Bundesversammlung

Assemblée fédérale

Assemblea federale

Assamblea federala

Délégation des Commissions de gestion
CH-3003 Berne

www.parlement.ch
gpk.cdg@parl.admin.ch

Recommandé

À l'attention de la Commission de la politique de sécurité du Conseil national
Palais du Parlement
3003 Berne

Le 22 avril 2014

Co-rapport de la Délégation des Commissions de gestion concernant la LRens (14.022)

Monsieur le Président,
Madame, Monsieur,

Conjointement avec la Délégation des finances (DélFin), la Délégation des Commissions de gestion (DélCdG) assure la haute surveillance parlementaire sur les domaines de la protection de l'État et du service de renseignement. Dans l'exercice de son activité, la DélCdG a relevé à plusieurs reprises des lacunes législatives dans ces domaines et en a informé le Conseil fédéral sous la forme de recommandations.

Jusqu'à présent, la DélCdG a notamment fait appel à l'instrument du co-rapport pour donner, lorsque cela s'est avéré nécessaire, davantage de poids aux recommandations qu'elle avait formulées à la suite de ses inspections. Ainsi, elle s'est prononcée sur tous les projets de loi relatifs au renseignement de ces dernières années, comme celui qui concernait la révision LMSI II du 15 juin 2007 (07.057) et son message complémentaire du 27 octobre 2010 ou le projet de modification de la LFRC du 14 août 2013 (13.064).

Selon la DélCdG, le projet de loi sur le renseignement (LRens) est le projet de réforme de la protection de l'État et du service de renseignement en Suisse le plus global qui ait été présenté. Ses objectifs sont plus vastes que ceux de l'ancienne loi instituant des mesures visant au maintien de la sûreté intérieure (LMSI) de 1997 et plus ambitieux que ceux du projet avorté de LMSI II de 2007. En outre, il peut avoir des conséquences de premier plan sur le travail de la DélCdG et sur son rôle institutionnel.

Pour ces raisons, le co-rapport de la DélCdG ci-joint ne se limite pas à certains aspects du projet, mais tente, essentiellement du point de vue des procédures de surveillance et de contrôle, d'apporter des propositions d'amélioration à l'ensemble du projet. Vous trouverez en annexe des propositions et des recommandations sur une trentaine de points qui, selon la DélCdG, méritent votre attention particulière.

En sa qualité d'organe de haute surveillance, la DélCdG accorde une importance particulière à ce que la LRens prévoie un contrôle sans faille de la part de l'exécutif. En effet, il ne peut lui

incomber de compenser d'éventuelles lacunes dans la conduite et la surveillance exercées par le Conseil fédéral et le département compétent ; ce principe est d'autant plus important si les compétences et les tâches du service de renseignement sont étendues.

En raison de l'évolution technique, de plus en plus d'aspects de la vie humaine se jouent dans l'espace numérique ou, du moins, y sont représentés. Cela concerne également des activités qui peuvent menacer la sécurité intérieure et extérieure de la Suisse. Par conséquent, la DélCdG estime indispensable que les possibilités du service de renseignement tiennent compte de cette évolution, comme c'est le cas de la poursuite pénale dans le cadre de la révision en cours de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication.

La DélCdG préconise une codification globale des tâches et des compétences du Service de renseignement de la Confédération (SRC) dans le cadre d'une nouvelle loi. Elle est toutefois consciente du défi que représente le fait de concilier les exigences relatives à la protection de la personnalité ainsi qu'à une surveillance efficace avec les différentes facettes de l'activité de renseignement en Suisse et à l'étranger.

À la lumière des expériences qu'elle a faites jusqu'à présent avec le SRC, la DélCdG a également examiné ce projet sous l'angle de sa mise en œuvre ultérieure, à laquelle elle devra accorder une attention particulière en sa qualité d'organe de haute surveillance. Pour cette raison, il est important que les effectifs supplémentaires prévus pour assumer les nouvelles tâches et compétences soient en adéquation avec ces dernières (cf. recommandation 1 de l'inspection de la DélCdG relative à la sécurité informatique au sein du SRC).

Vous remerciant de tenir compte de nos remarques lors de votre examen, nous vous prions d'agréer, Monsieur le Président, Madame, Monsieur, l'expression de notre considération distinguées.

DÉLÉGATION DES COMMISSIONS DE GESTION

Le président	La secrétaire
Paul Niederberger	Beatrice Meli Andres
Conseiller aux États	

Annexe : Co-rapport de la DélCdG du 22 mai 2014

Copie à la DélFin

Bundesversammlung

Assemblée fédérale

Assemblea federale

Assamblea federala

Délégation des Commissions de gestion
CH-3003 Berne

22. avril 2014

Co-rapport de la DélCdG relatif au P-LRens (14.022), annexe

Annexe au co-rapport de la DélCdG relatif au P-LRens (14.022)

1. Haute surveillance à l'échelon de la Confédération et dans les cantons (art. 77 et 78)

Problématique

Dans les cantons, les parlements cantonaux doivent conserver les possibilités légales existant actuellement pour la haute surveillance.

Propositions de la DélCdG

Art. 77 Haute surveillance parlementaire

1 La haute surveillance parlementaire sur les activités du SRC et sur les activités des autorités d'exécution cantonales agissant sur mandat ~~du SRC~~ de la Confédération relève ~~exclusivement~~ de la Délégation des Commissions de gestion et de la Délégation des finances dans les domaines de compétences qui leur sont propres, conformément à la loi du 13 décembre 2002 sur le Parlement.

2 Les autorités de surveillance parlementaire cantonales peuvent contrôler l'exécution des mesures visées à l'art. 81, al. 1, LRens.

Art. 78 Surveillance cantonale

2 ~~Les autorités de surveillance parlementaire cantonales peuvent contrôler de manière indépendante l'exécution des mesures visées à l'art. 81, al. 1. L'art. 77 régit la surveillance de l'exécution de mandats confiés par le SRC en vertu de l'art. 9, al. 2, et la recherche d'informations sur des organisations ou des groupements qui figurent sur la liste d'observation visée à l'art. 71.~~

[Proposition de nouvelle formulation du point 2 de cet al., qui porte sur la surveillance administrative dans les cantons, p. 5].

Justification

Aux termes de l'art. 77 P-LRens, la haute surveillance sur l'activité des autorités d'exécution cantonales qui agissent sur mandat du SRC relève exclusivement de la DélCdG et de la DélFin.

En revanche, l'art. 78, al. 2, P-LRens permet également, en principe, une haute surveillance sur l'exécution du P-LRens dans les cantons.

Or, la deuxième phrase de l'art. 78, al. 2, P-LRens restreint fondamentalement la compétence de la haute surveillance cantonale, puisqu'elle en exclut toute activité cantonale dès lors que celle-ci sert à exécuter des mandats confiés par le SRC ou à traiter des informations sur des organisations de la liste d'observation. D'après les explications y afférentes, la haute surveillance parlementaire dans les cantons doit se limiter exclusivement aux activités que les autorités d'exécution cantonales mènent de manière autonome en application directe de la LRens, « sans recevoir dans chaque cas une mission formelle du SRC » (message LRens du 19 février 2014, p. 102).

Le 8 mars 2013, le Conseil fédéral expliquait encore dans le cadre de la procédure de consultation : « 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 » (rapport sur l'avant-projet de LRens du 8 mars 2014, p. 72). Du reste, le projet d'alors ne prévoyait pas de haute surveillance par les parlements cantonaux.

Comme a pu l'observer la DélCdG lors de ses visites aux organes cantonaux chargés de la protection de l'État, la liste d'observation du Conseil fédéral est un outil important pour la définition de priorités en matière de protection de l'État dans les cantons. La DélCdG a par ailleurs constaté que les cantons n'exercent quasiment aucune tâche relevant de la protection de l'État qui ne soit pas en lien avec l'activité du SRC. Une autre démarche ne serait pas appropriée dans le monde actuel, dans lequel la menace d'un réseautage national et international est forte.

Dans le projet actuel, le Conseil fédéral fait valoir que le droit actuel (LMSI et LParl) a attribué exclusivement à la DélCdG la haute surveillance parlementaire à l'échelon de la Confédération et des cantons (message LRens, p. 100).

Or, dans son rapport du 2 mars 2012 donnant suite au postulat Malama (10.3045), il était encore d'avis que le droit fédéral reste muet concernant le contrôle parlementaire cantonal et que la possibilité d'une haute surveillance parlementaire au niveau des cantons n'est donc pas exclue. Et d'ajouter que cela découle du principe selon lequel l'autonomie d'organisation des cantons (art. 47, al. 2, Cst.) doit être respectée autant que possible, y compris lorsqu'il s'agit de mettre en œuvre le droit fédéral (rapport sur le po. Malama du 2 mars 2012, FF 2012 4203).

Il n'en demeure pas moins que, lors de la consultation, douze parlements cantonaux ont exigé dans une lettre de la Conférence législative intercantonale (CLI) datée du 28 juin 2013 que la surveillance administrative et la haute surveillance cantonales demeurent pleinement possibles tant de jure que de facto, y compris dans le cadre de la nouvelle loi. De même, devrait valoir le principe selon lequel la haute surveillance cantonale va aussi loin que la surveillance administrative cantonale (principe d'accessoriété).

Jusqu'à présent, la DélCdG partait elle aussi du principe que les CdG cantonales peuvent assumer une fonction de haute surveillance sur les organes cantonaux de protection de l'État (cf. point 2). C'est du reste sur cette base qu'elle a échangé par le passé avec des CdG cantonales (LU, BL).

Par ailleurs, elle ne partage pas les craintes du Conseil fédéral, selon lesquelles une compétence assumée tant par la DélCdG que par les CdG cantonales provoquerait des lacunes dans la haute surveillance (message LRens, p. 98, 100, 102). Si les parlements des différents cantons sont disposés à assumer une responsabilité, il n'en résulte aucune lacune en termes de surveillance mais plutôt des opportunités de synergies et de collaboration coordonnée.

Rien que sur le plan pratique, la DélCdG serait dans l'impossibilité de contrôler systématiquement les organes cantonaux de protection de l'État comme elle le fait avec le SRC, avec le Renseignement militaire (RM) et avec le Centre des opérations électroniques (COE). Il faut en outre tenir compte du fait que de nouveaux champs d'activité et les compétences supplémentaires en matière de recherche d'informations du SRC occasionneraient une charge de travail supplémentaire pour la DélCdG.

Autant que la DélCdG puisse le constater au travers de sa collaboration institutionnelle avec la DélFin, cette dernière ne s'est encore jamais penchée sur les organes cantonaux de protection de l'État. Si elle devait se voir attribuer de nouvelles tâches dans ce domaine, il faudrait répondre à la question de savoir dans quelle mesure elle pourrait compter à ce titre sur le soutien du Contrôle fédéral des finances (CDF).

2. Surveillance administrative dans les cantons (art. 76 et 78)

Problématique

Il est prévu de reprendre dans le P-LRens la surveillance par les exécutifs cantonaux, pour laquelle une solution concluante a été trouvée en 2010 à l'initiative de la CCDJP. L'aménagement concret ne doit pas être laissé aux soins du seul Conseil fédéral, mais il faut que ses grandes lignes soient inscrites dans la loi, dans le respect de l'autonomie des cantons.

Propositions de la DélCdG

Art. 78 Surveillance cantonale

1 Les membres des autorités d'exécution cantonales auxquels le canton a confié des tâches définies par la présente loi sont soumis au statut du personnel cantonal et à la surveillance de leurs supérieurs. (inchangé)

2 (nouveau) Au sein des cantons, la surveillance des services incombe aux organismes qui sont les supérieurs hiérarchiques de chacun des organes d'exécution cantonaux. Pour renforcer leur surveillance, ces organismes peuvent engager, sous leur responsabilité, un organe de contrôle séparé de l'organe d'exécution cantonal. [comme art. 35, al. 1, OSRC]

3 (nouveau) Pour ses contrôles, la surveillance cantonale reçoit une liste des mandats confiés par le SRC ainsi que la liste d'observation selon l'art. 71. [comme art. 35, al. 3, let. c, OSRC]

4 (nouveau) L'autorité cantonale de surveillance peut consulter les données que le canton traite sur ordre de la Confédération. La consultation peut être refusée lorsque des intérêts cruciaux en matière de sûreté l'exigent. [comme art. 35a, al. 1 et 4, OSRC]

5 (nouveau) Le Conseil fédéral règle la procédure de consultation. En cas de litige, il est possible d'intenter une action devant le Tribunal fédéral en application de l'art. 120, al. 1, let. b, de la loi sur le Tribunal fédéral.

6 (nouveau) Le Conseil fédéral règle l'assistance à l'autorité cantonale de surveillance par des services de la Confédération. [comme art. 35~~a~~, al. 4, OSRC]

Art. 76 Surveillance et contrôle par le Conseil fédéral

3 Il règle:

b. les exigences minimales auxquelles les contrôles menés dans les cantons doivent répondre et les compétences des organes de surveillance de la Confédération ~~*et des cantons*~~ à cet égard.

Justification

Lors de son inspection ISIS, la DélCdG s'était déjà penchée sur les droits à l'information des autorités cantonales de surveillance.

Comme la DélCdG l'expliquait dans son rapport, la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), en réaction à l'affaire bâloise des fiches, a proposé à l'automne 2010 une solution qui prévoyait que la surveillance cantonale connaisse les mandats concrets confiés par la Confédération à l'organe cantonal de la sûreté et soit à même de vérifier son travail sur la base de ces critères. Si le SRC rejetait une demande de consultation des données relatives à la protection de l'État, qui sont traitées au niveau cantonal sur la base des mandats de la Confédération, le canton devrait pouvoir saisir le DDPS. A la suite d'une décision du chef du DDPS, le canton a la possibilité d'intenter une action devant le TF en application de l'art. 120, al. 1, let. b, LTF (loi sur le Tribunal fédéral) (cf. rapport ISIS de la DélCdG

du 21 juin, FF 2010 7055/7056). Le Conseil fédéral a repris l'essentiel de la proposition de la CCDJP dans le cadre de la révision de l'OSRC du 18 août 2010 (art. 35 et suiv. OSRC, Ordonnance sur le SRC).

Dans l'optique du message complémentaire à la révision LMSI II, la DélCdG avait chargé le professeur Biaggini d'étudier s'il était nécessaire de régler la question de la surveillance cantonale dans la loi. Dans son co-rapport à la CAJ-E daté du 24 mars 2011, elle précise, en se basant sur cette étude, que les bases légales existantes semblent en principe permettre aux cantons d'exercer une surveillance adéquate. C'est la raison pour laquelle la DélCdG avait considéré qu'il n'était pas nécessaire de soumettre une proposition relative à une réglementation plus détaillée de la surveillance cantonale dans la loi. Elle a toutefois souhaité continuer de suivre ce dosser afin de pouvoir détecter à temps d'éventuels besoins d'intervention sur le plan législatif.

Sur le plan matériel, l'actuel art. 35 et suiv. OSRC régit de manière appropriée les tâches de la surveillance administrative cantonale. On peut toutefois se demander si le Conseil fédéral est la bonne autorité de réglementation, d'autant plus que la souveraineté des cantons est affectée. De plus, l'art. 78 P-LRens ne contient quasiment aucun élément de référence dans le cadre duquel le Conseil fédéral devrait régir en particulier la surveillance administrative par les cantons.

Pour toutes ces raisons, la surveillance cantonale et ses relations avec la Confédération devraient être définies par les Chambres fédérales, tout au moins dans leurs grandes lignes, dans l'art. 78 LRens. Les détails, en particulier s'ils concernent le SRC ou le DDPS, pourraient alors être réglés par le Conseil fédéral dans les dispositions d'exécution.

Dans cet esprit, il est justifiable que, dans l'art. 76, al. 3, let. b, P-LRens, le Conseil fédéral puisse continuer de fixer des exigences minimales pour les contrôles dans les cantons (analogue à l'art. 26, al. 3, LMSI). Les compétences fondamentales doivent toutefois être régies par le législateur.

3. Droits à l'information de la DélCdG (art. 76 et 70)

Problématique

Contrairement à ce que propose le Conseil fédéral, les devoirs d'information que celui-ci avait jusqu'à présent à l'égard de la DélCdG (identités d'emprunt, interdictions d'exercer une activité) ne doivent pas être supprimés dans le P-LRens.

En revanche, la nouvelle disposition selon laquelle la DélCdG doit être informée le plus rapidement possible de l'extension des tâches du SRC conformément à l'art. 3 P-LRens n'a aucune utilité pratique pour la haute surveillance. Ce devoir d'information du Conseil fédéral n'aura pas pour effet une autolimitation que le P-LRens ne prévoit de toute façon pas.

Propositions de la DélCdG

Art. 76 Surveillance et contrôle par le Conseil fédéral

2bis (nouveau) *Le DDPS informe le Conseil fédéral et la Délégation des Commissions de gestion, annuellement ou selon les besoins, du but et du nombre d'identités d'emprunt utilisées par les collaborateurs du SRC ou des organes de sûreté cantonaux. Le nombre de pièces d'identité nouvellement émises doit être présenté séparément. [comme art. 27, al. 1bis, LMSI]*

2ter (nouveau) Le Conseil fédéral fournit à la Délégation des Commissions de gestion, annuellement et selon les besoins, des renseignements sur les interdictions d'exercer une

activité qui ont été prononcées et sur les résultats des examens effectués selon l'art. 72, al. 3. [comme art. 27, al. 1ter, LMSI]

Art. 70, al. 4, P-LRens (biffer) ~~*Lorsqu'il confie au SRC un mandat au sens de l'al. 1, le Conseil fédéral en informe la Délégation des Commissions de gestion dans un délai de 24 heures.*~~

Justification

A l'instar du droit actuel, le P-LRens prévoit que le Conseil fédéral transmet à la DélCdG la liste d'observation après approbation (art. 69, al. 1, let. b, P-LRens) et que le plan de contrôle de la surveillance des services de renseignement doit être concerté avec les activités de surveillance parlementaire (art. 74, al. 1, P-LRens).

Le P-LRens n'évoque cependant plus explicitement les documents suivants :

- le rapport annuel du Conseil fédéral à l'intention de la DélCdG sur le nombre d'identités d'emprunt et leur usage au sein du SRC et des organes de sûreté cantonaux (art. 27, al. 1bis, LMSI) ;
- le rapport annuel du Conseil fédéral à l'intention de la DélCdG sur les interdictions d'exercer une activité (art. 27, al. 1ter, LMSI).

Ces informations à la DélCdG, qui sont en lien avec le devoir de surveillance du Conseil fédéral, doivent être ancrées dans la nouvelle loi. Il serait plus approprié de les formuler à l'art. 76 P-LRens relatif à la surveillance par le Conseil fédéral.

En revanche, l'art. 70, al. 4, P-LRens exige, et c'est nouveau, que le Conseil fédéral informe la DélCdG dans les 24 heures de l'attribution d'un mandat portant sur la sauvegarde d'intérêts essentiels de la Suisse dans des situations particulières en application de l'art. 3 P-LRens. Par rapport à la pratique déjà réglée par l'art. 154, al. 3, LParl, cette disposition n'apporte aucune valeur ajoutée clairement identifiable pour la haute surveillance parlementaire.

Au travers de l'art. 3, P-LRens, le législateur attribuerait au SRC pour ainsi dire à l'avance de nombreuses tâches nouvelles dans une « situation particulière ». Dans le même temps, le SRC doit être autorisé à utiliser, sans conditions préalables particulières, tous les moyens pour la recherche d'informations. Par conséquent, le P-LRens laisse à l'entière appréciation du Conseil fédéral le soin d'exploiter toutes les possibilités de l'art. 3 P-LRens. Même un contrôle immédiat de la DélCdG ne susciterait pas une autolimitation que la loi ne prévoit pas. De plus, aux termes der l'art. 26, al. 4, LParl, la haute surveillance parlementaire ne confère pas la compétence d'annuler ou de modifier une décision du Conseil fédéral.

Il faut par ailleurs souligner que, contrairement au terme « situation d'exception » (cf. art. 58, al. 2, Cst.), le terme « situation particulière » est nouveau du point de vue du droit public et très vague. Le P-LRens ne contient pas de propositions de définition légale. Par conséquent, un contrôle ex post de la DélCdG pour savoir s'il y a eu ou non « situation particulière » ne serait pratiquement pas possible.

Etant donné que le SRC ne dispose actuellement pas de connaissances spécialisées sur la place industrielle, économique et financière suisse, le Conseil fédéral devrait décider d'augmenter ses effectifs en la matière. Le message précise que, bien entendu, la souveraineté des Chambres fédérales en matière de budget n'est à cet égard nullement entamée (message LRens, p. 37). Pour cette raison, une consultation de la DélFin en temps voulu pourrait être importante.

4. Pilotage par le Conseil fédéral (art. 69)

Problématique

Élimination d'un vice de technique législative et de la duplication de dispositions dans le même article.

Proposition de la DélCdG

Art. 69, al. 2, P-LRens (biffer)

2 ~~Les documents liés aux tâches visées à l'al. 1 ne sont pas accessibles au public.~~

Justification

Aux termes de l'art. 69, al. 1, P-LRens, le Conseil fédéral continue d'approuver la liste d'observation (let. b), il confie une mission de base au SRC (let. a) et règle la collaboration entre ce dernier et les autorités étrangères (let. f). Ces deux dernières dispositions, reprises de l'ordonnance en vigueur (art. 2, al. 2 et art. 12, al. 2 OSRC), sont intégrées pour la première fois dans la loi.

Le rapport annuel du Conseil fédéral sur son appréciation de la menace (jusque-là art. 27, al. 1 LMSI) est lui aussi conservé. L'art. 69, al. 2, P-LRens interdit toutefois la publication de ce rapport, ce qui devrait être une erreur du point de vue de la technique législative. Étant donné que le mandat de base est secret et la liste d'observation confidentielle, il n'est pas nécessaire de rajouter dans la loi que ces documents ne sont pas accessibles au public.

5. Surveillance et contrôle par le Conseil fédéral (art. 76)

Problématique

Le P-LRens ne concrétise quasiment pas le rôle du Conseil fédéral en tant qu'autorité de surveillance suprême de l'administration fédérale (art. 187, al. 1, let. a, Cst.) par rapport aux services de renseignement. Or, d'importantes dispositions légales ont été supprimées sans être remplacées, en particulier l'approbation, par le Conseil fédéral, d'accords administratifs conclus entre le SRC et des services de sûreté partenaires.

Proposition de la DélCdG

Art. 76, al. 1bis, P-LRens (nouveau)

Le Conseil fédéral approuve les accords administratifs conclus entre le SRC et des services étrangers qui sont d'une certaine durée, ont des conséquences financières substantielles ou dont le Conseil fédéral devrait avoir connaissance pour des raisons légales ou politiques. La réserve d'approbation vaut également pour les accords non écrits. Les accords ne peuvent être exécutoires qu'une fois approuvés. [analogue à l' art. 26, al. 2 LMSI)

Recommandation de la DélCdG

Il faudrait éventuellement clarifier la question de savoir si l'art. 76, al. 3, let. a, P-LRens est conforme avec les dispositions de la loi sur le contrôle des finances et dans quelle mesure il concerne la DélFin.

Justification

Trois fonctions de surveillance du Conseil fédéral ancrées jusque-là dans des textes de loi ont été supprimées :

- L'approbation par le Conseil fédéral, avant leur exécution, d'accords administratifs entre le SRC et des services de sûreté partenaires (art. 8 LFRC en application de l'art. 26, al. 2, LMSI).
- L'information annuelle à l'intention du Conseil fédéral du nombre d'identités d'emprunt et de leur usage au sein du SRC et des cantons (cf. proposition au point 3).
- L'examen annuel, par le Conseil fédéral, pour savoir si une interdiction d'exercer une activité doit ou non être maintenue (cf. proposition au point 2).

Aux termes de la législation actuelle, l'approbation par le Conseil fédéral d'accords administratifs conclus entre le SRC et des services de sûreté partenaires requiert du Conseil fédéral qu'il exerce un certain contrôle sur les contacts qu'il a approuvés entre le SRC et des services étrangers. A titre d'exemple, le Conseil fédéral aurait dû préalablement approuver un accord entre le SRC et la NSA qui, selon le service de presse du DDPS, aurait constitué une condition préalable à l'échange d'informations entre les deux services.

La DélCdG a veillé, dans le cadre de l'iv. pa. Hofmann (07.404), à ce que l'obligation d'approbation par le Conseil fédéral, qui a été initialement ancrée dans la LMSI et s'applique pour les accords administratifs de ce type, soit également introduite pour le SRC. Elle veille en outre au respect de cette disposition (rapport annuel 2013 de la DélCdG du 30 janvier 2014, ch. 4.1.1, p. 59). La disposition proposée par la DélCdG limite le devoir d'approbation du Conseil fédéral aux accords importants. Dans le même temps, elle souligne que ce devoir d'approbation ne peut être contourné si le SRC renonce à conclure un accord par écrit ou à le signer.

La disposition biffée dans le P-LRens, selon laquelle le Conseil fédéral doit vérifier chaque année l'usage d'identités d'emprunt, se traduisait jusqu'à présent par un contrôle au niveau supérieur, qui consistait à vérifier l'utilisation de ces moyens et était limité au strict nécessaire. La disposition correspondante ancrée dans la LMSI doit donc être reprise dans le nouvel alinéa 2bis de l'art. 76 P-LRens (cf. propositions au point 3).

Aux termes de l'art. 72, al. 3, P-LRens, seul le DDPS (ou un autre département qui présente la demande d'interdiction) vérifie régulièrement la nécessite d'interdire l'exercice d'une activité. Comme stipulé à l'art. 9, al. 3, LMSI, le Conseil fédéral devrait continuer d'être tenu de justifier cette estimation devant la DélCdG (cf. proposition au point 3 concernant l'art. 76, al. 2ter, P-LRens).

Les autres dispositions de l'article ne créent aucune véritable tâche de surveillance du Conseil fédéral, mais définissent des compétences qu'il serait préférable d'intégrer dans les articles thématiquement pertinents.

En vertu de l'art. 76, al. 3, let. a, P-LRens, le Conseil fédéral règle la surveillance financière des domaines d'activité du SRC qui doivent rester secrets. Il faudrait répondre à la question de savoir si ce mandat de réglementation est conforme avec les dispositions de la loi sur le contrôle des finances et dans quelle mesure il concerne la DélFin.

6. Consultation de la Délsec (art. 29)

Problématique

Pour que la haute surveillance soit efficace, il est nécessaire que le DFAE et le DFJP soient consultés par écrit pour la validation d'une mesure de recherche soumise à autorisation. Il ne faut en revanche pas que l'autonomie d'organisation du Conseil fédéral soit restreinte du fait qu'une seule de ses délégations est ancrée pour la première fois dans la loi. En effet, les délégations du Conseil fédéral ne disposent pas de pouvoir décisionnel.

Proposition de la DélCdG

Art. 29 Aval

1 Une fois la mesure de recherche autorisée, le chef du DDPS décide s'il y a lieu de la mettre en œuvre après avoir consulté *le DFAE et le DFJP*. *Les cas d'importance particulière peuvent être présentés au Conseil fédéral.*

2 La procédure de consultation doit être organisée par écrit.

Justification

Conformément au droit actuellement en vigueur, le Conseil fédéral décide seul de constituer des délégations (art. 23, al. 1, LOGA). L'art. 29 P-LRens soulève donc la question de savoir si l'existence de la Délsec doit être ancrée dans la loi et si la composition de celle-ci doit être préjugée. Cela peut être évité si les départements DFAE et DFJP sont mentionnés en lieu et place de la Délsec. Sur le plan matériel, cela ne changerait rien s'agissant du contrôle du service de renseignement.

Le P-LRens ne précise pas quelles informations le chef du DDPS doit présenter aux deux autres conseillers fédéraux. Il n'indique notamment pas si ceux-ci doivent être informés dans la même ampleur que le TAF. Pour que les départements associés puissent participer à la conception de la consultation, la procédure doit être organisée par écrit, à l'instar des procédures d'autorisation (art. 3, let. a, Org DFJP, Ordonnance sur l'organisation du DFJP), lesquelles relèvent en principe de la compétence du DFJP.

7. Surveillance par le DDPS (art. 74)

Problématique

Afin de garantir un contrôle politique continu au niveau départemental, y compris des activités les plus sensibles du service de renseignement, le chef du DDPS devrait être tenu d'avoir connaissance au moins annuellement des activités de recherche d'informations qui ne sont pas déjà soumises à son autorisation par le biais de la loi. Il pourrait ainsi exercer sa fonction de surveillance.

Proposition de la DélCdG

Art. 74, al. 5, P-LRens (nouveau)

Le chef du DDPS reçoit chaque année un rapport dans lequel le SRC évalue l'opportunité de la poursuite des opérations non soumises à autorisation.

Justification

Selon le droit actuel, le chef du DDPS doit, pour répondre à la question de savoir si la poursuite d'une opération relevant du renseignement est justifiée, demander au SRC une fois par an une évaluation de chaque opération que celui-ci a menée seul ou en collaboration avec des partenaires cantonaux ou étrangers (art. 24, al. 5, OSRC).

Une telle information constitue une condition préalable nécessaire pour un contrôle politique continu au niveau du département, y compris pour le contrôle des activités les plus sensibles du service de renseignement, notamment celles menées à l'étranger.

L'alinéa 5 proposé par la DélCdG, nouveau, couvrirait en particulier la recherche d'informations pour laquelle une obligation d'autorisation du chef du DDPS ou d'une instance de contrôle particulière (exploration radio par exemple) n'est pas déjà prévue dans la loi.

Aux termes de l'art. 74, al. 2 P-LRens, l'organe de surveillance interne que le DDPS doit mettre en place accomplit ses tâches de contrôle sans recevoir d'instructions. Une telle garantie n'existait pas jusqu'à présent dans la législation en vigueur. Le Conseil fédéral a ainsi mis en œuvre la recommandation 11 du rapport d'inspection de la DélCdG relative à la sécurité informatique au sein du SRC, dès lors que cela est possible au niveau législatif. Dans cette recommandation, la DélCdG demandait au chef du DDPS de veiller au respect des droits à l'information garantis à la Surveillance SR. Elle ajoutait que le SRC ne peut limiter ces droits à l'information ni de son propre chef ni d'entente avec le chef du département.

8. Tâches du SRC (art. 3, 6, 16, 19, 26, 37 et 70)

Problématique

Par rapport au droit actuel, le P-LRens prévoit une extension substantielle des tâches légales du SRC. Ce dernier doit en particulier pouvoir utiliser les nouveaux instruments dont il dispose lorsque la Suisse et ses institutions ne sont pas menacées directement mais indirectement, par exemple au travers de l'affaiblissement d'un secteur de l'économie. Cela pose des problèmes sur le plan constitutionnel, étant donné que, faute de base constitutionnelle explicite, la protection de l'État doit d'ores et déjà s'appuyer sur une compétence constitutionnelle inhérente tacite.

Proposition de la DélCdG

Biffer les dispositions suivantes :

Art. 3 ; art. 6, al. 1, let. d ; art. 16, al. 2, let. d ; art. 37, al. 2, let. B ; art. 70

Supprimer les renvois à l'art. 3 P-LRens :

Art. 19, al. 1 ; art. 26, al. 1, let. c

Justification

L'art. 6 P-LRens énumère les tâches légales du SRC, dont les tâches qu'il effectuait jusqu'à présent à l'étranger (collecte d'infirmations importantes en termes de politique de sécurité) et celles qui étaient définies dans la LMSI (terrorisme, extrémisme violent, service de renseignement interdit, prolifération NBC).

Les tâches qui ont pour but de protéger la Suisse d'actes d'espionnage par des acteurs étrangers privés et étatiques (art. 6, al. 1, let. a, ch. 2, P-LRens) sont en outre concrétisées à l'art. 19, al. 2, let. b, P-LRens :

- Défense contre le service de renseignements politiques (art. 272 CP).
- Défense contre le service de renseignements économiques (art. 273 CP). Cela comprend par exemple le vol de données bancaires lorsqu'il se fait au profit d'un mandataire étranger.
- Défense contre le service de renseignements militaires (art. 274 CP).

Le SRC enquête également sur des activités de renseignement sur le territoire suisse qui portent préjudice à d'autres États (art. 301 CP). Cette disposition a notamment pour but de préserver la neutralité de la Suisse.

L'extension de la protection de l'État à la défense contre des attaques qui visent des infrastructures critiques (cf. art. 6, al. 1, let. a, ch. 4, P-LRens) est elle en revanche nouvelle. Tandis que, par exemple, une panne de l'infrastructure d'information et de communication peut remettre en cause le fonctionnement de l'État, de l'économie et de la société, un incendie dans un tunnel d'autoroute ou dans un tunnel ferroviaire ne devrait jamais avoir de conséquences comparables. Du reste, d'autres services de la Confédération ou des cantons sont déjà compétents en la matière.

L'art. 3 P-LRens, auquel il est renvoyé dans l'art. 6, al. 1, let. d, P-LRens, est lui aussi fondamentalement nouveau par rapport au droit actuel. Au travers de cet article, le législateur laisse à la libre appréciation du Conseil fédéral le recours à tous les moyens de recherche prévus par la loi en vue de sauvegarder les « intérêts essentiels de la Suisse » (politique extérieure, intérêts de la place industrielle, économique et financière, etc.).

Étant donné qu'une tâche générale telle que la protection de la place industrielle, économique et financière concerne une menace qui représente un danger indirect pour l'État et non pour son existence même, la question de la constitutionnalité de l'art. 3 P-LRens se pose.

Tant la jurisprudence que la doctrine reconnaissent à la Confédération le pouvoir, en vertu de sa compétence inhérente, d'adopter des mesures visant sa protection et celle de ses organes et institutions ; la Confédération doit garantir et assurer l'existence même de la collectivité suisse et veiller à écarter les dangers qui menacent l'existence de cette communauté. Dans son rapport donnant suite au postulat Malama, le Conseil fédéral souligne que l'étendue, la portée et les limites de cette compétence inhérente ne sont toutefois pas claires. Pour cette raison, il est d'avis que les activités de protection de l'État déployées par la Confédération devraient se fonder sur une base constitutionnelle explicite (rapport sur le po. Malama, FF 2012 4294).

Étant donné que, à ce jour, le législateur a renoncé à créer une base constitutionnelle explicite pour la protection de l'État, le P-LRens, tout comme la LMSI jusqu'à présent, ne peut que s'appuyer sur le droit constitutionnel inhérent.

Or, le droit constitutionnel, du fait de son imprécision, doit être manié avec la plus grande retenue. Cela vaut en particulier pour la prévention de dangers indirects qui menacent le fonctionnement de l'État, par exemple suite à l'affaiblissement d'un secteur de l'économie (rapport sur le po. Malama, FF 2012 4279). Par conséquent, l'art. 3 P-LRens semble discutable du point de vue constitutionnel.

La DélCdG rappelle que les art. 184 et 185 Cst. permettent d'ores et déjà au Conseil fédéral d'adopter des mesures limitées dans le temps pour sauvegarder les intérêts du pays ainsi que pour préserver la sécurité intérieure et extérieure contre des troubles graves. Cela est également possible dans le domaine du renseignement, les mesures devant être proportionnées, appropriées et, faute d'alternative plus douce, nécessaires.

Il convient d'indiquer à ce propos que le projet LMSI II de 2007, qui a été rejeté par le Parlement, ne prévoyait aucune extension des tâches du service de renseignement.

Il faut également souligner que l'exercice de nouvelles tâches de ce type peut se traduire par de substantiels besoins en effectifs supplémentaires pour le SRC (cf. point 31).

9. Obligations des autorités de fournir des renseignements (art. 19 et 20)

Problématique

Selon le P-LRens, le SRC peut recevoir des renseignements d'un nombre plus important de services et dans davantage de cas que par rapport au droit actuellement en vigueur. Dans le même temps, les conditions qui doivent être remplies pour une demande du SRC sont réduites. De même, le secret professionnel ne doit plus être protégé et des limites sont levées concernant la transmission des renseignements obtenus aux autorités de poursuite pénale. Les réglementations de la LMSI y afférentes doivent cependant être conservées.

Propositions de la DélCdG

Art. 19, al. 1, P-LRens : *Les autorités … tout renseignement ~~permettant de déceler ou d'écarter~~ nécessaire pour déceler ou écarter (…) ou ~~de~~ pour sauvegarder (…).* [comme art. 13a, al. 1, LMSI]

Art. 19, al. 5, P-LRens (nouveau) : Le Conseil fédéral désigne dans une ordonnance les organisations tenues de fournir des renseignements. Cela concerne notamment les organisations de droit public ou privé externes à l'administration fédérale qui émettent des actes législatifs ou des décisions de première instance au sens de l'art. 5 de la loi fédérale du 20 décembre 1968 sur la procédure administrative ou qui accomplissent des tâches d'exécution de la Confédération; les cantons sont exceptés. [comme art. 13a, al. 3, LMSI]

Art. 19, al. 6, P-LRens (nouveau) : Lorsque le SRC apprend par des renseignements visés à l'al. 1 qu'une personne concernée ou un tiers ont commis des infractions, il ne peut transmettre aux autorités de poursuite pénale que celles de ces informations qui peuvent être exploitées pour élucider des infractions graves. [comme art. 13a, al. 4, LMSI]

Art. 20, al. 1, let. a, P-LRens : ~~les tribunaux,~~ les autorités de poursuite pénale et les autorités d'exécution des peines et des mesures ;

Art. 20a Secret professionnel (nouveau)

Pour les renseignements visés aux articles 19 ou 20, le secret professionnel garanti par la loi est protégé. [comme art. 13d LMSI]

Recommandation de la DélCdG

Il serait judicieux de clarifier s'il ne faudrait pas exclure les services de la Confédération qui s'occupent de l'aide humanitaire ou de l'aide à l'étranger. En effet, une telle obligation pourrait faire encourir à ces services le risque d'être perçus à l'étranger comme des agents du SRC.

Justification

Les art. 19 et 20 P-LRens régissent l'aide administrative au SRC et la levée du secret de fonction auquel sont soumis les services fédéraux et cantonaux concernés.

En vertu de l'art. 19 P-LRens, le SRC est autorisé à exiger des renseignements en vue de déceler une menace concrète. Par rapport à l'art. 13*a* LMSI, le champ d'application est toutefois étendu à toutes les tâches du SRC :

- L'obligation de fournir des renseignements ne sert plus à déceler uniquement les menaces que représentent le terrorisme, l'espionnage ou la prolifération NBC, mais également, et c'est nouveau, les menaces qui s'expriment au travers de l'extrémisme violent ou qui portent sur des infrastructures critiques.
- Jusqu'à présent, seuls pouvaient être exigés les renseignements « nécessaires » pour déceler ou prévenir une menace (art. 13*a*, al. 1, LMSI). Il suffit désormais, aux termes de l'art. 19 P-LRens, qu'ils « permettent » de déceler ou d'écarter une menace.

Dans le même temps, on ne retrouve pas dans l'art. 19 P-LRens les anciennes dispositions qui contribuent à la sécurité et à la protection juridiques :

- Le Conseil fédéral ne désigne plus dans une ordonnance les organisations à qui la Confédération a confié des tâches et qui sont tenues de fournir des renseignements (art. 13*a*, al. 3, LMSI). Aujourd'hui, les organisations ci-après sont énumérées dans l'annexe 5 à l'OSRC : COMCO, FNS, ESTI, CFF, CFF Cargo, la Poste, BILLAG.
- Par ailleurs, le P-LRens ne prévoit plus aucune restriction concernant la transmission, aux autorités de poursuite pénale, de renseignements obtenus. L'art. 13*a* LMSI ne permet cette transmission que pour l'élucidation d'infractions graves. Cette lacune n'est pas compensée par l'art. 59, al. 3, P-LRens, étant donné que celui-ci ne régit que la transmission d'informations obtenues dans le cadre de mesures de recherche soumises à autorisation au sens de l'art. 25 et suiv. P-LRens.

Prévue dans la LMSI pour les obligations de fournir des renseignements, la protection du secret professionnel fait défaut dans le P-LRens. Aux termes de l'art. 13*d* LMSI, un médecin cantonal était par exemple tenu de fournir des renseignements généraux mais il n'était pas obligé de divulguer, dans le but de renseigner, les connaissances dont il dispose et qui relèvent du secret médical (message complémentaire LMSI II du 27 octobre 2010, FF 2010 7184).

L'art. 20 P-LRens étend à différentes autorités l'obligation générale de renseigner au sens de l'art. 13 LMSI. Il s'agit des tribunaux, des autorités de poursuite pénale et des autorités d'exécution des mesures, des autorités qui exploitent les systèmes informatiques et des autorités de surveillance des marchés financiers.

L'étendue à tous les tribunaux de l'obligation générale de fournir et de communiquer des renseignements est particulièrement problématique du fait du partage des pouvoirs. Notons que ceux-ci n'ont été ajoutés au P-LRens au titre d'autorités soumises à l'obligation de fournir et de communiquer des renseignements qu'à l'issue de la procédure de consultation relative au P-LRens et que les explications ne contiennent aucune justification y relative.

En raison de la réglementation des divergences selon l'art. 21, al. 2 P-LRens, il serait en outre désormais possible que le TAF décide, si le TF, par exemple, doit ou non communiquer des renseignements au SRC.

10. Communications et renseignements fournis par des tiers (art. 22)

Problématique

Pour que des tiers communiquent des renseignements au SRC sur la base du volontariat, celui-ci doit être clairement identifiable lorsqu'il se renseigne. Une appartenance au SRC masquée au moyen d'une couverture est en contradiction avec cette condition. La disposition ne doit s'appliquer qu'à la Suisse, ce qui correspond à l'approche du P-LRens, qui consiste à ne pas réglementer plus dans les détails la recherche d'informations à l'étranger.

Proposition de la DélCdG

Art. 22 Communications et renseignements fournis par des tiers *en Suisse*

3 ~~*Sauf recherche d'informations sous couverture,*~~ Le SRC indique aux personnes auxquelles il demande des renseignements qu'elles sont libres de les donner ou non.

Justification

Aux termes de l'art. 22, al. 3, P-LRens, le SRC doit préciser à la personne concernée qu'elle est libre de donner ou non des renseignements.

Un problème se pose cependant pour la demande de renseignements lorsque l'appartenance au Service de renseignement est masquée au moyen d'une couverture (voir art. 17). Dans ce cas, l'art. 22, al. 3, P-LRens autorise le SRC à ne pas indiquer aux personnes auxquelles il demande des renseignements qu'elles sont libres de les donner ou non. Or, cela est particulièrement problématique lorsque la couverture est choisie de sorte que la personne concernée ait l'impression d'être tenue de fournir des renseignements.

Il devrait être surtout important pour les représentants du service de renseignement qu'ils ne soient pas obligés de s'identifier en tant que tels à l'étranger lorsqu'ils collectent des informations.

Si le champ d'application de l'art. 22 P-LRens était limité explicitement à la Suisse, cette problématique n'existerait pas. Cela correspondrait en outre à l'approche du P-LRens, qui ne souhaite pas régler plus dans les détails la recherche d'informations à l'étranger.

Si l'identité du collaborateur du SRC en Suisse doit être protégée, celui-ci peut utiliser une identité d'emprunt qui, conformément aux explications relatives à l'art. 22, al. 3, P-LRens, « n'[implique] pas obligatoirement une dissimulation de l'appartenance au SRC » (message LRens, p. 56).

11. Appréhension de tiers (art. 23)

Problématique

L'art. 23 P-LRens, dont le titre est incomplet et prête de ce fait à équivoque, autorise les collaborateurs du SRC à appréhender potentiellement toute personne et à la conduire en un lieu choisi par le SRC – le message utilise l'expression « lieu protégé » – pour l'y interroger brièvement.

La loi ne fixe pas de durée maximale ou totale pour cette « appréhension ». On peut lire dans le message que la durée totale, par analogie à la distinction entre appréhension et arrestation par la police, doit être inférieure à trois heures.

Les collaborateurs du SRC sont ainsi dotés de compétences que la LMSI ne connaît pas sous cette forme et qui, donc, sont attribuées exclusivement à la police pour ses enquêtes (cf. art. 215 CPP, Appréhension).

L'appréhension (art. 215 CPP) est une mesure de contrainte. Bien que, conformément à l'art. 23, al. 1, P-LRens, le renseignement doive être fourni librement (renvoi à l'art. 22 P-LRens), la nouvelle disposition, qui ne faisait pas partie de la consultation, peut facilement être utilisée pour avoir le même effet qu'une mesure de contrainte de la police.

Proposition de la DélCdG

Biffer l'art. 23 P-LRens.

Justification

Conformément au message, l'art. 23 P-LRens est formulé sur la base de l'art. 215 CPP (« Appréhension ») et confère au SRC les mêmes compétences qu'à la police. Par conséquent, l'article intitulé « Identification et interrogatoire de personnes » se rapproche d'une arrestation par la police (cf. message CPP du 21 décembre 2005, FF 2006 1205/1206).

Contrairement à l'arrestation, qui concerne une personne contre laquelle il existe un soupçon d'infraction, l'appréhension par la police ne peut servir qu'à déterminer si une personne peut être soupçonnée d'un délit. Si un bref séjour au poste de police ne fait naître aucun soupçon, la personne doit être libérée immédiatement ; dans le cas contraire, il doit y avoir arrestation. Étant donné qu'une arrestation provisoire (art. 217 CPP) ne doit pas excéder trois heures si elle n'a pas été prononcée par un membre gradé de la police fédérale ou cantonale, le message conclut qu'une appréhension en application de l'art. 215 CPP doit « durer nettement moins de trois heures au total » (message CPP du 21 décembre 2005, FF 2006 1206).

On peut déduire des explications relatives à l'art. 23 P-LRens que le SRC peut amener la personne appréhendée au lieu de son choix, par exemple « dans un lieu protégé », lorsque les circonstances justifient cette décision. Si ce lieu devait obligatoirement être un poste de police, cela aurait été précisé dans le texte. Le message indique que la durée totale de l'appréhension peut être de « quelques heures », mais « doit être inférieure à trois heures » (message LRens, p. 56). Or, cela est plus que les « nettement moins de trois heures » qui s'appliquent dans le cadre du CPP (message CPP, FF 2006 1224).

Tandis que, en se fondant sur l'art. 215 CPP, la police ne peut restreindre la liberté de mouvement d'une personne que dans l'exercice de son droit d'investigation, le SRC exerce, pour la même mesure, sa libre appréciation dès lors qu'il considère que cela est approprié pour déceler à temps et prévenir les menaces pour la sûreté intérieure ou extérieure (art. 6, al. 1, let. a, P-LRens). Pour cela, ni un événement extérieur ni une menace concrète, qui sont par exemple requis pour les obligations spécifiques faites aux autorités ou aux particuliers de fournir des renseignements (art. 19 et art. 24 P-LRens), ne sont nécessaires. A priori, toute personne qui séjourne sur le territoire suisse peut être concernée.

En vertu de l'art. 23, al. 1, P-LRens, la personne appréhendée peut être interrogée conformément aux modalités formulées à l'art. 22 P-LRens ; autrement dit, elle est libre de refuser tout renseignement.

Dans la pratique, cette garantie légale devrait vite perdre de son efficacité si une personne peut être menée en un lieu secret pour une durée allant jusqu'à trois heures et doit pour cette raison subir des inconvénients concrets tels que, par exemple, un avion raté ou d'autres désagréments. Pour des situations de ce type, toute possibilité de plainte ultérieure fait par ailleurs défaut dans le P-LRens.

Il faut en outre souligner que l'art. 23 P-LRens dans sa totalité n'a été intégré dans la loi qu'à l'issue de la procédure de consultation et n'a donc jamais été soumis au débat public.

12. Obligations spécifiques faites aux particuliers de fournir des renseignements (art. 24)

Problématique

Par rapport au droit existant, l'art. 24 P-LRens ne se contente pas de réduire la protection juridique, il renonce en outre à réglementer la transmission, aux autorités de poursuite pénale, des informations obtenues. De plus, le message n'analyse pas la façon dont l'extension des obligations de renseigner se répercute sur les droits fondamentaux, non seulement des

entreprises concernées, mais également des particuliers sur lesquels des images et des données vidéo sont collectées.

Proposition de la DélCdG

Art. 24, al. 3 (nouveau) Lorsque le SRC apprend par des renseignements visés à l'al. 1 qu'une personne concernée ou un tiers ont commis des infractions, il ne peut transmettre aux autorités de poursuite pénale que celles de ces informations qui peuvent être exploitées pour élucider des infractions graves. [comme art. 13*c*, al. 3, LMSI]

Recommandation de la DélCdG

Il faudrait régler la question de l'impact, sur les droits fondamentaux (surveillance vidéo) et sur la protection juridique, de l'extension des obligations de renseigner de particuliers. Cela pourrait être effectué par le biais d'un complément à l'avis de droit (avis de droit du professeur Biaggini de juin 2009, JAAC 4/2009, p. 290-295) que la CAJ-N avait exigé dans le cadre du projet de LMSI II.

Justification

L'art. 24 P-LRens reprend l'obligation de renseigner des transporteurs commerciaux, introduite dans le cadre de la révision LMSI II (art. 13*c* LMSI).

Contrairement à la LMSI, l'obligation de renseigner s'applique désormais aux exploitants privés d'infrastructures de sécurité. Les explications relatives audit article citent comme exemple les installations de vidéosurveillance et les systèmes d'accès électroniques dans le domaine des transports et de la vente. De même qu'à l'art. 19 P-LRens, la condition à remplir pour fournir un renseignement est facilitée.

Par rapport à la LMSI, le P-LRens restreint par ailleurs les droits des personnes concernées :

- Pas de limitation de la transmission aux autorités de poursuite pénale (art. 13*c*, al. 3, LMSI).
- Nouveauté : le recours contre cette obligation n'a pas d'effet suspensif (art. 79, al. 2, P-LRens).

Pour le projet LMSI II, les possibles atteintes que les obligations de renseigner des transporteurs commerciaux peuvent porter aux droits fondamentaux relatifs à la protection de la personnalité (art. 13 Cst., art. 8 CEDH) et à la liberté économique (art. 27 Cst.) avaient été étudiées dans le détail.

Une évaluation de ce type fait défaut dans le message relatif au P-LRens s'agissant des nouvelles obligations de renseigner des exploitants d'infrastructures de sécurité, bien que la transmission de photos et de vidéos prises en des lieux publics et non publics concerne potentiellement un nombre beaucoup plus important de personnes et qu'il soit possible d'en tirer des conclusions sur le comportement des personnes autres que par le biais des renseignements de transporteurs privés.

13. Procédure relative aux mesures de recherche soumises à autorisation (art. 21 et 31a)

La procédure relative à la recherche d'informations selon l'art. 25 et suiv. P-LRens est fondée sur les mesures de surveillance secrètes conformément à l'art. 269 et suiv. CPP. Cependant, la distinction entre poursuite pénale et service de renseignement n'est pas assez prise en considération, tandis que différentes règles de la poursuite pénale, qui sont également

pertinentes pour la recherche par les renseignements, ne sont pas assez prises en compte dans le P-LRens.

Propositions de la DélCdG

Art. 28, al. 1, let. a, P-LRens (modification) : *l'indication du but spécifique de la mesure de recherche et la justification de sa nécessité ainsi que les raisons pour lesquelles les investigations ont été vaines jusque-là ;*

Art. 28, al. 2bis, P-LRens (nouveau) : Le président de la cour compétente du Tribunal administratif fédéral n'autorise pas une mesure de recherche demandée lorsque celle-ci a déjà été autorisée sur la base d'une procédure pénale engagée à l'encontre des personnes visées à l'al. 1, let. b, et que l'enquête pénale présente un lien avec la menace concrète que la mesure de recherche du SRC doit éclaircir. Les tribunaux des mesures de contrainte compétents fournissent au Tribunal administratif fédéral les renseignements dont il a besoin.

Art. 31a P-LRens (limitation du traitement des données) (nouveau)

1 Le SRC veille à ce que les données personnelles obtenues dans le cadre de mesures de recherche soumises à autorisation qui ne présentent aucun lien avec la menace justifiant la décision ne soient pas traitées et soient détruites au plus tard dans les 30 jours suivant l'arrêt de ces mesures. [comme 18h P-LMSI II, cf. proposition de la DélCdG au point 26]

2 Les informations qui ne présentent aucun lien avec la menace justifiant la décision doivent être triées et détruites sous la direction du Tribunal administratif fédéral lors de la surveillance d'une personne qui relève de l'une des catégories professionnelles citées aux articles 170 à 173 CPP. Lors de la surveillance d'autres personnes, les informations à propos desquelles une personne citée aux articles 170 à 173 pourrait refuser de témoigner doivent elles aussi être détruites. [analogue à l'art. 271 CPP]

Justification

La procédure d'autorisation pour les mesures de recherche particulières conformément à l'art. 25 et suiv. P-LRens s'inspire de la procédure en vigueur pour les mesures de surveillance secrètes des autorités de poursuite pénale (art. 269 et suiv. CPP).

Par analogie au CPP, l'art. 26, al. 1, let. c, P-LRens cite des recherches restées vaines parmi les conditions nécessaires au recours à des mesures soumises à autorisation. En poursuite pénale, cela apparaît comme un critère approprié pour justifier l'utilisation de mesures de surveillance en tant qu'argument ultime. Il faut en effet toujours qu'il y ait eu infraction ou tout au moins que de graves soupçons laissent présumer qu'une infraction a été commise (art. 269, al. 1, let. a, CPP). Si des indices sur les auteurs de l'acte font défaut, cela peut s'expliquer de manière plausible par le fait que les auteurs ont tellement bien dissimulé leur acte que celui-ci ne peut être découvert qu'à l'aide de mesures d'enquête très étendues.

En ce qui concerne la recherche d'informations pour le renseignement, en revanche, des investigations peuvent être vaines parce que la menace supposée n'existe pas (cf. avis de droit du professeur Biaggini, p. 263). Le P-LRens devrait tenir compte de ces deux situations initiales différentes.

Dans le cadre de l'autorisation, il est donc indispensable que le SRC soit tenu d'indiquer au TAF quelles mesures de recherche il a d'ores et déjà entreprises et comment il s'explique qu'elles soient restées vaines.

A l'instar du CPP, le P-LRens autorise la surveillance de personnes qui sont soumises au secret professionnel (art. 171 à 173 CPP) par le biais de mesures de recherche soumises à

autorisation. Conformément au P-LRens, ces personnes peuvent certes, dans certaines circonstances (tiers selon l'art. 27, al. 2, P-LRens), ne pas être surveillées. Le projet est cependant dénué de règle analogue à celle de l'art. 271 CPP, qui régit l'utilisation d'informations soumises au secret professionnel.

Selon les explications, « une éventuelle procédure pénale et des mesures de surveillance ordonnées dans ce cadre priment les recherches d'informations prévues par la présente loi » (message SRC, p. 59). Or, le P-LRens ne règle pas la question de savoir comment le TAF peut déterminer qu'une procédure pénale est d'ores et déjà engagée contre une personne et, pour cette raison, refuser d'autoriser la mesure du SRC.

Dans son co-rapport sur le projet initial LMSI II, qu'elle avait remis à la CAJ-N le 29 février 2008, la DélCdG avait proposé que la protection préventive de l'État ne puisse pas recourir à des mesures de recherche d'informations soumises à autorisation si une enquête de police judiciaire était déjà en cours contre la même personne. Il s'agissait d'éviter que la poursuite pénale et le service de renseignement mettent sur écoute les mêmes personnes ou ne tentent de pénétrer dans les systèmes informatiques des mêmes personnes en même temps.

Contrairement au CPP, le P-LRens ne contient pas l'obligation de détruire les informations collectées lorsque celles-ci n'ont pas de lien avec le but autorisé de la mesure de recherche (art. 276 CPP). Le projet LMSI II de 2007 exigeait encore que les données personnelles de ce type soient détruites au plus tard dans les 30 jours suivant l'établissement de la mesure (art. 18*h* P-LMSI).

En revanche, le projet de LMSI II de 2007 ne prévoyait pas l'utilisation d'appareils de localisation (GPS par exemple) selon l'art. 25, al. 1, let. b, P-LRens, ni la fouille de locaux, de véhicules ou de conteneurs selon l'art. 25, al.1, let. e, P-LRens. La fouille de locaux et de véhicules avait même été explicitement refusée notamment en vue de « traduire l'idée de proportionnalité » (message complémentaire LMSI II, FF 2010 4846).

14. Haute surveillance par rapport au TAF (art. 28)

Problématique

La haute surveillance parlementaire ne peut s'exercer sur des décisions du TAF. Par conséquent, le travail de la DélCdG se limite à contrôler la procédure d'autorisation à proprement parler. Pour cela, toutefois, elle a besoin d'informations du TAF.

Proposition de la DélCdG

Art. 28, al. 6, P-LRens (nouveau) : *Le président de la cour compétente du Tribunal administratif fédéral établit un rapport d'activité annuel à l'intention de la DélCdG.*

Justification

Aux termes de l'art. 26, al. 4, LParl, la haute surveillance exclut tout contrôle sur le fond des décisions judiciaires. La DélCdG ne peut donc pas vérifier si des mesures de recherche autorisées l'ont été à juste titre.

En dépit de ses vastes droits à l'information, la DélCdG n'a plus aucune influence pour apporter des corrections aux cas déjà autorisés par le TAF. Lorsqu'il conclut son introduction aux explications relatives à la section 4 du P-LRens, qui régit les mesures de recherche soumises à autorisation, par l'assurance, qui se veut avant tout rassurante, que la DélCdG aura plein accès aux données et pièces nécessaires pour la surveillance, le Conseil fédéral témoigne de

ce fait de son manque de compréhension du travail de la haute surveillance (message LRens, p. 60).

La DélCdG pourrait éventuellement vérifier ultérieurement auprès du SRC si des mesures autorisées par le TAF ont fourni des résultats utiles. Si les cas d'autorisations inappropriées se multipliaient, la DélCdG pourrait s'entretenir avec le TAF en vue de constater la possible existence d'un problème systématique. La haute surveillance pourrait par la suite tenter d'apporter des améliorations dans l'optique de cas futurs.

En vue du contrôle du fonctionnement général de la procédure d'autorisation, il serait utile que la DélCdG ait une discussion approfondie avec le TAF une fois par an. Dans cette optique, la loi devrait charger le TAF de rédiger à l'intention de la DélCdG un rapport annuel sur ses activités en application de la loi.

15. Coordination entre le P-LRens et la révision de la LSCPT

Problématique

Tandis que le Conseil fédéral a visiblement l'intention d'octroyer au SRC toutes les compétences que les Chambres fédérales octroieront aux autorités de poursuite pénale dans le cadre de la révision de la LSCPT en cours, le P-LRens ne contient pas les dispositions indispensables pour coordonner entre eux le P-LRens et la LSCPT révisée.

Recommandation de la DélCdG

L'examen portant sur la disposition du P-LRens concernée par la révision de la LSCPT en cours ne devrait commencer qu'une fois cet objet clôturé dans les deux conseils.

Le moment voulu, les commissions chargées de l'examen préalable devraient demander au Conseil fédéral un message complémentaire sur les modifications de la LSCPT spécifiques à la LRens.

Justification

En vertu de l'art. 25, al. 1, let. a, P-LRens, le SRC doit se voir attribuer toutes les compétences dont est dotée la poursuite pénale sur la base de l'actuelle LSCPT. Les modifications qui doivent de ce fait être apportées à la LSCPT actuellement en vigueur figurent dans l'annexe concernant la modification d'autres actes.

Manifestement, l'intention du Conseil fédéral est de faire profiter le service de renseignement de toutes les possibilités que les Chambres fédérales approuveront dans le cadre de la révision totale de la LSCPT (13.025).

Or, le projet ne contient pas de dispositions qui auraient garanti une coordination avec la révision totale de la LSCPT, actuellement en cours. Seules les explications présentent différentes dispositions qui devraient encore être intégrées dans la LSCPT au profit du SRC (message LRens, p. 118 et suiv.). Toutefois, la reprise de formulations de la poursuite pénale telle qu'elle est proposée ne semble pas s'appuyer partout sur une réflexion suffisante (art. 22*a* LSCPT par exemple).

Manifestement, le Conseil fédéral pense que le Parlement veillera de lui-même, le moment voulu, à ce que, une fois totalement révisée, la LSCPT soit adaptée aux besoins du SRC.

Les explications contiennent du reste une proposition de disposition pour le P-LRens, selon laquelle l'utilisation des dispositifs spéciaux de surveillance (IMSI-Catchers) qui sont l'objet de la révision totale de la LSCPT (art. 269bis, P-CPP) est autorisée.

Le recours à des chevaux de Troie par le SRC est en revanche possible en application de l'art. 25, al. 1, let. d, ch. 1, P-LRens : celui-ci permet au SRC de s'introduire dans des systèmes informatiques (y compris ordinateurs portables, smartphones, etc.) pour y rechercher les informations qu'ils contiennent ou qui ont été transmises depuis ces systèmes. Cependant, les explications ne précisent pas explicitement cette possibilité ni ne présentent la manière dont elle doit être réalisée.

16. Introduction dans des systèmes informatiques en vue de collecter des informations (art. 25 et 36)

Problématique

Conformément au P-LRens, la question de savoir si l'introduction dans des systèmes informatiques est soumise à autorisation dépend du lieu où se trouve le système concerné et du lieu depuis lequel le SRC prend cette mesure. Cela suscite des incertitudes et relativise le rôle du TAF, notamment pour les mesures de recherche qui sont potentiellement les plus intrusives. Par conséquent, l'introduction dans des systèmes informatiques devrait dans tous les cas être soumise au TAF pour autorisation.

Propositions de la DélCdG

Art. 36 Introduction dans des systèmes et réseaux informatiques

2 ~~Pour accomplir les tâches définies par la présente loi,~~ Le SRC peut ~~également~~ s'introduire ~~depuis la Suisse~~ dans des systèmes et réseaux informatiques étrangers en vue de rechercher les informations qu'ils contiennent ou qui ont été transmises à partir de ces systèmes et réseaux. ~~Lorsque la situation politique est délicate, le directeur du SRC doit obtenir l'aval du chef du DDPS.~~

3 (nouveau) La procédure d'autorisation est régie par les art. 28 à 31.

Justification

Aux termes de l'art. 25, al. 1, let. d, ch. 1, P-LRens, le SRC est autorisé à s'introduire dans des systèmes informatiques (y compris ordinateurs portables, smartphones, etc.) pour y rechercher les informations qu'ils contiennent ou qui ont été transmises depuis ces systèmes.

Le SRC peut ainsi utiliser des chevaux de Troie (cf. point 15) et il se voit par ailleurs attribuer la compétence de « perquisitionner en ligne » un système informatique, une possibilité que même la révision totale de la LSCPT ne prévoit pas pour les autorités de poursuite pénale.

Tandis que l'utilisation de chevaux de Troie se limite aux informations qui sont communiquées à des tiers par le propriétaire de l'ordinateur, la perquisition en ligne permet d'accéder à des informations que l'utilisateur n'est disposé à partager avec personne.

Les explications relatives à l'art. 25 P-LRens font naître l'impression que l'introduction dans un système informatique doit toujours être soumise au TAF et au chef du DDPS pour autorisation. Or, cela est le cas uniquement lorsque le système concerné se trouve en Suisse, ce qui résulte *a contrario* de l'art. 36, al. 2, P-LRens, qui régit la recherche d'informations dans des systèmes

informatiques qui se trouvent à l'étranger et n'exige pas pour cela de façon explicite l'autorisation du TAF.

Si l'ordinateur se trouve à l'étranger, l'art. 36, al. 2, P-LRens prévoit simplement une autorisation du chef du DDPS « lorsque la situation politique est délicate ». Mais cela ne vaut que si le SRC s'introduit dans ces systèmes depuis la Suisse, et non depuis l'étranger.

Il peut donc être permis, en s'appuyant sur l'art. 36, al. 2, P-LRens, de s'introduire dans l'ordinateur portable ou le smartphone d'un citoyen suisse sans l'autorisation du TAF.

Pour cela, il suffit que le citoyen suisse se trouve à l'étranger avec son appareil et que la collecte d'informations vaille pour une menace qui revêt une composante transnationale plausible, ce qui est le cas par exemple pour le terrorisme international. Compte tenu du fait que les appareils mobiles sont très répandus et de la forte propension des Suisses à voyager, il ne s'agit pas là d'un simple scénario hypothétique.

La réserve d'autorisation pour la collecte d'informations à l'étranger depuis la Suisse (art. 35, al. 2, P-LRens) est elle aussi nulle et non avenue pour l'introduction dans des appareils mobiles lorsque leurs propriétaires suisses s'en munissent pour leurs voyages à l'étranger.

Il se peut également qu'un cheval de Troie utilisé pour la recherche d'informations à l'étranger transmette des données au SRC lorsque la personne entre en Suisse. Or, une telle procédure devrait, aux termes de l'art. 25 P-LRens, être autorisée par le TAF.

Le projet initial LMSI II de 2007 exigeait que l'introduction dans un système informatique soit soumise à l'autorisation d'un tribunal quelle que soit la localisation de l'appareil (art. 18*m*, P-LMSI concernant la perquisition secrète d'un système informatique). En d'autres termes, l'obligation d'autorisation valait également pour le cas où un ordinateur se trouvait à l'étranger.

Le critère du lieu du système informatique, proposé par le P-LRens, met en question l'efficacité même de la procédure d'autorisation prévue. Le TAF ne peut exercer aucune fonction de contrôle puisqu'il n'est même pas informé des cas problématiques potentiels. De même, la DélCdG ne peut avoir pour tâche de vérifier le lieu des systèmes informatiques dans lesquels le SRC s'est introduit sans l'autorisation du TAF.

Un principe de contrôle crédible suppose que toutes les mesures visées à l'art. 25, al. 1, let. d, ch. 1, P-LRens et à l'art. 36, al. 2, P-LRens soient autorisées selon la même procédure. Cette dernière doit valoir indépendamment du lieu où se trouve le système informatique concerné et du lieu depuis lequel a lieu l'introduction.

Si la mesure vaut exclusivement pour la recherche d'informations sur des événements se produisant à l'étranger, il est possible de renoncer à l'obligation d'information ultérieure selon l'art. 32 P-LRens comme le P-LRens le propose déjà pour l'exploration du réseau câblé.

17. Sabotage de systèmes informatiques en Suisse (art. 25 et 28)

Problématique

Aux termes de l'art 25, al. 1, let. d, ch. 2, P-LRens, le SRC est habilité, au moyen de mesures électroniques, à empêcher des systèmes informatiques en Suisse d'attaquer des infrastructures critiques en Suisse. Cette disposition nécessite toutefois d'être coordonnée avec d'autres afin d'éviter que de telles mesures n'entrent en conflit avec le travail des autorités de poursuite pénale.

Proposition de la DélCdG

Nouvel art. 28, al. 2bis, P-LRens conformément à la proposition au point 13 (le TAF assure lors de l'autorisation la priorité de la poursuite pénale).

Justification

Si des systèmes et réseaux informatiques sont utilisés dans des attaques visant des infrastructures critiques en Suisse, le SRC peut s'y introduire afin de perturber, d'empêcher ou de ralentir l'accès à des informations.

Si les ordinateurs se trouvent en Suisse, le SRC a besoin d'une autorisation du TAF selon l'art. 25, al. 1, let. d, ch. 2, P-LRens.

Les explications ne détaillent pas les mesures devant être mises en œuvre pour perturber, empêcher ou ralentir l'accès à des informations. Le but cité, en revanche, concerne toute attaque qui, sous quelque forme que ce soit, perturbe le flux de données entre les composantes d'un ordinateur ou d'autres systèmes.

Il s'agit notamment de modifier des programmes pour changer des accès internes à la mémoire et de surcharger la connexion Internet de l'ordinateur attaqué au travers d'un nombre trop élevé de demandes de connexion. Il n'est également pas exclu que des données puissent être effacées. Il s'agit sans doute du moyen le plus sûr d'empêcher l'accès aux informations dans un système.

La situation serait particulièrement problématique si le SRC supprimait ou modifiait sur l'ordinateur attaqué des données qui seraient ultérieurement nécessaires au titre de preuves dans une procédure pénale.

Selon les explications, le SRC ne peut intervenir que si les systèmes [informatiques] […] sont utilisés pour des attaques contre des infrastructures critiques (message LRens, p. 59). Le but de la mesure est de « lutter contre un dommage imminent ou contre un dommage total ou partiel découlant d'une attaque en cours » (message LRens, p. 61).

Le SRC a ainsi la compétence, s'il découvre qu'une attaque se prépare ou est informé d'une attaque en cours, d'empêcher à l'aide des moyens appropriés le fonctionnement des ordinateurs qui sont utilisés pour l'attaque. En revanche, la police n'a pas cette possibilité de s'introduire dans des ordinateurs. Si elle est informée qu'un système informatique est utilisé pour une attaque en cours, elle peut cependant « débrancher » l'appareil sur place.

Selon les explications relatives à l'art. 25, al. 1, let. d, ch. 2, P-LRens, une éventuelle procédure pénale prime les recherches d'informations et le SRC pourrait n'intervenir que si les conditions préalables pour une procédure pénale ne sont pas (encore) remplies ou que cette dernière ne permet pas de lutter contre une attaque réelle (principe de subsidiarité). Tant le projet de loi que les explications y relatives omettent cependant de dire comment le SRC doit tenir compte de cette exigence.

La disposition de l'art. 28, al. 2bis, P-LRens, qui est relative à la coordination et proposée au point 13, peut permettre de désamorcer de possibles conflits entre la démarche du service de renseignement et celle de la poursuite pénale. Cela ne sera cependant garanti que si le SRC applique face au TAF la procédure d'autorisation ordinaire et non la procédure en cas d'urgence selon l'art. 30 P-LRens.

18. Sabotage de systèmes informatiques à l'étranger (art. 36)

Problématique

Une contre-attaque contre des systèmes informatiques à l'étranger qui sont utilisés pour des attaques en Suisse soulève différentes questions relevant du droit international public, lesquelles ne sont pas évoquées dans le message.

Recommandation de la DélCdG

Les Chambres fédérales devraient clarifier la question de savoir s'il est nécessaire sur le plan légal de préciser dans quelles circonstances le Conseil fédéral peut faire intervenir le SRC contre des ordinateurs se trouvant à l'étranger et – au vu des relations bilatérales – quel dommage peut être pris en considération.

Justification

L'art. 36, al. 1, P-LRens autorise une « contre-attaque » contre des systèmes informatiques étrangers qui sont utilisés pour attaquer des infrastructures critiques en Suisse.

Les explications ne se penchent pas sur d'éventuelles questions pertinentes concernant la coordination avec la poursuite pénale et l'entraide judiciaire. Que se passe-t-il, par exemple, si la Suisse, lors d'une attaque perpétrée par des criminels depuis l'étranger, y fait une demande d'entraide judiciaire et que l'État à qui elle adresse sa demande s'aperçoit que les ordinateurs concernés ont été par la suite eux-mêmes attaqués depuis la Suisse ?

En cas d'attaque électronique, il peut être extrêmement compliqué d'identifier sans problème aucun les ordinateurs à la source de l'attaque. Du fait de connaissances insuffisantes, les mesures du SRC peuvent, pour cette raison, toucher des ordinateurs qui n'ont pas participé à l'attaque contre la Suisse ou tout au moins y ont participé sans que leurs propriétaires ne le sachent. Des connaissances lacunaires sur la source de l'attaque ou des erreurs techniques de procédure peuvent occasionner des dommages non intentionnels à l'étranger.

Les explications n'évoquent pas les implications sur le plan du droit international public dont le Conseil fédéral doit tenir compte lors d'une autorisation selon l'art. 36, al. 1, P-LRens. L'OFJ (Office fédéral de la justice) et la DDIP (Direction du droit international public) ont déjà établi deux avis de droit sur la question :

- Avis de droit de l'OFJ et de la DDIP du 10 mars 2009 sur les bases légales des opérations dans les réseaux informatiques par les services du DDPS (publié dans JAAC 3/2009)
- Avis de droit de l'OFJ et de la DDIP du 1er novembre 2013 sur les Computer Network Operations (CNO) – Bases légales et aspects relevant du droit international de contre-mesures en cas de cyber-attaque contre la Suisse (non publié)

Si une cyber-attaque ne peut être imputée à un État dans un cas concret, une intervention unilatérale contre les ordinateurs concernés n'est pas autorisée du point de vue du droit international public étant donné que, en l'espèce, la dimension internationale, nécessaire, fait défaut.

Si la cyber-attaque peut être imputée à un État, il convient d'opérer la distinction suivante en termes de droit international public : l'incident constitue-t-il, dans ses effets, une agression armée au sens de l'art. 51 de la Charte des Nations Unies ou n'en est-il pas une ? S'il y a agression armée, la Suisse serait alors en état de guerre avec l'État concerné, et le droit international public autoriserait des contre-mesures comparables. Si la cyber-attaque ne constitue pas une agression armée mais seulement une violation de l'interdiction d'intervention ancrée dans le droit

international public, ce dernier n'exclut pas, sous certaines conditions, que la Suisse puisse prendre des contre-mesures unilatérales comparables dans le domaine d'Internet.

19. Coopération avec des services partenaires en matière de recherche d'informations (art. 33, al. 1)

Recommandation de la DélCdG

Il convient de vérifier si le SRC a le droit d'associer des services partenaires à la réalisation de mesures de recherche soumises à autorisation.

Justification

Aux termes de l'art. 33, al. 1, P-LRens, le SRC peut collaborer avec des services de renseignement étrangers pour la recherche d'informations en Suisse.

Cette possibilité existe en principe également pour les mesures soumises à autorisation.

La disposition exige cependant que le service partenaire mandaté présente la garantie que l'ordre juridique suisse sera respecté.

Or, lorsque le service partenaire utilise des appareils techniques ou des logiciels d'espionnage en Suisse, le SRC devrait avoir bien du mal à être sûr que ces moyens ne sont pas utilisés à des fins autres que celle de la collaboration qu'il a demandée. Ainsi, le SRC pourrait, lors d'une opération commune avec un service partenaire, installer pour le compte de ce dernier un logiciel d'espionnage sur l'ordinateur d'une personne cible afin de tirer profit des informations ainsi collectées. Or, au final, seul le créateur du programme serait probablement en mesure de décider quelles informations parviendraient effectivement au SRC.

Les explications ne disent pas comment le SRC peut apporter la preuve au TAF que le service partenaire respectera le droit suisse.

Se pose donc la question essentielle de savoir dans quelle mesure il est raisonnable pour le SRC de recourir au soutien de services étrangers, sous forme technique ou autre, en particulier dans le domaine des mesures soumises à autorisation.

20. Coopération avec des particuliers en matière de recherche d'informations (art. 33, al. 2)

Recommandation de la DélCdG

Il convient de vérifier si le SRC peut confier à des particuliers des mandats portant sur la réalisation de mesures de recherche soumises à autorisation.

Justification

En vertu de l'art. 33, al. 2, P-LRens, le SRC peut également confier à des particuliers des mandats en matière de recherche d'informations.

Il peut s'agir, selon les explications, de mesures de recherche qui nécessitent des appareils techniques de surveillance d'une grande complexité, qui ne sont exploités que par des entreprises privées spécialisées. Toujours selon les explications, il est également envisageable de faire appel à des spécialistes en informatique privés pour des réseaux de données hautement protégés (message LRens, p. 68). Des restrictions, spécifiquement par rapport à des entreprises étrangères, n'ont pas été mentionnées.

Enfin, l'art. 33, al. 2, P-LRens permet l'*achat externe* de compétences clés en termes de technique et de personnel dont le SRC a besoin pour mettre en œuvre ses nouvelles compétences pour la collecte d'informations. Avec la possibilité de recourir à des externes, le DDPS risque de ne pas devoir se rendre compte des besoins réels en personnel liés à l'extension des compétences du service de renseignement (cf. point 30).

Selon les explications, la garantie que ces externes respecteront le droit suisse, en particulier lorsqu'ils sont responsables d'une part essentielle de la préparation et de la réalisation de la mesure de recherche, doit être fournie contractuellement. Or, le SRC ne peut le vérifier que si lui-même dispose des compétences clés nécessaires pour comprendre par exemple le fonctionnement d'un logiciel d'espionnage.

La question se pose également de savoir, lorsque des entreprises externes recherchent des informations pour le compte du SRC, si elles traitent les données collectées et comment, et qui est responsable de la protection des données et de la surveillance.

Selon les explications, il serait suffisant de régler la question de la sécurité des informations et de la protection des données dans le contrat avec les externes. Les explications ne disent en revanche pas comment le SRC contrôlera la sécurité des informations et la protection des données ni comment les « droits de contrôle du PFPDT » doivent être exercés (message LRens, p. 68). On ne sait pas non plus si la Surveillance SR serait habilitée à effectuer les audits nécessaires auprès des prestataires externes.

21. Protection des sources par rapport aux autorités de poursuite pénale (art. 34, al. 2 et 4)

Problématique

L'art. 34, al. 2 et 4, P-LRens correspond dans une large mesure à l'actuel art. 17, al. 5, LMSI, qui doit son origine à un co-rapport de la DélCdG relatif à la révision LMSI II. En cas de litige, c'est le TPF qui statue. Rien ne justifie la remise en question de cette solution élaborée par la DélCdG, ni l'attribution de cette responsabilité au TAF.

Proposition de la DélCdG

Art. 34, al. 4, P-LRens (modification): En cas de litige, le *Tribunal pénal fédéral* ~~*Tribunal administratif fédéral statue conformément à l'art. 36a LTAF*~~ statue. Les dispositions déterminantes en matière d'entraide judiciaire sont au surplus applicables.

Recommandation de la DélCdG

Il conviendrait également de vérifier si, pour des raisons de compréhension, l'ordre des alinéas 3 et 4 ne devrait pas être inversé.

Justification

Se fondant sur ses investigations concernant l'affaire dite de l'attentat du Grütli, la DélCdG était parvenue à la conclusion que l'identité d'une source en Suisse doit être communiquée aux autorités suisses de poursuite pénale dans certaines circonstances, notamment lorsqu'un informateur est soupçonné d'avoir commis un acte pénalement répréhensible poursuivi d'office ou si l'identification de cette personne est indispensable à l'élucidation d'une infraction grave.

Le 25 mars 2011, la DélCdG a formulé dans son co-rapport une proposition allant dans ce sens, que les Chambres fédérales ont suivie en adoptant l'actuel art. 17, al. 5, LMSI. Le législateur a également décidé qu'en cas de litige, ce n'est pas le TAF mais le TPF qui doit statuer.

L'art. 34, al. 2, P-LRens correspond dans une large mesure à l'actuelle réglementation de la LMSI. Notons toutefois qu'à l'alinéa 4 le Conseil fédéral reprend une proposition que le DDPS avait déjà soumise à la CAJ-E lors de l'examen du message complémentaire à la LMSI II, et prévoit qu'en cas de litige, ce n'est plus le TPF mais de nouveau le TAF qui doit statuer.

Le Conseil fédéral justifie cette mesure notamment par le fait que, le P-LRens attribuant d'ores et déjà un rôle important au TAF en tant qu'instance de décision, celui-ci doit également statuer dans les affaires d'entraide judiciaire.

Cette argumentation omet cependant le fait qu'aucune opération incluant des informateurs ne doit être approuvée par le TAF et qu'en cas de litige, les questions juridiques soulevées se concentrent sur le fait de savoir si le délit à élucider et une éventuelle infraction commise par la source justifient que l'identité de cette dernière soit communiquée aux autorités de poursuite pénale.

22. Exploration radio et organe de contrôle (art. 37 et art. 75)

Problématique

Le co-rapport sur la révision LMSI, que la DélCdG a remis à la CAJ-E en 2011, est à l'origine de l'actuelle réglementation de l'exploration radio et de l'autorité de contrôle indépendante (ACI), laquelle vérifie la légalité de l'exploration radio. Le P-LRens reprend pour une grande part ces dispositions (art. 4a et 4b, LFRC) dans l'art. 37 et dans l'art. 75 P-LRens.

En raison des discussions qu'elle mène chaque année avec l'ACI, la DélCdG a pu se faire une idée de l'efficacité, dans la pratique, des dispositions dont elle est à l'origine. Un potentiel d'amélioration ayant été identifié, elle propose trois modifications, toutes soutenues par l'ACI.

Proposition de la DélCdG concernant l'art. 37 P-LRens

Art. 37, al. 6, P-LRens (modification) : *Si, lors de son travail, il découvre des enregistrements des communications qui ne contiennent ni informations sur l'étranger importantes en matière de politique de sécurité ni indices de menaces concrètes pour la sûreté intérieure, il efface ceux-ci le plus rapidement possible.*

Justification

Hormis l'introduction, la disposition correspond à l'actuel art. 4*a*, al. 6, LFRC. La modification a pour but une délimitation par rapport à l'al. 3, aux termes duquel le Conseil fédéral régit la durée de conservation des communications enregistrées. Le service chargé de l'exploration ne doit effacer les communications clairement non utilisables qu'avant expiration du délai de conservation lorsqu'il remarque de telles communications dans le cadre de son travail. Par conséquent, il ne doit pas sonder ses données en ciblant de telles communications, ce qui, au vu de l'important volume, serait quasiment impossible.

Propositions de la DélCdG concernant l'art. 75 P-LRens

Art. 75, al. 1, P-LRens (modification) : *Une autorité de contrôle indépendante, interne à l'administration, vérifie la légalité de l'exploration radio. Elle accomplit ses tâches sans recevoir d'instructions. Ses membres sont désignés par le Conseil fédéral.*

Art. 75, al. 2, P-LRens (modification) : *L'autorité de contrôle vérifie les missions attribuées au service chargé de l'exploration ainsi que le traitement et la transmission des informations que*

celui-ci a enregistrées. Pour cela, les services compétents lui donnent accès à toutes les informations et tous les dispositifs utiles.

Justification

Avec l'art. 75, al. 1, P-LRens, le Conseil fédéral déroge à l'actuel art. 4*b*, al. 1, LFRC sans en indiquer les raisons et fait naître une marge d'interprétation inutile s'agissant de la nature de l'ACI.

L'art. 75, al. 2, P-LRens correspond à la formulation de l'art. 4*b*, al. 2, LFRC. L'ACI considérait que cette disposition était problématique, puisqu'elle exigeait d'elle qu'elle vérifie le traitement des informations enregistrées avant et après leur transmission au SRC par le service chargé de l'exploration. L'ACI a fait valoir à juste titre que cela était quasiment impossible. La DélCdG avait voulu garantir en premier lieu, au travers de la formulation initiale, que l'ACI puisse effectuer son contrôle tant auprès de l'organisation qui enregistre les données qu'auprès du SRC. Cela doit désormais être formulé explicitement.

23. Exploration du réseau câblé (art. 38 à 42)

Problématique

Comme il ressort des explications du message, les bases légales formelles proposées pour l'exploration du réseau câblé poursuivent les buts suivants :

- effectuer des clarifications et des essais techniques plus approfondis avec l'exploration du réseau câblé ;
- effectuer une analyse des flux de données à travers la Suisse ;
- en se basant sur cette analyse, vérifier si l'exploration du réseau câblé permet d'obtenir un nombre suffisant d'informations utiles également en Suisse.

Selon le message, la charge de travail que représente la réalisation de l'exploration du réseau câblé ne peut être estimée.

La procédure d'autorisation proposée s'accompagne elle aussi d'importantes incertitudes :

- Seules les catégories de mots-clés de recherche sont soumises au TAF pour autorisation, car de nombreuses personnes concernées ne peuvent être identifiées qu'au cours de la réalisation du mandat.
- Une fois l'autorisation accordée, ces mots-clés de recherche doivent être « traités de manière dynamique » ; ils ne peuvent être affinés qu'au cours de l'exploration.
- L'autorisation doit être accordée pour une durée de six mois, contrairement à la durée de trois mois pour les mesures qui relèvent de l'art. 25 et suiv. P-LRens.

Cela signifie que le TAF autoriserait à chaque fois une étude de faisabilité d'une durée de six mois, laquelle pourrait équivaloir à chercher une aiguille dans une botte de foin.

Le flou règne quant à savoir comment le Tribunal doit décider du nombre et de l'identité des prestataires de télécommunication qui peuvent être associés à la réalisation d'une mission d'exploration pour qu'une mesure puisse encore être considérée comme étant proportionnée.

Remarque de la DélCdG

La DélCdG a conscience depuis des années déjà qu'une part croissante des communications internationales se fait par le câble et que, de ce fait, l'importance de l'exploration radio ne cesse de diminuer. Il est donc compréhensible que le Conseil fédéral souhaite préserver l'avantage procuré par les investissements réalisés jusqu'à présent en recherchant de nouvelles sources de données.

La DélCdG n'est cependant pas en mesure de dire si la procédure proposée par le Conseil fédéral permettra d'atteindre cet objectif.

24. Bases de données et contrôle de qualité (art. 43 à 56)

Problématique

Le P-LRens prévoit un contrôle de la protection des données par un organe indépendant de contrôle de la qualité tel qu'il est stipulé dans la LMSI pour seulement 30 % des données contenues jusque-là dans ISIS (celles qui concernent l'extrémisme violent). Le contrôle de qualité des données ISIS restantes ainsi que des informations collectées sur l'étranger, traitées jusqu'à présent dans le système ISAS, est en revanche confié aux utilisateurs de ces données, ce qui déroge aux anciennes dispositions.

Conformément à l'art. 56 P-LRens, les données de ce type sont tout d'abord archivées dans le système de stockage des données résiduelles, lequel n'est toutefois soumis qu'à un contrôle de qualité minimal. Un contrôle de qualité plus concluant n'est obligatoire que lorsque ces données sont transférées vers le système IASA SRC. Or, cela vaut uniquement pour les annonces dont le SRC estime qu'elles sont suffisamment pertinentes pour justifier une analyse ultérieure. Dans le même temps, le P-LRens ne répond explicitement pas à la question de savoir si, en cas d'effacement de données dans IASA SRC, les copies correspondantes doivent également être effacées dans le système de stockage des données résiduelles.

Pour éviter que le système de stockage des données résiduelles ne soit submergé de données peu pertinentes et peu contrôlées, il faudrait, pour compenser la faible réglementation de la protection des données stipulée à l'art. 56 P-LRens, ancrer dans la loi une durée maximale de conservation des données. Cela permettrait en outre de combler quelque peu le manque de personnel affecté aux contrôles de qualité auquel il faut s'attendre bien que le message ne l'évoque à aucun moment.

Proposition de la DélCdG

Art. 56, al. 4, P-LRens (nouveau) *La durée maximale de conservation des données est de dix ans.*

Justification

Systèmes d'information actuels

Selon le droit actuel, toutes les informations collectées dans le cadre de la LMSI sont traitées dans le système d'information relatif à la protection de l'État (ISIS). La LMSI exige pour les données versées dans ISIS un contrôle de la protection des données complet et périodique ainsi que de stricts délais concernant leur effacement.

Les informations collectées sur l'étranger sont en partie traitées dans le système d'information sécurité extérieure (ISAS). Depuis la dernière révision de la LFRC (13.064), adoptée lors la session de printemps 2014, des contrôles des saisies ISAS et des contrôles de qualité

périodiques sont également prévus pour les données enregistrées dans le système ISAS. Conformément aux explications relatives à ce projet de loi, l'organe interne de contrôle de la qualité, qui a fait ses preuves pour ISIS, doit également se charger de ces contrôles (message LFRC du 14 août 2013, FF 2013 5960).

Les autres informations collectées sur l'étranger sont classées dans un système de stockage des données brutes (environ quatre millions de communications). A ce jour, il n'existe pas de dispositions régissant la protection des données pour ce système.

Outre les systèmes d'information de données relatives au renseignement, le SRC a introduit différents systèmes dans lesquels des données administratives et des données moins sensibles sont traitées (GEVER SRC, portail ROSO, PES, base de données pour les données relatives aux photos d'identité, etc.) A la suite d'une recommandation formulée par la DélCdG dans son rapport ISIS, les données relatives aux photos d'identité sont traitées dans une base de données distincte (P4, Quattro P) et doivent être effacées au bout de cinq ans.

Futurs systèmes d'information

Le P-LRens prévoit le remplacement de l'actuel système ISIS.

Environ 30 % des annonces stockées jusqu'à présent dans ISIS (état 2013) seront versés dans la nouvelle base de données IASA-EXTR SRC, qui doit contenir exclusivement des informations relatives à l'extrémisme violent. Les données contenues dans IASA-EXTR SRC doivent être soumises aux mêmes contrôles que ceux qui valent jusqu'à présent pour toutes les données ISIS. L'organe interne de contrôle de la qualité est compétent en la matière.

Stockés dans le futur système IASA SRC, les 70 % restants des données ISIS et les données versées dans ISAS seront soumis à de nouvelles règles en matière de protection des données : ce sont les utilisateurs du système d'information (c'est-à-dire les collaborateurs de la division 'analyse') qui seront responsables du contrôle de la qualité, et non plus l'organe interne de contrôle de la qualité. Ce dernier ne procède plus qu'à des contrôles périodiques par sondage.

D'importantes ressources humaines devraient être libérées du côté des utilisateurs pour le contrôle de qualité, ne serait-ce que pour garantir que le contrôle ne subisse aucune réduction au niveau de la qualité, dans IASA SRC, des données traitées auparavant dans ISIS.

Étant donné que l'on ne trouve dans les explications du message relatives aux besoins en personnel aucune mention de cette problématique, un retour en arrière par rapport aux acquis de la LMSI semble inévitable. Il faut également souligner qu'au cours des dernières années, le service d'analyse n'a quasiment pas profité des ressources supplémentaires octroyées au SRC.

La haute surveillance parlementaire risque donc, au bout de quelques années, de parvenir à la même conclusion que pour son inspection ISIS, à savoir que le SRC n'était pas en mesure, pour le système IASA SRC, d'effectuer les contrôles relatifs à la protection des données voulus par la loi.

Tandis que le P-LRens exige obligatoirement que les informations relatives à l'extrémisme violent soient traitées exclusivement dans le système IASA-EXTR SRC, toutes les autres informations pertinentes pour le renseignement peuvent en principe être enregistrées dans le système de stockage des données résiduelles en vertu de l'art. 56 P-LRens. Selon les explications, les informations proviendraient de l'exploration radio et de l'exploration du réseau câblé, de services partenaires et d'informateurs (message LRens, p. 88). Les données issues de l'actuel système de stockage des données brutes (cf. plus haut) devraient également pouvoir y être versées.

Les collaborateurs du SRC décident au cas par cas de transférer sous forme structurée les annonces archivées dans le système de stockage des données résiduelles vers le système IASA SRC. Par conséquent, ce sont également eux qui décident de l'intensité du contrôle de qualité pour ces informations.

En effet, contrairement au système IASA SRC, par exemple, le contrôle périodique n'est pas effectué dans le système de stockage des données résiduelles au moyen de toutes les informations classées relatives à une personne (bloc de données), mais uniquement pour l'annonce entrée et classée dans le système de stockage des données résiduelles.

L'efficacité de cette forme de contrôle de la qualité se limite à la détection de lacunes au sein d'une annonce. Par conséquent, l'exactitude et la pertinence des informations contenues dans cette annonce ne sont pas vérifiées à travers d'autres informations. Un utilisateur compétent peut éventuellement constater lors du contrôle qu'une information ne correspond pas au niveau de connaissances qu'il a lui-même et décider si, pour cette raison, elle doit être effacée.

Si le SRC omet de transférer une information versée dans le système de stockage des données résiduelles vers le système IASA SRC, ces données restent soumises à ce seul dispositif de protection des données, peu efficace.

Par ailleurs, la loi ne règle pas la question de savoir si l'effacement dans IASA SRC d'une personne enregistrée et de ses données a pour effet que les copies de ces données doivent également être effacées dans le système de stockage des données résiduelles. L'art. 43, al. 3, P-LRens autorise en effet explicitement le SRC à verser les mêmes données dans plusieurs systèmes et à les traiter en fonction des dispositions spécifiques à chacun de ces systèmes.

Contrairement à ce qu'indique son nom, le système de stockage des données résiduelles s'avère être le système d'information qui, par rapport aux autres systèmes d'information, devrait, et de loin, stocker le plus données et qui, cependant, est soumis en même temps aux contrôles de qualité les moins stricts.

La question se pose donc de savoir s'il ne faudrait pas compenser l'efficacité limitée du contrôle de qualité telle qu'elle ressort de l'art. 56, al. 2, P-LRens par une limitation de la durée de conservation. Une durée maximale de dix ans semble opportune, car, durant cet intervalle, le SRC peut vraisemblablement transférer dans le système IASA SRC, à des fins d'analyse, les données qui l'intéressent réellement. Dans le même temps, la réduction du volume de données garantit que la charge de travail liée au contrôle de qualité n'explosera pas.

25. Question non résolue du rapport coût-utilité de Quattro P / P4 (art. 54)

Problématique

La DélCdG considère que l'actuel programme fondé sur le contrôle des photos d'identité, qui fournit les données pour le système Quattro P, n'est pas satisfaisant s'agissant du rapport charges-recettes et a, en collaboration avec la DélFin, recommandé son abrogation. Une disposition potestative permettrait de lier la poursuite du programme à son efficacité.

Proposition de la DélCdG

Art. 54, al. 1, P-LRens (modification) : Le SRC *peut* exploiter un système d'information qui sert à identifier certaines catégories de personnes étrangères qui entrent en Suisse ou qui sortent du territoire suisse et à déterminer les dates de leur entrée et de leur sortie.

Justification

Les dispositions relatives au système d'information Quattro P correspondent aux prescriptions de la base de données P4 concernant le programme fondé sur le contrôle des photos d'identité. Si, comme le prévoit le P-LRens, la base de données est ancrée dans la loi, le législateur mandate le Conseil fédéral pour qu'il poursuive le programme fondé sur le contrôle des photos d'identité, dont la DélCdG avait recommandé initialement qu'il y soit mis un terme (rapport annuel 2013 de la DélCdG, ch. 4.2.5, p. 70 et suiv.).

Si toutefois la poursuite du programme venait à dépendre de son efficacité, l'art. 54 P-LRens devrait régir ce système par le biais d'une disposition potestative.

26. Contrôles de qualité des informations provenant de mesures de recherche soumises à autorisation (art. 46 et 57)

Problématique

Le P-LRens ne prévoit pas de contrôle de la protection des données justement pour les données personnelles que le SRC a désormais le droit de collecter, sur la base des nouveaux moyens de recherche conformément à l'art. 25 P-LRens, dans le domaine de la sphère privée, qui lui était inaccessible jusqu'à présent. Pour que cette lacune soit comblée, ces données ne doivent plus être exclues des dispositions générales de l'art. 46 P-LRens. De plus, les données qui n'ont aucun lien avec la mesure de recherche autorisée doivent être effacées le moment venu (cf. proposition au point 13, qui s'inspire du projet initial LMSI II de 2007).

Proposition

Art. 46, al. 1, let. h (nouveau) *le système d'information pour le traitement de données visées à l'art. 57*.

Proposition du point 13 pour le nouvel art. 31*a*, al. 1, P-LRens.

Justification

En vertu de l'art. 57 P-LRens, les données provenant d'une mesure de recherche soumise à autorisation (art. 25 P-LRens) sont traitées dans des systèmes d'information distincts. Cela concerne également les données émanant de la recherche sur des événements se produisant à l'étranger, comparables aux mesures de recherche soumises à autorisation (art 35, al. 5, P-LRens).

Il ressort des explications que les données collectées peuvent être très volumineuses et « contenir de nombreuses informations n'ayant aucun rapport avec le but de la recherche, parce qu'elles sont par ex. de nature strictement privée » (message LRens, p. 88). Cette précision concerne probablement en premier lieu les données qui sont collectées par le biais de l'introduction dans des systèmes informatiques.

Les dispositions générales qui sont applicables à tous les systèmes d'information sur la base de l'art. 46 P-LRens ne valent pas pour le système visé à l'art. 57 P-LRens. Elles sont remplacées par une réglementation spéciale aux termes de l'art. . 57, al. 4, P-LRens. Le Conseil fédéral doit certes régler la durée maximale de conservation des données (art. 57, al. 4, let. c, P-LRens), mais aucun contrôle de qualité n'est prévu.

Par conséquent, le P-LRens ne prévoit pas de contrôle sérieux de la protection des données justement pour les données personnelles que le SRC a désormais le droit de collecter, sur la

base des nouveaux moyens de recherche conformément à l'art. 25 P-LRens, dans le domaine de la sphère privée, qui lui était inaccessible jusqu'à présent.

Il est donc nécessaire que le traitement des données au sens de l'art. 57 P-LRens soit lui aussi soumis aux règles générales stipulées à l'art. 44 et à l'art. 46 P-LRens. A cette, fin, le système concerné doit être intégré dans l'énumération des systèmes d'information à l'art. 46, al. 1, P-LRens, faute de quoi il pourrait être permis de biffer l'art. 57, al. 4, P-LRens.

De plus, la durée de conservation des données, en particulier du volume important de données qui n'ont aucun rapport avec le but de la recherche, devrait être limitée. C'est notamment le but de la proposition formulée au point 13 du présent document, conformément au projet de LMSI II de 2007, d'introduire un *nouvel* art. 31*a*, al. 1, P-LRens.

27. Transmission de données personnelles à des autorités étrangères (art. 60)

Problématique

Les dispositions de l'art. 60 P-LRens ne sont pas suffisamment claires et ne permettent pas de savoir dans quelle mesure la transmission de données personnelles à l'étranger dépend de la question de savoir si l'Etat concerné garantit un niveau de protection des données comparable à celui de la Suisse. Seule une nouvelle systématique au sein de l'article permettrait de clarifier les choses. Lors de la consultation des offices, l'Office fédéral de la justice (OFJ) avait déjà soumis une proposition adéquate.

Recommandation de la DélCdG

La commission chargée de l'examen préalable prie l'OFJ de reformuler l'art. 60 P-LRens. La DélCdG propose les dispositions suivantes comme base du mandat à l'OFJ :

Art. 60 Transmission de données personnelles à des autorités étrangères

1 Le SRC peut, dans des cas particuliers, communiquer des données personnelles à l'étranger. Si la législation de l'Etat destinataire n'assure pas un niveau de protection adéquat des données, des données personnelles peuvent lui être communiquées si la Suisse entretient avec l'Etat destinataire des relations diplomatiques et que l'une des conditions suivantes est remplie :

a. la Suisse est tenue de lui communiquer les données personnelles en vertu d'une loi ou d'une convention internationale;

b. la communication est, en l'espèce, indispensable à la sauvegarde d'un intérêt public prépondérant;

c. la communication est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de tiers;

d. la personne concernée a donné son consentement ou les circonstances du cas d'espèce permettent de présumer un tel accord;

e. l'Etat destinataire fournit, dans le cas d'espèce, des garanties suffisantes permettant d'assurer, dans le cas d'espèce, un niveau de protection adéquat.

2 Il peut au surplus communiquer des données personnelles à des États avec lesquels la Suisse entretient des relations diplomatiques si l'Etat requérant assure par écrit disposer de l'accord de la personne concernée et avoir la possibilité de juger si cette personne peut collaborer à des projets classifiés du pays étranger dans le domaine de la sûreté intérieure et extérieure ou avoir

accès à des informations, du matériel ou des installations classifiés du pays étranger. [art. 17 al. 3 let. e LMSI]

3 Aucune donnée personnelle ne peut être communiquée à un Etat tiers si la personne concernée risque, par suite de la transmission de ces données, une double condamnation ou des préjudices sérieux contre sa vie, son intégrité corporelle ou sa liberté au sens de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, du 4 novembre 1950 ou d'autres instruments internationaux pertinents ratifiés par la Suisse.

4 Si la communication des données personnelles est requise dans le cadre d'une procédure, les dispositions pertinentes relatives à l'entraide judiciaire sont applicables.

5 Le Conseil fédéral détermine :

a. les destinataires autorisés;

b. l'étendue des garanties à fournir;

Justification

Hormis des modifications rédactionnelles, l'art. 60 P-LRens correspond au nouvel art. 6*h* LFRC, adopté par les Chambres fédérales lors de la session de printemps 2014 dans le cadre de la dernière révision de ladite loi. Cependant, ces nouvelles dispositions de la LFRC concernent exclusivement les informations qui proviennent de la recherche sur l'étranger. Dans le P-LRens, ces nouvelles règles valent également pour les données liées à la protection de l'État qui proviennent de Suisse, l'ancienne restriction de la transmission au cas particulier disparaissant cependant.

L'art. 60 P-LRens soulève des questions, en particulier concernant l'application future, auxquelles ni le texte de loi ni les explications y relatives n'apportent de réponse concluante.

L'art. 60, al. 1, P-LRens est-il désormais la règle et le SRC doit-il, dès que cela s'avère possible, obtenir des garanties suffisantes pour la protection de la personne afin de transmettre des données à l'étranger en dérogation aux dispositions relatives à la protection des données ? Ces garanties concernent-elles la personne même ou seulement ses données ?

L'art. 60, al. 1, P-LRens doit-il être considéré comme une *lex specialis* par rapport à l'art. 6, al. 2, LPD, dont les exceptions, selon le message, doivent s'appliquer si l'État étranger ne dispose pas d'une législation relative à la protection des données comparable à celle de la Suisse (message LRens, p. 90) ? Partant, le SRC peut-il ne s'appuyer que sur les garanties de l'étranger (comme pour l'art. 6, al. 2, let. a, LPD) et non sur les autres mesures prévues par la LPD pour la transmission de données à des pays qui ne garantissent pas un niveau de protection des données comparables à celui de la Suisse ?

L'art. 60, al. 2, P-LRens présuppose-t-il que le pays étranger garantit un niveau de protection des données comparables ou ce deuxième alinéa n'intervient-il que lorsque le SRC ne peut obtenir du pays étranger les garanties visées à l'al. 1 ?

Étant donné que l'art. 60, al. 3, P-LRens exige dans tous les cas qu'aucune donnée ne soit transmise à l'étranger si, en raison de la transmission de données, la personne concernée risque un préjudice sérieux contre sa vie, son intégrité corporelle ou sa liberté, la question se pose de savoir si, dans ces circonstances, le SRC serait même habilité à demander une garantie pour la protection de la personne.

Il faudrait également clarifier les circonstances dans lesquelles un service partenaire peut garantir suffisamment la protection d'une personne si celle-ci se trouve en Suisse ou dans un pays tiers.

Lors de la consultation des offices, l'OFJ avait proposé au SRC une autre règle pour la transmission de données à l'étranger. Celle-ci pourrait, sous une forme simple et adaptée, lever les ambigüités de l'actuel art. 60 P-LRens.

28. Droit d'accès (art. 63)

Problématique

Le Conseil fédéral est d'avis que les dispositions de l'actuel art. 18 LMSI devraient être reprises dans le P-LRens. Une faute rédactionnelle dans l'art. 63, al. 2, P-LRens a toutefois pour effet que le PFPDT doit désormais trancher entre l'une des deux réponses à apporter au requérant plutôt que communiquer une réponse toujours formulée de manière identique, comme le stipule le droit actuel et comme l'exige explicitement l'art. 65, al. 1, P-LRens.

Proposition de la DélCdG

Art. 63, al. 2, P-LRens (modification) Il indique à la personne concernée*: soit qu'aucune donnée la concernant n'est traitée illégalement, soit qu'il a constaté une erreur relative au traitement des données ou au report de la réponse et qu'il a adressé au SRC la recommandation d'y remédier en vertu de l'art. 27, LPD.* [comme art. 18, al. 4, LMSI]

Remarques

Selon les explications du message, le projet, s'agissant du droit d'accès, reprend dans une large mesure la solution adoptée par le Parlement dans le cadre du message complémentaire à la LMSI II sur la base de l'art. 8 LSIP (Loi fédérale sur les systèmes d'information de police de la Confédération.

Cela est certes vrai, mais les explications ne précisent pas que, dans le cadre de la dernière révision de la LFRC, une solution moins restrictive basée sur les art. 8 et 9 LPD avait été proposée au travers de l'art. 6*j* LFRC pour les données provenant de la recherche d'informations sur l'étranger. Cette solution a du reste été acceptée par les Chambres fédérales lors de la session de printemps. Au niveau de l'ordonnance, elle était en vigueur dès le début 2010 pour le système ISAS (art. 23 OSI-SRC).

Par conséquent, le P-LRens uniformise le droit d'accès en s'appuyant sur l'approche plus restrictive des solutions légales retenues jusqu'à présent.

Cela a pour effet que, pour plus de la moitié des données du SRC en lien avec les personnes, le droit d'accès est restreint par rapport aux dispositions légales en vigueur jusqu'à présent.

29. Archivage (art. 67)

Problématique

Le projet ne mentionne nulle part la nouvelle règle d'archivage en vigueur pour le SRC que les deux conseils ont élaborée dans le cadre de la révision de la LFRC et sur la base du co-rapport de 2013 adressé par la DélCdG à la CAJ-E. Une nouvelle solution est de nouveau proposée au Parlement sans justification aucune. Celle-ci est non seulement superflue, mais également inappropriée, car elle repose sur un manque de compréhension de la loi sur l'archivage. Pour cette raison, les Chambres fédérales devraient conserver, pour l'art. 67, al. 2, P-LRens, la règle qu'ils ont approuvée il y a peu dans l'art. 7*a*, al. 2, LFRC.

Proposition de la DélCdG

Art. 67, al. 2, P-LRens (modification) *Le Conseil fédéral peut, selon l'article 12 de la loi fédérale du 26 juin 1998 sur l'archivage, prolonger de façon répétée pour une durée limitée le délai de protection applicable aux archives qui proviennent d'un service de sûreté étranger, si le service concerné émet des réserves sur une éventuelle consultation. [comme art. 7a, al. 2, LFRC]*

Justification

Dans son co-rapport du 9 octobre 2013 relatif à la révision de la LFRC (13.064), la DélCdG proposait une solution pour l'archivage des documents du SRC qui était basée dans une large mesure sur les dispositions de la loi sur l'archivage (LAr). Pour les documents qui proviennent de services étrangers, le délai de protection ne doit cependant plus expirer au bout d'une durée unique de 50 ans, mais le Conseil fédéral doit pouvoir régulièrement le prolonger et ce, tant que le service étranger concerné demande cette prolongation.

Les deux conseils ont repris l'intégralité de la proposition de la DélCdG dans l'art. 7*a*, al. 1 et 2, LFRC. Le Parlement n'a pas suivi en particulier la contre-proposition que le DDPS avait encore soumise à la commission du conseil prioritaire (CPS-E).

La protection particulière des documents qui proviennent de services étrangers s'appuie sur la prolongation du délai de protection telle qu'elle est prévue à l'art. 12, al. 1, LAr.

Ces délais de protection prolongés sont présentés en annexe 3 de l'ordonnance sur l'archivage (OLAr). Ils concernent des documents relatifs aux mandats sur la base desquels la Suisse représente les intérêts de pays tiers. Des exemples connus en sont l'Iran et les États-Unis ainsi que la Russie et la Géorgie.

Dans l'art. 67, al. 2, P-LRens, le Conseil fédéral déroge à la solution approuvée récemment par les Chambres fédérales : au lieu de s'appuyer sur la prolongation du délai de protection conformément à l'art. 12, al. 1, LAr, la nouvelle proposition du Conseil fédéral est basée sur l'art. 12, al. 2, LAr. Or, le 2e alinéa de l'art. 12 LAr ne peut être appliqué que pour certaines archives et ne peut s'appliquer qu'une fois que leur délai de protection est levé. L'art. 12, al. 2, LAr a pour unique but de limiter de nouveau, a posteriori, l'accès aux documents si leur délai de protection a été levé trop tôt par erreur. La législation en vigueur sur l'archivage offre d'ores et déjà cette possibilité.

En revanche, les dispositions que les Chambres fédérales ont adoptées sur proposition de la DélCdG exigent de vérifier avec le service partenaire étranger si le délai de protection peut véritablement être levé pour une catégorie de documents sans qu'il faille craindre que, par la suite, l'accès à certains de ces documents doive être retiré.

30. Liste d'observation (art. 71)

Problématique

Dans le cadre de la révision LMSI II, les Chambres fédérales ont repris une règle selon laquelle le Conseil fédéral devrait inscrire sur la liste d'observation, sans autres vérifications, les organisations qui figurent sur une liste du terrorisme de l'UE ou de l'ONU.

Or, un avis de droit de la DélCdG demandé à l'OFJ a montré que cela établissait un automatisme indésirable entre ces listes et la liste d'observation. Malheureusement, le nouvel art. 71 P-LRens ne remédie que partiellement à ce problème.

Proposition de la DélCdG

Il convient de clarifier la question de savoir si le but de l'art. 71 P-LRens est effectivement qu'une organisation qui a été inscrite sur la liste d'observation, non pour des raisons réelles mais pour sa simple mention dans une liste internationale, ne peut pas en être radiée tant qu'elle sera sur une liste internationale.

Si l'art. 71 P-LRens ne définit pas une telle « voie à sens unique » mais a pour but d'accorder au Conseil fédéral la latitude nécessaire pour radier une telle organisation de la liste, il convient de le formuler dans ce sens.

Justification

Les dispositions relatives à la liste d'observation (art. 11 LMSI) ont été adaptées lors de l'examen du message complémentaire à la révision LMSI II du 27 octobre 2010. Bien que cela ne fût pas l'intention du SRC, le nouveau texte établissait un automatisme entre les organisations figurant sur les listes du terrorisme de l'UE et de l'ONU et les organisations figurant sur la liste d'observation. Contrairement à ce que pensait le SRC, une autre interprétation n'était pas possible, comme l'a montré l'avis de droit de l'OFJ du 5 avril 2013, demandé par la DélCdG.

C'est la raison pour laquelle la DélCdG a souligné dans son rapport annuel 2013 que, lors de l'examen du P-LRens par les Chambres fédérales, il faudrait clarifier les relations entre les listes internationales du terrorisme et la liste d'observation suisse. Elle y précisait qu'il y aurait également lieu de garantir que les dispositions votées par le Parlement correspondent à la volonté politique, sans la moindre marge d'interprétation.

Or, aux termes de l'art. 71, al. 2, P-LRens, il suffit désormais qu'une organisation figure, par exemple sur la liste de l'UE, pour qu'elle soit présumée menacer la sûreté de la Suisse (fiction juridique). Dans ce cas, le Conseil fédéral peut l'inscrire sur la liste d'observation sans devoir apporter de justifications supplémentaires quant à sa dangerosité. Il le peut mais il n'est pas obligé de le faire. Lorsqu'une telle organisation est inscrite sur la liste suisse, il n'y a donc pas d'automatisme entre les listes.

Le texte ne dit cependant pas si une organisation qui a été inscrite sur la liste d'observation uniquement sur la base de la fiction juridique de l'alinéa 2 pourra par la suite en être radiée si elle figure toujours sur une liste internationale, par exemple sur celle de l'UE.

Si aucun indice réel ne permet d'affirmer que l'organisation menace la sûreté de la Suisse, celle-ci devrait pouvoir être radiée de la liste en vertu de l'art. 71, al. 3, let. a, P-LRens.

Étant donné toutefois que la fiction juridique de l'alinéa 2 maintient l'hypothèse selon laquelle l'organisation constitue une menace tant qu'elle figure sur la liste de l'UE, on est en droit de se demander si l'art. 71, al. 3, let. a, P-LRens peut être appliqué et, partant, si l'organisation peut être radiée de la liste.

L'art. 71, al. 3, let. b, P-LRens n'est pas applicable dans ce cas étant donné qu'il présuppose que l'organisation ne figure plus sur aucune liste internationale. L'art. 71 P-LRens ne contient pas une lettre c pour la radiation dans le cas où l'organisation figure toujours sur une liste internationale.

31. Conséquences sur l'état du personnel (ch. 3.1.2 du message)

Problématique

Lors de son inspection relative à la sécurité informatique au sein du SRC, la DélCdG était parvenue à la conclusion qu'une importance trop faible avait été accordée à la question des effectifs de personnel nécessaires lors de la création du SRC. Elle avait en outre constaté que pas même la moitié des besoins en personnel prévus dans le projet de LMSI II de 2007, moins ambitieux, n'était présentée dans le rapport de consultation sur la LRens. Afin d'éviter qu'un déséquilibre entre tâches nouvelles et ressources ne voue à l'échec la plus grande réforme du Service de renseignement suisse jamais entreprise jusque-là, la DélCdG avait exigé que le Conseil fédéral présente au Parlement une analyse approfondie des besoins en ressources humaines. Bien que celui-ci ait promis de mettre en œuvre cette recommandation au travers de son message sur la LRens, il ne s'est jamais acquitté du mandat de la DélCdG.

Proposition de la DélCdG

Le Conseil fédéral doit présenter dans un message complémentaire les clarifications demandées par la DélCdG dans sa recommandation 1 de l'inspection relative à la sécurité informatique au sein du SRC. Une version confidentielle peut éventuellement être établie à l'intention de la DélCdG et de la DélFin.

Justification

Se basant sur son inspection relative à la sécurité informatique au sein du SRC, la DélCdG était parvenue à la conclusion qu'une importance trop faible avait été accordée à la question des effectifs de personnel nécessaires lors de la fusion des services de renseignement civils au sein du DDPS et de la création du SRC qui s'en était suivie. Elle était d'avis que la pénurie de personnel dans le service informatique avait rendu impossible une gestion des risques adéquate par le SRC.

Craignant que la mise en œuvre du P-LRens ne pose au service de renseignement des défis semblables à ceux qu'avait posés la création du SRC, la DélCdG a souhaité éviter que les erreurs commises alors ne se reproduisent. C'est la raison pour laquelle elle a demandé au Conseil fédéral dans la première recommandation de son rapport d'inspection de charger le DDPS d'effectuer une analyse approfondie et détaillée des ressources humaines qui seraient nécessaires pour la réalisation des tâches supplémentaires que le P-LRens propose. La recommandation a été remise au Conseil fédéral le 2 juillet 2013, c'est-à-dire après que le P-LRens a été mis en consultation.

Le message du 19 février 2014 à l'intention des Chambres fédérales ne mentionne pas la recommandation 1 de la DélCdG et les explications ne contiennent pas l'analyse demandée.

Les explications relatives aux répercussions sur les effectifs (ch. 3.1.2) ne se distinguent en rien ou presque du message concernant la procédure de consultation. La seule différence réside dans le fait que le Conseil fédéral prévoit désormais la création de 20,5 postes contre 16 auparavant. On notera cependant qu'une partie est prévue pour des postes en-dehors du SRC (TAF, Archives fédérales, COE).

On ne sait pas si les deux postes supplémentaires attribués au SRC et au COE, lesquels sont évoqués dans les explications relatives à l'art. 42 P-LRens et sont nécessités pour l'exploitation test de l'exploration du réseau câblé, font ou non partie de ces 20,5 postes.

Le flou règne également s'agissant des besoins en personnel pour le contrôle de qualité des données du SRC. On peut lire, d'une part que des postes supplémentaires doivent être créés

pour la garantie de la qualité, en particulier des nouveaux systèmes d'information, d'autre part que l'augmentation des exigences pour la gestion des données peut en grande partie être assumée avec les ressources disponibles (message LRens, p. 120).

La proposition du DDPS à l'intention du Conseil fédéral en date du 10 février 2014 ne contient elle non plus aucune analyse allant au-delà du message. Il y est seulement indiqué que les calculs détaillés afférents aux postes ont été communiqués au DFF.

Ni le DDPS ni le Conseil fédéral n'ont communiqué à la DélCdG un complément d'informations concernant la mise en œuvre de sa recommandation.

Sachant que le Conseil fédéral avait prévu 40 postes supplémentaires pour le projet initial LMSI II, son estimation actuelle de 20,5 postes paraît très problématique.

La LRens introduit en effet de nouveaux moyens de recherche, non seulement pour le renseignement intérieur mais également pour l'étranger. De plus, les moyens de recherche d'informations vont plus loin que dans le projet initial de LMSI. Enfin, le champ d'activité est étendu dans la pratique à la protection des infrastructures critiques et potentiellement à la politique extérieure ainsi qu'à la protection de la place industrielle, économique et financière.

Rien que pour cette dernière mission, le DDPS avait, dans une analyse effectuée en 2011, estimé à environ 20 postes à temps complet les besoins pour les domaines de la collecte et de l'analyse.

Selon une évaluation récente, une demi-douzaine de postes supplémentaires ne suffirait pas au SRC pour remplir ses missions légales actuelles dans le domaine du contre-espionnage.