nouvelle)*

L'accès en ligne par le SRC à la banque de données PISA est désormais prévu, afin que le SRC puisse identifier les menaces émanant pour la sûreté de l'armée de personnes qui appartiennent par exemple à des groupements extrémistes violents et qui sont incorporées dans l'armée. On veut ainsi empêcher que des personnes ayant des prédispositions à la violence mettent en péril la sécurité de l'armée d'une part et soient d'autre part formées par l'armée au maniement d'armes et d'explosifs ainsi qu'à l'utilisation de procédures de combat.

### 10. Loi du 21 mars 2003 sur l'énergie nucléaire[41]

[38] RS **361**
[39] RS **510.10**
[40] RS **510.91**
[41] RS **732.1**

*Art. 101, al. 3*

L'office central ATOME, dont il est question ici, est subordonné au SRC. La tâche de l'office central consiste à rechercher et à traiter des données visant à exécuter la LENu ainsi qu'à prévenir des délits et à lancer des poursuites pénales. La pratique a démontré qu'il était nécessaire d'étendre le champ d'activités de l'office central au domaine de la loi sur la radioprotection, similaire à celui de la LENu. Il est ainsi possible d'éviter des questions de délimitation sur le type de substances radioactives (matériel fissible et 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.

**11. Loi fédérale du 19 décembre 1958 sur la circulation routière**[42]

*Art. 104c, al. 5, let. c (nouvelle)*

Grâce à l'adaptation de l'art. 104c, al. 5, le SRC doit obtenir l'accès en ligne au registre des autorisations de conduire. Cet accès est nécessaire pour pouvoir vérifier les autorisations de conduire de personnes, sans lesquelles l'exécution de mesures relevant du renseignement telles que des observations ne pourrait être préparée que de manière insuffisante.

**12. Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication**[43]

*Art. 1, al. 1, let. d (nouvelle)*

Le SRC peut désormais ordonner une surveillance de la correspondance par poste et de la correspondance par télécommunication (art. 22, al. 1, let. a à d). L'exécution de ces mesures doit respecter les procédures prévues dans la LSCPT et se faire à travers l'organe compétent en la matière au sein du DFJP, à savoir le SSCPT. A cette fin, le SRC doit désormais aussi être ancré dans la LSCPT comme organe habilité à donner un tel ordre.

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

Dans ces deux dispositions, le SRC est désormais également désigné comme organe habilité à confier des missions de surveillance. Il s'agit ici de la corrélation logique avec la compétence du SRC de faire surveiller la correspondance par poste et télécommunication d'une personne, telle qu'elle est prévue à l'art. 22, al.1, let. a à d, LRens.

*Art. 14, al. 2$^{bis}$*

Le renvoi vers la LMSI a ici simplement été remplacé par celui vers la nouvelle LRens.

[42] RS **741.01**
[43] RS **780.1**

**13. Loi du 30 avril 1997 sur les télécommunications**[44]

*Art. 34, al. 1ter et 1quater (nouveau)*

Le SRC est désormais également mentionné dans cet alinéa. On crée ainsi dans la LTC le pendant juridique formel nécessaire de l'art. 5, al. 1, let. d, LRens. La coordination entre les deux lois est mise sur pied en parallèle.

**Remarque récapitulative par rapport aux chiffres 15 et suivants:**

Les actes législatifs cités ci-après n'ont subi que des adaptations formelles dans les articles se rapportant à la communication de données. A chaque fois, le renvoi vers la LMSI est remplacé par celui vers la LRens. Aucune modification n'intervient sur le plan matériel.

De plus, dans quelques lois, le renvoi introduit avec la LMSI II vers la communication de données « dans des cas d'espèce et sur demande écrite et motivée » a été supprimé. Ce renvoi s'est avéré inutile, car chaque donnée de renseignements au SRC est déjà contenue dans la disposition antéposée. Il s'ensuit dès lors une simple correction d'une méprise législative et non une modification de la situation juridique.

**14. Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants**[45]

*Art. 50a, al. 1, let. dbis et e, ch. 7*

**15. Loi fédérale du 19 juin 1959 sur l'assurance-invalidité**[46]

*Art. 66a, al. 1, let. c*

**16. Loi fédérale du 25 juin 1982 sur la prévoyance professionnelle vieillesse, survivants et invalidité**[47]

Art. 86a, al. 1, let. g, et 2, let. G

**17. Loi fédérale du 18 mars 1994 sur l'assurance-maladie**[48]

[44] RS **784.10**
[45] RS **831.10**
[46] RS **831.20**
[47] RS **831.40**
[48] RS **832.10**

*Art. 84a, al. 1, let. g^bis et h, ch. 6*

**18. Loi fédérale du 20 mars 1981 sur l'assurance-accidents**[49]

*Art. 97, al. 1, let. h^bis et i, ch. 6*

**19. Loi fédérale du 19 juin 1992 sur l'assurance militaire**[50]

*Art. 1a, al. 1, let. q (nouvelle)*

Cette disposition fait office de pendant à l'art. 32, al. 6, LRens, selon lequel les collaborateurs du SRC engagés à l'étranger sont soumis à l'assurance militaire. Cette disposition doit désormais aussi être ancrée dans la LAM comme indication de la source.

*Art. 95a, al. 1, let. h^bis et i, ch. 8*

Il s'agit ici de l'adaptation purement formelle mentionnée en guise d'introduction (remplacement du renvoi vers la LMSI par celui vers la LRens).

**20. Loi fédérale du 25 juin 1982 sur l'assurance-chômage**[51]

*Art. 97a, al. 1, let. e^bis et f, ch. 8*

[49] RS **832.20**
[50] RS **833.1**
[51] RS **837.0**

*Annexe I*

## Mesures de recherche d'informations prévues par le projet de loi sur le renseignement

| Recherche en Suisse | | | Recherche à l'étranger |
|---|---|---|---|
| But de la recherche | Mesures non soumises à autorisation selon les art. 11 ss | Mesures soumises à autorisation selon les art. 22 ss | |
| 1. Art. 4, al. 1, let. a, ch. 1 à 5:<br>→ Terrorisme<br>→ Espionnage<br>→ Prolifération<br>→ Attaques contre des infrastructures critiques | Applicable | Applicable | 1. *Mesures de recherche secrètes*<br>Condition préalable: recherche d'informations sur l'étranger importantes en termes de politique de sécurité sur la base de l'art. 4, al. 1, let. b.<br><br>2. *Exploration radio* (art.33)<br>Condition préalable: recherche d'informations sur l'étranger importantes en termes de politique de sécurité.<br><br>Les informations sur les événements se produisant en Suisse ne peuvent être transmises que si elles indiquent une menace concrète pour la sûreté intérieure (art. 33, al. 5).<br><br>3. *Exploration du réseau câblé* (art. 34 ss)<br>Dans le but de rechercher des informations sur des incidents relevant de la politique de sécurité à l'étranger et de sauvegarder des intérêts essentiels de la |
| 2. Art. 4, al. 1, let. a, ch. 6:<br>→ Extrémisme violent | Applicable | Non applicable | |

| | | | |
|---|---|---|---|
| | | | Suisse (art. 62), il est possible d'enregistrer les signaux issus de réseaux tributaires d'éléments conducteurs. |
| 3. Recherche d'informations en Suisse sur des incidents se produisant à l'étranger (art. 32, al. 2) | Applicable | Applicable. Autorisation en principe similaire à la recherche en Suisse. Exception: introduction dans des systèmes informatiques lorsque ceux-ci se trouvent à l'étranger (art. 32, al. 2). | |
| Sauvegarde d'autres intérêts essentiels de la Suisse | | | |
| Le Conseil fédéral peut, au sens de l'art. 1, al. 3 du présent projet, charger le SRC de mesures pour sauvegarder d'autres intérêts essentiels de la Suisse (art. 62). | | | |