13.064

Message concernant la modification de la loi fédérale sur le renseignement civil (LFRC)

du 14 août 2013

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

Par le présent message, nous vous soumettons le projet de modification de la loi fédérale sur le renseignement civil en vous proposant de l'adopter.

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

14 août 2013

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ueli Maurer
La chancelière de la Confédération, Corina Casanova

Condensé

Le présent projet de loi crée une base légale formelle pour l'exploitation du «Système d'information sécurité extérieure» du Service de renseignement de la Confédération.

Contexte

Le Service de renseignement de la Confédération (SRC) a été créé par le regroupement de l'ancien service de renseignement intérieur (Service d'analyse et de prévention) et du service de renseignement extérieur (Service du renseignement stratégique). Le SRC existe dans sa forme actuelle depuis le 1er janvier 2010. C'est à la même date qu'est entrée en vigueur la loi fédérale sur le renseignement civil (LFRC), adoptée par les Chambres fédérales le 3 octobre 2008. A l'époque, le législateur partait du principe que les tâches réglées dans la LFRC seraient accomplies par deux services séparés, le Service d'analyse et de prévention et le Service du renseignement stratégique.

*Après la fusion, le SRC s'est vu confronté à la situation de devoir appliquer les prescriptions de deux bases légales distinctes pour le traitement des informations. La loi fédérale instituant des mesures visant au maintien de la sûreté intérieure règle en détail le traitement des données intérieures dans le «Système d'information sécurité intérieure (ISIS)». En revanche, les dispositions de la loi fédérale sur l'armée, reprises dans la LFRC pour le traitement des données sur l'étranger, ne répondent plus aux exigences actuelles d'une base légale pour la gestion automatisée des données. Alors qu'ISIS est exploité dans sa forme actuelle depuis 2005, le Système d'information sécurité extérieure (ISAS) n'a pu être introduit que le 21 juin 2010 à titre d'essai pilote selon l'art. 17*a *de la loi fédérale sur la protection des données (LPD). Le 8 juin 2012, se fondant sur un rapport d'évaluation de l'essai, le Conseil fédéral en a autorisé la poursuite pour trois années supplémentaires, c'est-à-dire jusqu'en juin 2015. Conformément à la LPD, le traitement de données automatisé doit être interrompu dans tous les cas si aucune loi au sens formel n'est entrée en vigueur dans un délai de cinq ans à partir de la mise en œuvre de l'essai pilote (art. 17*a*, al. 5, LPD).*

Les systèmes d'information actuels seront à l'avenir réglés dans la loi sur le renseignement, en voie d'élaboration. On ne peut cependant assurer que la nouvelle loi sur le renseignement entrera déjà en vigueur en juin 2015. Il importe donc, en créant une base légale formelle dans la LFRC, de garantir que le système ISAS puisse continuer à être exploité au-delà de juin 2015 si la loi sur le renseignement n'est pas entrée en vigueur d'ici là. Comme le projet de loi prévoit des règles de contrôle de qualité plus strictes que l'exploitation pilote, mais essentiellement parce que c'est le lien entre ISIS et ISAS – tout en conservant leur séparation logique – qui permet l'appréciation globale de la situation exigée par la LFRC, une mise en vigueur aussi rapide que possible du présent projet est indiquée.

Contenu du projet

Le traitement des données dans ISAS est actuellement régi par voie d'ordonnance. Comme elle a fait ses preuves pendant la phase d'essai, les règles correspondantes doivent maintenant être ancrées dans une loi. La structure de la LFRC doit être adaptée à cet effet. Avec la création de la base légale pour ISAS, des règles sont en particulier fixées pour les aspects suivants: organe responsable et but, contenu et structure du système d'information, contrôle de la qualité, droits d'accès, transmission de données personnelles à des autorités suisses, des autorités étrangères et des tiers, droit d'accès, durée de conservation et archivage des données.

Message

1 Présentation du projet

1.1 Contexte

Le 1er janvier 2009, les unités de renseignement de l'Office fédéral de la police (fedpol) ont été transférées au Département fédéral de la défense, de la protection de la population et des sports (DDPS), puis regroupées le 1er janvier 2010 avec le Service du renseignement stratégique (SRS) en un nouvel office: le Service de renseignement de la Confédération (SRC).

La loi fédérale sur le renseignement civil (LFRC)[1], adoptée par les Chambres fédérales le 3 octobre 2008, est également entrée en vigueur le 1er janvier 2010. A l'époque de son adoption, le législateur partait du principe que les tâches de renseignement civil seraient accomplies par deux services séparés sur le plan organisationnel, le SRS et le Service d'analyse et de prévention (SAP). Chaque service aurait, dans ce cas, continué à traiter ses informations dans son propre système en se fondant sur les prescriptions correspondantes.

Après la fusion, le SRC s'est vu confronté à la situation particulière de devoir appliquer les prescriptions de deux bases légales distinctes pour le traitement de ses informations. Il s'agissait, d'une part, d'appliquer avec conséquence les dispositions restrictives de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[2], sans pour autant que la recherche de renseignements sur l'étranger s'en trouve restreinte. Le Conseil fédéral a alors décidé d'étendre les dispositions plus strictes de la LMSI au traitement de toutes les informations ayant un lien direct avec la Suisse et ses habitants. Les règles moins sévères de la LFRC concernent exclusivement les informations du SRC sur l'étranger sans lien avec la Suisse. Par conséquent, si le contenu des données du SRC comporte un lien direct avec la Suisse ou s'il ne concerne que l'étranger, ces données sont traitées dans deux systèmes d'information distincts: les données «suisses» sont traitées dans le «Système d'information sécurité intérieure» (ISIS), les données sur «l'étranger» dans le «Système d'information sécurité extérieure» (ISAS).

Alors qu'ISIS est exploité dans sa forme actuelle depuis 2005, ISAS a été introduit le 21 juin 2010 à titre d'essai pilote au sens de l'art. 17*a* de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[3].

L'art. 17*a*, LPD, contient une règle d'exception à l'obligation d'une base légale formelle pour le traitement automatisé de données sensibles ou de profils de la personnalité. Elle permet au Conseil fédéral d'autoriser un tel traitement avant l'entrée en vigueur d'une loi au sens formel si – comme c'est le cas pour ISAS – une phase d'essai est indispensable.

Conformément à l'art. 17*a*, al. 4, LPD, l'organe fédéral responsable transmet au Conseil fédéral, au plus tard deux ans après la mise en œuvre de la phase d'essai, un rapport d'évaluation dans lequel il lui propose la poursuite ou l'interruption de

1 RS **121**
2 RS **120**
3 RS **235.1**

l'essai. Le 8 juin 2012, le Conseil fédéral a approuvé ce rapport et autorisé la poursuite de l'essai pilote pour trois années supplémentaires, c'est-à-dire jusqu'en juin 2015. Si aucune loi au sens formel n'est entrée en vigueur d'ici là, le traitement des données automatisé doit être interrompu (cf. art. 17*a*, al. 5, LPD).

La loi sur le renseignement (LRens), en voie d'élaboration, prévoit un nouveau concept pour le traitement et la conservation des données, qui doit remplacer les systèmes ISIS et ISAS. Comme on ne peut pour l'instant assurer que la LRens entrera en vigueur en juin 2015, il importe de créer une base légale formelle suffisante pour que le système ISAS puisse continuer à être exploité au-delà de juin 2015 si les travaux pour la LRens devaient se prolonger au-delà de cette date. Le présent projet de modification de la LFRC tient compte, autant que faire se peut, des résultats des deux consultations des offices concernant la LRens. Cette révision partielle concerne donc exclusivement le traitement par le SRC des données sur l'étranger (c'est-à-dire les données sur l'étranger sans lien direct avec la Suisse).

1.2 Dispositif proposé

Le traitement des données dans le cadre du système pilote ISAS se fonde actuellement sur une ordonnance (voir les art. 17 à 24 de l'ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération [OSI-SRC][4]).

La révision partielle de la LFRC a pour objectif de créer la base légale nécessaire pour qu'ISAS puisse continuer à être exploité sans interruption après juin 2015 si la LRens n'est pas entrée en vigueur d'ici là. Pour la réglementation d'ISAS dans la LFRC, l'ajout de plusieurs articles est nécessaire. C'est pourquoi la structure de la LFRC doit être adaptée et nouvellement structurée en sections. Les articles relatifs à ISAS règlent en résumé les points suivants:

- Organe responsable
- But
- Contenu
- Contrôle de qualité
- Structure
- Droits d'accès
- Transmission de données personnelles
- Droit d'être informé
- Durée de conservation des données
- Archivage
- Dispositions d'exécution.

Pour les explications détaillées des articles voir ch. 2.

4 RS **121.2**

1.3 Appréciation de la solution retenue

Le rapport d'évaluation sur la phase pilote d'ISAS, approuvé par le Conseil fédéral, conclut notamment que «L'essai pilote du système ISAS a montré que les exigences fonctionnelles des utilisateurs pour leur travail d'analyse et que les conditions légales et celles posées par les pouvoirs publics peuvent être remplies. Le fonctionnement pilote du système ISAS est stable». En d'autres termes, l'essai pilote a fait ses preuves, raison pour laquelle sa prolongation pour trois années supplémentaires a été autorisée.

Les dispositions et règles correspondantes doivent maintenant être ancrées dans une loi.

Le projet de révision partielle de la LFRC comporte d'une part, pour plus de clarté, des titres de sections sans modifications quant au fond des dispositions respectives et, d'autre part, des règles pour un système d'information exclusivement exploité et géré par la Confédération. En font partie les données sur l'étranger sans lien direct avec la Suisse. Dans cette perspective, l'essai pilote en cours a notamment permis d'optimiser les prescriptions concernant le traitement des données. Lors de son évaluation, en été 2012, l'essai pilote n'a fait l'objet d'aucune critique. Le contenu essentiel de la réglementation en vigueur n'est pas modifié par la présente révision. Sur le plan chronologique, la modification de la LFRC est une réglementation de transition de durée limitée puisque, avec l'entrée en vigueur de la LRens, les dispositions qui régissent les activités du renseignement, fixées jusqu'à présent dans divers actes législatifs, dont la LFRC, devraient être abrogées. Par ailleurs, la révision proposée ne touche ni la recherche d'informations à l'étranger ni leur utilisation par le SRC; n'est en effet réglé «que» le traitement de ces données par le SRC. Une certaine urgence s'impose dans la mesure où la révision partielle doit être entrée en vigueur au plus tard à la fin de l'essai pilote et que d'ici là, les adaptations des ordonnances et directives respectives doivent également être approuvées.

Dans le cadre du concept global de la nouvelle loi sur le renseignement en voie d'élaboration, la présente révision de la LFRC a caractère de réglementation transitoire et constitue de ce fait un projet de portée secondaire, principalement parce qu'ISAS est un système d'information exclusivement exploité et alimenté par la Confédération (sans implication directe des cantons). Comme une procédure de consultation n'aurait pas apporté de nouveaux éléments sur la pertinence quant au fond, la capacité d'exécution ou l'acceptation du projet, le choix s'est porté sur une procédure d'audition. A ce sujet, il faut également prendre en compte le fait que tous les milieux intéressés, dans le cadre de la consultation relative à la LRens, ont pu s'exprimer sur les futures règles définitives.

La procédure d'audition a été ouverte par le DDPS le 27 février 2013 et elle s'est achevée le 31 mai 2013. Au total, 24 services ont été approchés. Le DDPS a reçu 15 réponses, dont cinq renonçant explicitement à une prise de position.

Le PDC et le PRD soutiennent la révision de la loi. L'UDC, qui la soutient aussi, exprime toutefois des réserves par rapport la Convention européenne des droits de l'homme. Le PS salue la création d'une base légale et fait diverses propositions de modifications de caractère matériel.

La Conférence des directrices et directeurs des départements cantonaux de justice et police salue la création d'une base légale pour l'exploitation d'ISAS.

L'Union suisse des arts et métiers refuse le projet tant qu'un lien existe entre les banques de données ISIS et ISAS et tant que les données sont soumises à la loi sur la transparence. Elle demande que les termes «intérieur» et «étranger» soient clarifiés. Le Centre Patronal et la Chambre vaudoise des arts et métiers soutiennent la révision à condition que les dispositions modifiées n'entrent pas en vigueur avant juin 2015.

Privatim salue le fait qu'une base légale formelle soit créée pour ISAS avant l'achèvement de sa phase pilote et souligne que le projet tient compte des exigences élevées de réglementation et des critères pour la délégation au Conseil fédéral des compétences d'édicter des règles de droit.

Le Comité du «Référendum contre la modification de la LMSI» oppose un refus catégorique au projet et part du principe que l'exploitation pilote pourra être arrêtée fin juin 2015 sans modification de la loi.

L'avant-projet de modification a été révisé. Les principaux changements apportés par rapport à l'avant-projet ayant fait l'objet de la procédure d'audition sont les suivants:

- Contenu: limitation explicite au but assigné et reformulation concernant la réglementation pour le traitement de fausses informations;
- Contrôle de la qualité: application des standards de contrôle de qualité d'ISIS pour la vérification des données saisies à double dans ISAS et ISIS;
- Droits d'accès: ouverture de l'accès à l'index pour les services de la Confédération chargés de procéder aux contrôles de sécurité relatifs aux personnes;
- Transmissions de données personnelles à des autorités étrangères: transmission supplémentaire de données en vue d'empêcher ou d'élucider un délit également punissable en Suisse;
- Archivage: limitation de la consultation de données personnelles après leur archivage à des cas où il s'agit de sauvegarder un intérêt public ou privé prépondérant ou d'évaluer une menace pour la sécurité intérieure et extérieure de la Suisse;
- Dispositions d'exécution: fixation du catalogue des données personnelles sensibles qui peuvent être traitées.

1.4 Comparaison avec le droit étranger, notamment européen

Dans le cadre des travaux préparatoires pour la LRens, le Center for Security Studies de l'EPF de Zurich a publié en septembre 2011 un rapport global sur les systèmes de renseignement civil dans l'entourage européen de la Suisse[5]. Ce rapport contient en particulier une comparaison entre un certain nombre de services de renseignement civil intérieurs et extérieurs regroupés ou distincts.

En Europe, les Pays-Bas, l'Espagne, le Luxembourg et la Slovénie disposent chacun d'un service de renseignement civil qui – à l'instar de la Suisse – est compétent pour l'intérieur et pour l'étranger. Les services de ces quatre pays collaborent avec les

5 Ce rapport peut être consulté sous: www.css.ethz.ch > Think-Tank > Schweiz: Produkte

autorités de police du pays et avec des services de renseignement et de sûreté étrangers.

Ces quatre services regroupés sont compétents pour le service de renseignement intérieur et extérieur. Leurs tâches comportent en particulier la recherche d'informations sur l'étranger importantes pour le pays du point de vue stratégique, politique et économique. Dans le cas des Pays-Bas et de la Slovénie, la gestion des données personnelles et des droits des personnes concernées sont réglés dans une loi sur le service de renseignement. L'Espagne ne semble pas disposer d'une réglementation spécifique pour la protection des données en relation avec le service de renseignement. Au Luxembourg, selon la loi sur le renseignement, le service de renseignement de l'Etat est soumis aux dispositions habituelles sur la protection des données, qui autorisent toutefois certaines exceptions pour la gestion de données personnelles dans l'intérêt de la sûreté nationale.

1.5 Mise en œuvre

La révision partielle de la LFRC proposée dans le présent projet peut entièrement être appliquée dans les structures du SRC en place.

2 Commentaire des dispositions

Les exigences de la réglementation légale pour l'exploitation d'un système automatisé de traitement de données personnelles sont élevées (voir le Guide pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles de l'Office fédéral de la justice[6]), ce qui aboutit ici à une série de 13 nouveaux articles contenant des règles très détaillées pour le système d'information «ISAS». La révision de la LFRC offre par ailleurs l'occasion d'en adapter la structure. Sur le plan matériel, seule la section 5 (Système d'information sécurité extérieure) contient de nouveaux articles, les autres sections reprennent les dispositions en vigueur. Dorénavant, la LFRC comportera les huit nouveaux titres de sections suivants:

Section 1:	Missions et organisation
Section 2:	Collaboration
Section 3:	Traitement des données personnelles
Section 4:	Traitement des données personnelles collectées en vertu de la LMSI
Section 5:	Système d'information pour la sécurité extérieure
Section 6:	Protection des sources, indemnisation et primes
Section 7:	Contrôle
Section 8:	Dispositions finales

6 www.bj.admin.ch > Themen > Staat & Bürger > Legistik > Andere Hilfsmittel

Explications relatives aux nouveaux articles

Art. 6a Organe responsable

Al. 1

Pour accomplir son mandat et ses tâches légales conformément à l'art. 1, let. a, LFRC, le SRC doit pouvoir traiter des informations importantes sur l'étranger à l'aide de moyens électroniques. Ce traitement est effectué depuis le 21 juin 2010 par un cercle limité d'utilisateurs dans le cadre de l'essai pilote d'ISAS et se fonde sur l'art. 17*a* de la LPD.

Al. 2

C'est le SRC qui est le maître du ficher. Il est responsable du respect des prescriptions relatives à la protection des données, du traitement des demandes d'accès et de rectification des informations, de l'accomplissement des tâches de contrôle et de la garantie de la sécurité informatique.

Art. 6b But

Al. 1

Sont traitées dans ISAS des informations importantes sur l'étranger en matière de politique de sécurité. On entend par là des événements et des développements à l'étranger susceptibles de mettre en danger l'autodétermination de la Suisse, ses bases démocratiques et d'Etat de droit ainsi que de causer dommages directement liés à la sécurité du pays ou encore d'entraver la capacité d'agir de ses autorités.

Al. 2

Les informations importantes sur l'étranger en matière de politique de sécurité sont enregistrées et traitées dans ISAS. Elles sont en priorité analysées à l'attention des départements fédéraux et du Conseil fédéral dans le but de pouvoir leur fournir une appréciation globale de la situation de la menace. Mais ISAS sert aussi à la documentation et à la gestion de dossiers contenants des informations importantes sur l'étranger en matière de politique de sécurité.

Art. 6c Contenu

Al. 1

Sont traitées dans ISAS des informations qui permettent d'identifier des personnes, des entreprises, des organisations et des institutions, par exemple des noms, prénoms, dates de naissance, adresses, nationalités, lieux d'origine, numéros de téléphones, entreprises et leur siège. Sont aussi saisies des informations importantes du point de vue de la politique de sécurité, en particulier des données sur des événements survenus à l'étranger significatifs pour la situation, tels que des lieux, des dates, des actes et des personnes, des organisations et des institutions impliquées. Peuvent être enregistrées dans ISAS des données sous forme de textes, d'images, de vidéos, de documents sonores ou d'autres formats appropriés ou qui combinent ces éléments.

Les saisies à double doivent rester l'exception. Le principe de base selon lequel un état de faits doit être enregistré exclusivement soit dans le système d'information ISAS ou dans celui d'ISIS demeure ainsi inchangé. La justification qu'une information ne peut pas être séparée doit ressortir soit de l'annonce elle-même soit être documentée par le SRC.

Al. 2

Des données sensibles peuvent être traitées dans ISAS. Pour accomplir ses tâches, le SRC peut en effet être tributaire de telles informations, par exemple pour la saisie de données sur l'appartenance religieuse lors d'actes terroristes commis pour des motifs religieux.

Al. 3

Cet alinéa précise que seules pourront être traitées des informations répondant aux buts prévus par la loi.

Al. 4

En dérogation aux dispositions ordinaires sur la protection des données, le SRC doit aussi pouvoir traiter et conserver des données reconnues comme inexactes. Lors de l'évaluation d'informations provenant d'activités de renseignement, il s'agit aussi de pouvoir reconnaître des données relevant de la désinformation ou de fausses informations. De telles informations permettent de connaître les intentions d'un producteur ou d'un fournisseur d'informations. Des données relevant de la désinformation ou de fausses informations doivent rester disponibles pour ne pas provoquer d'appréciations erronées par la suite. De plus, dans le cadre de la collaboration internationale, il doit également être possible d'accéder à de fausses informations pour pouvoir évaluer un éventuel futur colportage de fausses informations (par ex. identification erronée d'une personne comme membre d'un groupe terroriste) et éventuellement y réagir. Par ailleurs, les données reconnues comme inexactes peuvent être précieuses pour évaluer la fiabilité ou les intentions d'une source humaine ou d'un service partenaire.

Art. 6d Contrôle de qualité

Al. 1

Le processus d'évaluation des informations entrantes comporte un examen de la pertinence et de l'exactitude des données communiquées, c'est-à-dire un examen déterminant si l'annonce est importante pour l'accomplissement des tâches légales confiées au SRC et si elle est exacte. Les communications qui sont saisies dans le système de classement des dossiers sont évaluées dans leur globalité.

Al. 2

La fréquence des contrôles de qualité est fixée par le Conseil fédéral.

Al. 5

Divers rapports des organes de surveillance ont montré à quel point un contrôle périodique fiable est important pour la qualité des données du SRC. La mise en place d'un service interne de contrôle de la qualité des données dans ISIS a fait ses preuves et doit être ancré dans la loi. Des formations internes doivent aussi être organisées pour garantir la qualité et la pertinence des informations traitées dans

ISAS et des contrôles réguliers garantir la qualité et la pertinence des informations traitées dans ISAS.

Art. 6e Structure

Al. 1

ISAS comporte trois systèmes: un système de classement des dossiers, où les informations importantes sur l'étranger du point de vue de la politique de sécurité recherchées par le SRC ou communiquées au SRC sont numérisées et enregistrées, un système d'analyse des données et de suivi de la situation, avec un accès aux informations enregistrées dans les dossiers, où ces informations sont classées par objets, par relations et par communications et étoffées de métadonnées, et d'un index donnant accès aux objets du système d'analyse et de suivi de la situation qui peut être consulté par les autorités externes disposant d'un droit d'accès (voir les explications ci-après concernant l'art. 6*f*).

Al. 2

Le SRC traite aussi bien des informations importantes du point de vue de la politique de sécurité ayant un lien avec la Suisse (ISIS) que des informations qui ont un lien avec l'étranger (ISAS). Compte tenu des dispositions différentes qui régissent la gestion des informations contenues dans ces deux systèmes, ils continueront à être exploités séparément. Pour que le SRC puisse procéder à une analyse globale de la menace (voir art. 3, al. 1, LFRC), il doit toutefois pouvoir accéder rapidement à tous les systèmes contenant des informations importantes pour l'accomplissement de ses tâches. Cette possibilité de consultation simultanée des deux systèmes en vue de l'analyse et de l'appréciation globale de la situation est aujourd'hui déjà fixée à l'art. 6 OSI-SRC. Dans ce cas, les utilisateurs ne peuvent consulter que les informations concernant une personne, une organisation ou un événement qu'ils auraient également obtenues par une consultation séparée des systèmes d'information.

Art. 6f Droits d'accès

Al. 1

Pendant la phase pilote d'ISAS, le cercle des utilisateurs était limité à un petit nombre de personnes, suffisant toutefois pour réaliser le test. Avec l'achèvement de cette phase et l'introduction du système d'information ISAS, cette restriction peut être levée et le cercle des utilisateurs étendu à tous les collaborateurs du SRC chargés de la saisie, de la recherche, de l'analyse et du contrôle de qualité des données qui doivent pouvoir y accéder pour accomplir leurs tâches légales. Le cercle interne des utilisateurs du SRC va de ce fait s'agrandir et sera pratiquement identique à celui des utilisateurs d'ISIS.

Al. 2

Pour que les collaborateurs du SRC puissent procéder à une recherche intersystèmes ISAS-ISIS (voir les explications ci-dessus concernant l'art. 6*e*, al. 2), ils doivent disposer des droits d'accès pour les deux systèmes. Le résultat de la recherche ne contient que les informations qui auraient aussi été obtenues par la consultation séparée d'ISIS ou d'ISAS.

Al. 3

Les utilisateurs externes, c'est-à-dire l'Office fédéral de la police, les organes de sûreté des cantons ainsi que les services de la Confédération chargés de procéder aux contrôles de sécurité relatifs aux personnes, n'ont accès qu'à l'index.

Art. 6g Transmission de données personnelles à des autorités suisses

Pour que le SRC puisse remplir son mandat, il doit pouvoir transmettre des données personnelles à des autorités suisses (par ex. des autorités de poursuite pénale, de justice et de sécurité). Le Conseil fédéral détermine quelles sont ces autorités.

Pour le reste, les secrets professionnels lors du traitement des données sont gardés comme jusqu'à tant en Suisse qu'à l'étranger.

Art. 6h Transmission de données personnelles à des autorités étrangères

Cet article reprend dans une large mesure les dispositions de l'art. 17, al. 3 et 4, LMSI, qui ont fait leur preuve. La LPD prévoit que des données personnelles ne peuvent être communiquées en règle qu'à des Etats qui en garantissent une protection de niveau comparable à celui de la Suisse (art. 6, al. 1). Cette règle exclurait une collaboration du SRC avec la plupart des pays extra-européens si les exceptions restrictives de l'art. 6, al. 2, LPD, ne pouvaient de cas en cas être appliquées, faute de quoi le SRC serait dans l'impossibilité d'accéder à d'importantes sources d'informations, en particulier dans des régions en crise.

Concernant la collaboration avec des services de renseignement à l'étranger (y compris la transmission de données personnelles), il existe une pratique de longue date, accompagnée et contrôlée par les organes de surveillance (Surveillance des services de renseignement du DDPS, anciennement rattachée au DFJP, et Délégation des Commissions de gestion des Chambres fédérales).

L'al. 2, let. a, permet par exemple d'échanger à titre préventif des informations en lien avec un appel public d'incitation au crime ou à commettre des actes de violence (par ex. prédicateurs incitant à la haine).

L'al. 2, let. d, concerne les demandes de conformité ou de *clearing* en faveur de personnes qui doivent pouvoir accéder à l'étranger à des projets, des informations, des installations, etc. classifiés. Ces renseignements sont en général dans l'intérêt de la personne concernée qui, sans ces informations, ne pourrait pas prendre un emploi ou entreprendre une activité commerciale.

Dans ce contexte, les exigences de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)[7] doivent également être respectées.

Art. 6i Transmission de données personnelles à des tiers

Les activités de renseignement impliquent parfois la nécessité de communiquer des données à des particuliers. Le cas le plus fréquent est de motiver une demande de renseignement: lorsqu'il veut obtenir des informations sur des personnes physiques

7 RS **0.101**

ou morales, le SRC doit pouvoir dire à la personne interrogée sur quelle personne il souhaite obtenir des informations et dans quel contexte.

Art. 6j Droit d'accès

Le droit d'accès se fonde sur les art. 8 et 9 de la LPD (droit direct d'être informé).

Art. 6k Durée de conservation des données

La compétence de fixer la durée de conservation des données dans ISAS est déléguée au Conseil fédéral. Si le contrôle de qualité interne conclut que des données ne sont plus nécessaires, il les détruit immédiatement.

Art. 6l Archivage

Al. 2

Dans certains cas particuliers et de façon analogue aux autorités de poursuite pénale, le SRC, en tant qu'autorité ayant versé des documents aux Archives fédérales, doit pouvoir consulter des données personnelles dans les documents remis. Comme cette possibilité n'est pas prise en compte dans la législation concernant l'archivage, cette disposition a caractère de *lex specialis*.

3 Conséquences

Dans l'ensemble, il faut partir d'un niveau de sécurité accru. Les modifications proposées ne créent toutefois pas de nouvelles tâches. Elles n'ont pas d'effets directs sur les finances et les effectifs du personnel de la Confédération. Le projet n'a aucune conséquence pour les cantons et les communes (ou centres urbains, agglomérations ou régions de montagne), l'économie publique, la société ou l'environnement.

4 les stratégies nationales du Conseil fédéral

Le projet n'a été annoncé ni dans le message du 25 janvier 2012 sur le programme de la législature 2011 à 2015[8] ni dans l'arrêté fédéral du 15 juin 2012 sur le programme de la législature 2011 à 2015[9]. La LRens, annoncée dans le programme de la législature 2011 à 2015, remplacera toutefois le LFRC (et la LMSI) et créera simultanément une nouvelle base légale formelle pour le traitement des données par le SRC.

8 FF **2012** 349
9 FF **2012** 6667

5 Aspects juridiques

5.1 Constitutionnalité et légalité

La LFRC se fonde sur les art. 54, al. 1, et 173, al. 2, de la Constitution (Cst.)[10]. L'art. 54, al. 1, Cst., accorde une compétence générale à la Confédération dans le domaine des affaires étrangères. Celle-ci est donc habilitée à régler les activités de renseignement sur et à l'étranger. L'art. 173, al. 2, Cst. dispose que l'Assemblée fédérale est compétente pour tous les objets qui ne ressortissent pas à une autre autorité fédérale. C'est dans ce cadre-là que se situe la présente révision partielle; elle ne va pas au-delà du domaine d'activité fixé à l'art. 1 LFRC.

Le présent projet concerne le traitement en Suisse de données sur l'étranger, raison pour laquelle le respect des droits constitutionnels doit être garanti.

Les modifications proposées sont susceptibles de porter atteinte aux droits fondamentaux, tout particulièrement à la sphère privée (art. 13, Cst.). En tant qu'élément de la sphère privée, l'autodétermination en matière d'information (art. 13, al. 2, Cst.) protège en particulier toute personne contre le traitementde données la concernant (comparer ATF *122* I 360, dans lequel le Tribunal fédéral déduit ce droit à l'autodétermination en matière d'information du droit fondamental non écrit de la liberté personnelle).

Conformément à l'art. 36, Cst., toute restriction d'un droit fondamental doit être fondée sur une base légale, être justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui et répondre au principe de la proportionnalité. De plus, l'essence des droits fondamentaux est inviolable.

Afin de garantir l'exploitation d'ISAS sans délai d'échéance, les dispositions correspondantes doivent formellement être ancrées dans une loi, c'est-à-dire dans la LFRC. La recherche des données enregistrées dans ISAS ainsi que leur traitement se fondent sur la LFRC et concernent des informations importantes sur l'étranger en matière de politique de sécurité.

L'intérêt public pour la recherche et le traitement des données est évident puisqu'il s'agit de la protection de la sûreté intérieure et extérieure.

Pour évaluer la proportionnalité d'une règlementation, il convient d'examiner si elle est appropriée et nécessaire et si elle se justifie raisonnablement par rapport au but visé. La mesure relative au traitement et à la conservation d'informations importantes sur l'étranger en matière de politique de sécurité est appropriée pour assurer la protection de la sûreté intérieure et extérieure. Le principe de la nécessité est également incontestable puisqu'aucun moyen moins incisif n'est à disposition pour la détection précoce de dangers potentiels pour la sécurité intérieure et extérieure.

Pour tenir compte du principe de la proportionnalité, un contrôle interne de la qualité examine la pertinence et l'exactitude des données lors de leur saisie dans ISAS. Lors d'une évaluation périodique, la nécessité des données enregistrées pour l'accomplissement des tâches est examinée, les données qui ne sont plus nécessaires sont supprimées. De plus, les droits d'accès aux données font l'objet de règles strictes et leur durée de conservation sera limitée par le Conseil fédéral.

10 RS **101**

La réglementation proposée est conforme à la Constitution; les principes de l'Etat de droit sont pleinement préservés.

5.2 Compatibilité avec les obligations internationales de la Suisse

L'essence des droits de l'homme concernés, les droits de l'homme de la CEDH qui ne souffrent aucune dérogation ainsi que les droits concernés consacrés par les pactes relatifs aux droits de l'homme de l'ONU sont respectés.

Le droit de chaque personne à ce que les données la concernant ne soient ni enregistrées ni utilisées, c'est-à-dire traitées, doit être considéré comme un élément du droit au respect de la vie privée (art. 8, CEDH). Des restrictions doivent correspondre aux conditions de l'art. 8, al. 2, CEDH; une base légale dans le droit national pouvant justifier une ingérence, un but légitime et une nécessité dans une société démocratique.

Les ingérences ne sont justifiées que si elles sont prévues par la loi. La Cour européenne des droits de l'homme reconnaît une loi au sens matériel si elle est formulée de manière précise et qu'elle est suffisamment accessible aux citoyens. Le présent projet a pour objet de créer une base légale formelle qui réponde à l'exigence de règles précises, puisque la réglementation sur le but du traitement des données et sur le contenu du système de traitement des données permet à chaque citoyen d'être informé de façon suffisante des conditions dans lesquelles le SRC traite les données. L'exigence de l'accessibilité ne doit pas être examinée plus avant puisque toutes les lois fédérales sont publiées dans le Recueil officiel du droit fédéral (RO) et que toute personne peut, de ce fait, y accéder.

Une autre condition pour la licéité d'une ingérence est qu'elle poursuive un but légitime. Comme but légitime pour justifier une ingérence dans le domaine protégé par l'art. 8, al. 1, CEDH, le ch. 2 cite notamment la sécurité nationale et la sûreté publique. Pour protéger la sécurité nationale, il peut être indispensable de traiter des données sur l'identité de personnes physique et morales et d'organisations.

En plus d'un but légitime, l'ingérence doit être «nécessaire dans une société démocratique». C'est sur cette formulation précisément que se fonde le principe de la proportionnalité et on peut donc renvoyer à ce qui a été mentionné au ch. 5.1.

La révision proposée répond aux exigences d'une loi quant au fond, les mesures prévues constituent un but légitime en vue du maintien de la sûreté intérieure et extérieure de la Suisse et elles sont nécessaires dans une société démocratique. L'extrait d'un arrêté du Tribunal fédéral[11] précise à ce sujet que la Cour a estimé que la surveillance secrète de personnes ainsi que la gestion secrète de fiches les concernant était compatible, sous certaines conditions, avec l'art. 8 CEDH: *«Unter solchen Voraussetzungen, bei genauer Prüfung der tatsächlichen Gegebenheiten und mit Blick auf die konkrete Ausgestaltung der Regelung hat der Gerichtshof sowohl die geheime Überwachung von Personen als auch das geheime Anlegen, Aufbewahren und Verwenden von Fichen über Personen in unterschiedlichen Konstellationen als mit der Garantie von Art. 8 EMRK im Einklang befunden [...].»*

11 ATF **138** I 6

Le présent projet ne modifie en rien les bases pour la recherche d'informations à l'étranger. Il ne concerne que la gestion de données déjà enregistrées. Tant que certains critères sont respectés, la recherche d'informations à l'étranger, dans la pratique des Etats, n'est en principe pas considérée comme acte contraire au droit international. Le suivi du traitement des données sur l'étranger dans une banque de données n'est pas non plus interdit par le droit international si les dispositions mentionnées relatives aux droit de l'homme sont respectées.

5.3 Forme de l'acte à adopter

Les actes législatifs de l'Assemblée fédérale doivent prendre la forme d'une loi fédérale ou d'une ordonnance. Le présent texte législatif contient des dispositions qui fixent des restrictions de droits constitutionnels et de droits et obligations de particuliers; il doit donc être édicté sous forme d'une loi fédérale.

5.4 Délégation de compétences législatives

La loi contient des normes de délégation au Conseil fédéral et au DDPS.

Une délégation au Conseil fédéral intervient en rapport avec le catalogue des données sensibles qui peuvent être traitées, les compétences pour le traitement des données, les droits d'accès, la fréquence du contrôle de qualité, la durée de conservation et la destruction des données, les dispositions concernant la sécurité des données, le cercle des destinataires lors de la transmission de données à des autorités suisses ainsi que l'archivage ou la destruction des données. Cette délégation est nécessaire car elle concerne des règles dont le degré de concrétisation dépasserait le cadre législatif.

La délégation au DDPS concerne uniquement la réglementation relative aux champs de données.

5.5 Conformité à la législation sur la protection des données

La présente révision partielle répond aux exigences en matière de protection des données d'une base légale formelle pour la banque de données ISAS.