



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense, de la
protection de la population et des sports DDPS

Service de renseignement de la Confédération SRC

CH-3003 Berne SRC

Berne, le 27 février 2013

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

1 Présentation du projet

1.1 Situation initiale

Le 1^{er} 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 1^{er} janvier 2010 avec le Service du renseignement stratégique en un nouvel office: le Service de renseignement de la Confédération (SRC).

La loi fédérale sur le renseignement civil (LFRC; RS 121), après avoir été adoptée par les Chambres fédérales le 3 octobre 2008, est également entrée en vigueur le 1^{er} janvier 2010. A l'époque, le législateur partait du principe que les tâches de renseignement civil seraient accomplies par deux services séparés sur le plan organisationnel, le Service du renseignement stratégique (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 dispositions correspondantes.

Après cette fusion, le SRC s'est retrouvé dans 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 LMSI 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 au titre d'essai pilote au sens de l'art. 17a de la loi fédérale du 19 juin 1992 sur la protection des données¹ (LPD).

L'article 17a, LPD, prévoit une exception à l'obligation d'une base légale formelle pour le traitement automatisé de données personnelles particulièrement sensibles ou de profils de la personnalité. Cette disposition permet au Conseil fédéral d'autoriser un tel traitement avant l'entrée en vigueur d'une loi au sens formel si – comme cela est le cas pour ISAS – des mesures techniques doivent être prises pour un traitement spécifique ou qu'une phase d'essai est indispensable pour un système informatique.

Conformément à l'art. 17a, al. 4, LPD, l'organe fédéral responsable transmet un rapport d'évaluation au Conseil fédéral au plus tard deux ans après la mise en œuvre de la phase d'essai. Dans ce rapport, il lui propose la poursuite ou l'interruption de 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, jusqu'en juin 2015. Si

¹ RS 235.1

aucune loi au sens formel n'est entrée en vigueur d'ici-là, le traitement des données automatisé doit être interrompu (cf. art. 17a, al. 5, LPD).

La nouvelle loi sur le renseignement (LRens), en voie d'élaboration, prévoit de remplacer les systèmes ISIS et ISAS par un nouveau concept pour le traitement et la conservation des données. Comme on ne peut pour l'instant assurer que cette loi entre 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 nouvelle loi devaient se prolonger. Le présent projet tient cependant compte en substance des résultats des deux procédures de consultation des offices de la LRens. Par rapport à la LRens, le projet ne comporte pas de modifications aux dispositions de la LMSI. La révision concerne exclusivement le traitement des données du SRC sur l'étranger (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 Confédération² [OSI-SRC]).

La révision partielle de la LFRC a pour objectif de créer la base légale nécessaire pour qu'ISAS puisse continuer à être exploité après juin 2015 si la nouvelle loi sur le renseignement n'est pas entrée en vigueur d'ici-là. Le projet de révision offre par ailleurs l'occasion d'adapter pour plus de clarté la structure de la LFRC par l'ajout de huit nouveaux titres de sections, sans rien modifier quant au fond (Tâches et organisation; Collaboration; Traitement de données personnelles; Traitement de données personnelles collectées en vertu de la LMSI; Système d'information sécurité extérieure; Protection des sources, indemnisation et primes; Contrôle; Disposition finales).

Pour créer la base légale formelle pour le système d'information ISAS, il est prévu d'ajouter les dispositions suivantes dans la nouvelle section correspondante (pour l'explication détaillée des articles, voir ci-après le chiffre 2):

- Organe responsable (SRC);
- But (traitement d'informations importantes sur l'étranger en matière de politique de sécurité);
- Contenu (données personnelles, particulièrement dignes d'être protégées ou non, et profils de la personnalité);
- Contrôle de la qualité (examen de l'exactitude et de la pertinence des données);
- Structure (système de classement des dossiers, système d'analyse et de suivi de la situation, index, resp. liens avec ISIS);
- Droits d'accès (collaborateurs du SRC pour le traitement d'informations importantes sur l'étranger en matière de politique de sécurité, Office fédé-

² RS 121.2

ral de la police et services cantonaux de la protection de l'Etat chargés du maintien de la sûreté de la Suisse);

- Transmission de données personnelles à des autorités suisses (pour l'accomplissement de leurs tâches selon la LFRC);
- Transmission de données à des autorités étrangères (pour la sauvegarde des intérêts de la personne concernées ou d'intérêts importants de la Suisse ou du pays destinataire en matière de sécurité);
- Transmission de données personnelles à des tiers (pour la sauvegarde des intérêts de la personne concernée ou pour détourner un grave danger imminent, resp. pour justifier une demande de renseignement);
- Droit d'être informé (droit direct d'être informé conformément aux art. 8 et 9, LPD);
- Délai de conservation (aussi longtemps que nécessaire ou durée maximale conformément au délai fixé par le Conseil fédéral);
- Archivage (Archives fédérales, SRC);
- Dispositions d'exécution (Conseil fédéral: la compétence pour le traitement des données, les droits d'accès, le rythme du contrôle de qualité, la durée de conservation des données, la suppression des données et les dispositions pour la sécurité des données; DDPS: les champs de données).

2 **Commentaires concernant les divers articles**

Les exigences des bases légales nécessaires pour exploiter un système de traitement automatisé 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 justice³), ce qui aboutit ici à une série de 14 nouveaux articles contenant des règles très détaillées pour le système d'information « Sécurité extérieure ISAS ». La révision de la LFRC offre par ailleurs l'occasion d'en adapter la structure pour la rendre plus claire en y ajoutant huit nouveaux titres de sections. Quant au fond, seule la section 5 (Système d'information sécurité extérieure) contient de nouveaux articles, les autres sections reprenant les dispositions en vigueur. Dorénavant, la LFRC comportera les huit nouveaux titres de sections suivants:

Section 1 (nouveau): Tâches et organisation

Section 2 (nouveau): Collaboration

Section 3 (nouveau): Traitement des données personnelles

Section 4 (nouveau): Traitement des données personnelles collectées en vertu de la LMSI

Section 5 (nouveau): Système d'information sécurité extérieure

Section 6 (nouveau): Protection des sources, indemnisation et primes

³ <http://www.ejpd.admin.ch/content/dam/data/staat_buerger/legistik/leitf-rechtsgrundlagen-f.pdf>

Section 7 (nouveau): Contrôle

Section 8 (nouveau): Dispositions finales

Section 5 (nouveau): Système d'information sécurité extérieure (ISAS)

Art. 6a (nouveau) Organe responsable

Al. 1

Pour accomplir son mandat et ses tâches légales conformément à l'art. 1, let. a, le SRC doit pouvoir traiter des informations importantes sur l'étranger à l'aide de moyens électroniques. Cette possibilité est conférée depuis le 21 juin 2010 à un cercle limité d'utilisateurs dans le cadre de l'essai pilote d'ISAS et elle se fonde sur l'art. 17a de la loi fédérale sur la protection des données (LPD; RS 235.1). Avec l'entrée en vigueur de la présente base légale, le cercle des utilisateurs doit être étendu à toutes les personnes qui doivent pouvoir accéder à ISAS pour accomplir leurs tâches (voir les explications ci-après concernant l'art. 6f).

Al. 2

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

Art. 6b (nouveau) But

Al. 1

Dans ISAS sont gérées des informations importantes sur l'étranger en matière de politique de sécurité. On entend par « informations importantes sur l'étranger en matière de politique de sécurité » 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 des dommages économiques ou d'autres dommages ou encore d'entraver la capacité d'agir de ses autorités. Les informations qui comportent un lien direct avec la Suisse sont traitées dans le Système d'information sécurité intérieure (ISIS).

Al. 2

Les informations importantes sur l'étranger en matière de politique de sécurité sont enregistrées et traitées dans ISAS. Elles sont analysées en priorité à l'attention des départements fédéraux et du Conseil fédéral afin 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 basés sur des informations importantes sur l'étranger en matière de politique de sécurité.

Art. 6c (nouveau) Contenu

Al. 1

Sont enregistrées dans ISAS des informations qui permettent d'identifier des personnes, des entreprises, des organisations et des institutions, telles que noms, pré-

noms, dates de naissance, adresses, nationalités, lieux d'origine, numéros de téléphones, entreprises et sièges d'entreprises. Sont aussi enregistrées 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, telles que des lieux, des dates, des actes, des personnes, des organisations et des institutions impliquées. Les données dans ISAS peuvent être enregistrées sous la forme de textes, d'images, de sons ou sous une forme combinant ces éléments.

Al. 2

Comme dans ISIS, les données sensibles et les profils de la personnalité enregistrés dans ISAS sont traités conformément aux prescriptions de la LPD. Pour accomplir ses tâches, le SRC doit pouvoir traiter des données personnelles particulièrement dignes d'être protégées, par exemple sur l'appartenance religieuse de terroristes motivés par une idéologie fondamentaliste. Le SRC établit et traite aussi des profils de la personnalité, par exemple pour évaluer la menace émanant d'auteurs isolés ou de groupes extrémistes violents.

Al. 3

Contrairement aux prescriptions habituelles en matière de protection des données, le SRC doit aussi pouvoir conserver les données reconnues comme incorrectes et exploitées comme telles. Concernant 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'une source humaine ou d'un service partenaire.

Art. 6d (nouveau) Contrôle de la qualité

Al. 1

L'al. 1 définit l'appréciation des données à laquelle le SRC procède avant leur saisie dans ISAS. Cette vérification porte sur la pertinence et l'exactitude des données, c'est-à-dire si l'annonce est en lien avec les tâches légales du SRC (art. 1) et si elle ne doit pas, de toute évidence, être considérée comme erronée. Dans le classement des dossiers, cet examen n'est pas effectué pour les données personnelles individuelles d'une annonce, mais pour l'annonce dans sa globalité.

Al. 2

Le SRC vérifie régulièrement les données enregistrées dans ISAS. Les données qui ne lui sont plus nécessaires pour l'accomplissement de ses tâches sont supprimées et archivées conformément aux dispositions des Archives fédérales (art. 6I).

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. Comme pour ISIS, des formations internes devront régulièrement être organisées pour garantir la qualité et la pertinence des informations traitées dans ISAS. La fréquence des contrôles doit être fixée par le Conseil fédéral (voir art. 6m, al. 1, let. c). Bien qu'ISAS ne contienne que des informations importantes en matière de politique de sécurité ayant un lien avec l'étranger, il est concevable que le système d'analyse et de suivi de la situation contienne aussi des informations sur des personnes physiques ou morales ayant leur domicile en Suisse (par ex. dans le domaine de la prolifération en relation avec des exportations). Dans ce cas, les informations enregistrées porteront une mention spéciale et seront soumises aux règles plus restrictives des prescriptions pour le traitement des données de la LMSI, c'est-à-dire assujetties au contrôle de saisie et à l'appréciation globale périodique selon l'art. 29, al. 5, OSI-SRC (voir aussi l'art. 32, OSI-SRC), et cela pour répondre à la volonté du législateur de soumettre le traitement des données sur des Suisses à un régime plus sévère.

Art. 6e (nouveau) Structure

Al. 1

ISAS comporte trois systèmes: un système de classement des dossiers, dans lequel 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 où elles sont 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. 6f).

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), il doit 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 un accès séparé aux systèmes concernés.

Al. 1

Comme nous l'avons mentionné (voir les explications concernant l'art. 6a, al. 1), le cercle des utilisateurs d'ISAS, pendant la phase pilote, 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 ISAS, cette restriction peut être levée et le cercle des utilisateurs étendu à tous les collaborateurs du SRC chargés de saisir, de consulter, d'évaluer et de garantir la qualité des données et qui doivent de ce fait 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 de la banque de données de la protection de l'Etat ISIS.

Al. 2

Pour que les collaborateurs du SRC puissent procéder à une recherche inter-systèmes ISAS-ISIS (voir les explications ci-devant concernant l'art. 6e, 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 (l'Office fédéral de la police et les services de renseignement cantonaux) n'ont accès qu'à l'Index.

Pour que le SRC puisse remplir son mandat, il doit pouvoir transmettre des données personnelles à des autorités politiques, des autorités de poursuite pénale, de justice et de sécurité. Cette règle correspond en grande partie au droit en vigueur (art. 17 LMSI). Le cercle des autorités concernées est fixé par le Conseil fédéral.

Cet article reprend dans ses grandes lignes les dispositions de l'art. 17, al. 3 et 4 de la LMSI. La loi sur la protection des données 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, LPD; RS 235.1). 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. Le SRC serait dans l'impossibilité d'accéder à d'importantes sources d'informations, en particulier dans des régions en crise.

La LMSI a de ce fait fixé des règles particulières pour la collaboration entre services de renseignement et pour la transmission de données personnelles à des autorités étrangères, reprises ici par la LFRC. Il existe dans ce domaine une pratique de longue date, accompagnée et contrôlée par les organes de surveillance (Surveillance des services de renseignement du DDPS, anciennement du DFJP, et Délégation des commissions de gestion des Chambres fédérales).

L'al. 3, let. d, concerne les demandes de conformité ou de clearing en faveur de personnes qui auraient accès 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.

Par ailleurs, les conditions de la CEDH doivent toujours être prises en compte.

Art. 6i (nouveau) 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 ou juridiques, le SRC doit pouvoir dire à la personne interrogée sur quelle personne il souhaite obtenir des informations et dans quel contexte. Cette disposition correspond à l'actuel art. 17, al. 2, LMSI.

Art. 6j (nouveau) Droit d'être informé

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

Art. 6k (nouveau) Délais de conservation

Conformément à la recommandation de l'Office fédéral de la justice dans le cadre de la consultation des offices, c'est au Conseil fédéral qu'est déléguée la compétence générale de fixer les délais de conservation des données dans ISAS. Si le contrôle interne de l'assurance-qualité conclut que des données ne sont plus nécessaires, il les supprime immédiatement.

Art. 6l (nouveau) Archivage

Al. 1

En principe, le SRC est lui aussi tenu de proposer les données et les dossiers devenus inutiles ou destinés à être détruits aux Archives fédérales aux fins d'archivage.

Al. 2

Le SRC, en tant qu'autorité ayant versé des documents aux Archives fédérales, doit pouvoir, dans certains cas et de façon analogue aux autorités de poursuite pénale, consulter des données personnelles dans les documents remis afin de pouvoir accomplir les tâches légales qui lui sont dévolues de par la loi. Cette possibilité, qui n'est pas prise en compte dans l'art. 14, LAr, est ajoutée ici au titre de *lex specialis*.

Art. 6m (nouveau) Dispositions d'exécution

Al. 1

Il incombe au Conseil fédéral d'édicter les dispositions d'exécution.

Al. 2

L'ordonnance du DDPS sur les champs de données et les droits d'accès aux systèmes d'information ISAS et ISIS (RS 121.22) continuera à fixer les champs de

données et les droits d'accès pour ces deux systèmes. Le Conseil fédéral fixe à cet effet un cadre de catégories de données personnelles à traiter .

3 Conséquences

Les modifications proposées ne créent pas de nouvelles tâches. Il ne faut donc pas s'attendre à des effets directs au niveau des finances ou de l'effectif du personnel. Le projet n'a par ailleurs aucune conséquence pour les cantons, les communes, l'économie publique, la société ou l'environnement.

4 Constitutionnalité et légalité

La LFRC se fonde sur l'art. 54, al. 1, et sur l'art. 173, al. 2, de la Constitution fédérale du 18 avril 1999⁴ (Cst.). L'art. 54, al. 1, Cst., fixe les compétences matérielles de la Confédération dans le domaine des affaires étrangères et règle de ce fait les activités de renseignement sur et à l'étranger. Dans son art. 173, al. 2, la Cst. définit 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 de la LFRC; elle ne va pas au-delà du domaine d'activité fixé à l'art. 1, LFRC.

Les modifications proposées sont susceptibles de porter atteinte aux droits fondamentaux, par exemple 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 traitement de données la concernant (voir ATF 122 I 360).

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 ne doit jamais être lésée.

L'exploitation pilote d'ISAS, régie actuellement sous forme de disposition transitoire, doit formellement être ancrée 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. La légitimité de l'intérêt public est dès lors incontestable.

Pour évaluer la proportionnalité d'une réglementation, 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.

⁴ RS 101

Pour tenir compte du principe de la proportionnalité, une assurance-qualité interne vérifie la pertinence et l'exactitude des données personnelles lors de leur saisie dans ISAS. Dans le cadre d'une appréciation périodique, la nécessité des données enregistrées pour l'accomplissement des tâches est examinée. Les données qui ne sont plus nécessaires sont supprimées. Par ailleurs, les droits d'accès aux données font l'objet de règles strictes et leur durée de conservation est limitée.

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