14.004

Rapport annuel 2013 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales

du 31 janvier 2014

Messieurs les Présidents,
Mesdames et Messieurs,

Conformément à l'art. 55 de la loi du 13 décembre 2002 sur l'Assemblée fédérale (loi sur le Parlement, LParl; RS *171.10*), nous vous soumettons le rapport d'activité des Commissions de gestion et de leur délégation pour l'année 2013 et vous demandons de bien vouloir en prendre connaissance.

Le présent rapport donne des indications sur les principaux contrôles effectués durant l'année et dégage les résultats et les enseignements qui peuvent en être tirés. Il accorde également une attention particulière aux suites données aux recommandations des commissions et de la délégation.

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

31 janvier 2014

Au nom des Commissions de gestion des Chambres fédérales:

Le président de la CdG-N,
Rudolf Joder, conseiller national

Le président de la CdG-E,
Hans Hess, conseiller aux Etats

Pour cette raison, le Conseil fédéral a décidé que les services linguistiques et le service juridique de la ChF contrôleraient désormais aussi la qualité des actes et des traités internationaux qui ne sont pas publiés en vertu de l'art. 6 LPubl. Par ailleurs, il convient de préciser, dans les directives sur les affaires du Conseil fédéral, que les offices doivent également être consultés – de manière confidentielle – sur les textes juridiques non publiés.

Le Conseil fédéral a déclaré qu'il avait chargé la ChF d'élaborer et de mettre en œuvre pour la fin du mois de juin 2013, en collaboration avec le DDPS, une stratégie visant à contrôler la qualité des textes juridiques concernés par l'art. 6 LPubl, par analogie avec la procédure du « circuit » électronique. Il a également chargé la ChF d'inscrire dans les directives sur les affaires du Conseil fédéral, également pour fin juin 2013, l'obligation de consulter les offices sur les textes juridiques concernés par l'art. 6 LPubl et de contrôler la qualité de ces textes par analogie avec la procédure du « circuit » électronique. Au préalable, la ChF devra déjà veiller, conjointement avec les services concernés (notamment le DDPS), à ce que tous les textes concernés par l'art. 6 LPubl soient soumis à un contrôle de la qualité.

En ce qui concerne l'organe de la ChF qui, selon la proposition de la DélCdG, serait chargé de centraliser les textes juridiques visés par l'art. 6 LPubl, le Conseil fédéral a rappelé que ces textes n'étaient pas publiés pour des raisons liées au maintien du secret et que, partant, ils ne devraient être accessibles qu'à un cercle restreint de personnes. Toutefois, le Conseil fédéral est disposé à vérifier s'il est possible d'instituer un tel organe et, le cas échéant, à quelles conditions. Il a souligné que le DFAE avait déjà créé, en son sein, un organe chargé de rassembler les traités internationaux (y c. les accords concernés par l'art. 6 LPubl). Pour ces raisons, le Conseil fédéral a chargé la ChF d'examiner pour la fin du mois de juin 2013, en collaboration avec le DDPS, comment fonctionnerait un tel organe au sein de la ChF et quelles seraient ses attributions.

Les investigations menées en 2013 par la ChF et le DDPS en la matière se sont manifestement heurtées à certains problèmes, car la DélCdG n'a été informée de leurs résultats que le 7 octobre 2013. Comme l'a écrit la ChF, l'examen a montré « qu'un dépôt de ce type [géré par l'organe chargé de centraliser les actes non publiés] n'était pas indiqué à l'heure actuelle, pour diverses considérations pratiques ainsi qu'en raison de la protection des informations »[94].

4.2 Suivi du rapport de la Délégation des Commissions de gestion sur le système ISIS

4.2.1 Evolution de la base de données dans le système ISIS

Dans son rapport d'inspection du 21 juin 2010[95] sur le système d'information relatif à la protection de l'Etat ISIS[96], la DélCdG était parvenue à la conclusion que l'assurance de la qualité des données contenues dans le système ne répondait pas aux prescriptions légales. Les contrôles périodiques de la qualité ont notamment été

94 Lettre de la ChF du 7.10.2013 à l'intention de la DélCdG

95 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS), rapport de la DélCdG du 21.6.2010 (FF **2010** 7003)

96 Avant 2010, ISIS signifiait « informatisiertes Staatsschutzinformationssystem » ; aujourd'hui, il est l'acronyme de « Informationssystem Innere Sicherheit ».

reportés d'année en année. Cette situation découlait aussi des difficultés imprévues liées au passage à un nouveau système informatique fin 2004.

Sur la recommandation de la DélCdG, le SRC a effectué les contrôles concernés, avec le soutien d'un préposé externe à la protection des données, achevant ses travaux fin 2012. A la suite de ces contrôles, le nombre des personnes et des tiers enregistrés dans ISIS a diminué de 80 %. Vers la moitié de l'année 2013, 36 000 personnes et 5000 tiers environ étaient encore enregistrés dans ISIS ; ce nombre a très peu évolué sur le reste de l'année.

En 2013, le nombre des institutions est passé au-dessous du seuil des 10 000. Ce nombre, qui inclut les institutions tierces, s'élevait encore à quelque 16 000 à la fin de l'année 2010.

En 2009, le TAF avait critiqué la pratique consistant à enregistrer des médias (par ex. des journaux) dans ISIS en tant qu'objets distincts, arguant qu'une telle pratique ne peut être compatible avec l'art. 3 LMSI que « si l'activité médiatique sert de couverture pour dissimuler la préparation ou l'exécution d'actes relevant du terrorisme, du renseignement ou de l'extrémisme violent »[97] .Le SAP (Service d'analyse et de prévention) comme institution compétente, remplacée ultérieurement par le SRC, s'était alors engagée à remplir cette exigence du TAF.[98]

Lors de son contrôle de suivi concernant l'inspection ISIS, la DélCdG avait constaté que, contrairement aux autres catégories d'objets, jusqu'à fin 2011 le nombre de médias enregistrés dans ISIS n'avait pratiquement pas évolué. C'est ensuite seulement que ce chiffre a commencé à diminuer; d'abord de moitié en 2012, pour atteindre une centaine de médias, puis d'un quart supplémentaire jusqu'au milieu de l'année 2013. Après une nouvelle augmentation durant l'automne, ce chiffre est retombé à environ 60 unités à la fin de 2013.

Pour vérifier si, ces dernières années, le SRC avait effectivement entrepris ce qu'il fallait pour satisfaire aux exigences posées par le TAF, la DélCdG a exigé qu'il lui communique les noms des médias encore enregistrés dans ISIS à fin 2013. La haute surveillance n'avait pas à évaluer de manière définitive si ces médias – pour la plupart étrangers – représentaient un intérêt du point de vue de la protection de l'Etat. Néanmoins, la DélCdG a pu relever quelques cas qui, conformément aux critères énoncés par le TAF en 2009, n'auraient de toute évidence pas dû être enregistrés dans ISIS. La délégation en conclut que le SRC n'a pas encore achevé l'examen des médias enregistrés dans ISIS, exigé par le TAF.

4.2.2 Séparation des données administratives de celles relevant de la protection de l'Etat

La recommandation 6 du rapport ISIS de la DélCdG demandait au Conseil fédéral de pourvoir à ce que seules les données relevant de la protection de l'Etat soient enregistrées dans la banque de données « ISIS01 Protection de l'Etat ». La délégation voulait ainsi éviter que, à l'avenir, des personnes dont le SRC – à l'instar d'autres services de la Confédération – doit s'occuper pour des raisons

97 Arrêt non publié du TAF du 18.3.2009 (A-5919/2008) [en allemand]
98 Lettre du SAP au TAF du 8.9.2009

administratives ne fassent l'objet d'un enregistrement dans ISIS01. La DélCdG avait constaté ce problème lorsqu'elle avait elle-même consulté ISIS par sondage[99].

Dans son rapport, la DélCdG avait expressément souligné que les documents issus de l'activité administrative du SRC devaient être enregistrés dans « ISIS02 Administration » et que seule la base de données ISIS01 pouvait contenir des informations relevant de la protection de l'Etat[100].

Pour répondre à la recommandation de la DélCdG, le directeur du SRC a édicté, le 1er juin 2011, une directive concernant le traitement des données dans ISIS02. Aux termes de celle-ci, les données administratives doivent désormais être enregistrées uniquement dans la banque de données ISIS02 et non plus dans la banque ISIS01. Cette directive n'avait toutefois aucune incidence sur les données administratives qui avaient déjà été enregistrées par erreur dans ISIS01.

Comme la DélCdG l'a souligné dans son rapport annuel 2012, la recommandation 6 ne pourra être considérée comme mise en œuvre qu'une fois que toutes les données de nature purement administrative auront été supprimées de la banque de données relevant de la protection de l'Etat et, éventuellement, transférées dans un autre système[101]. Pour cette raison, à la mi-avril 2013, le SRC a présenté à la DélCdG – à la demande de cette dernière – un rapport faisant état de la mise en œuvre de cette recommandation[102].

Selon ce rapport, le SRC a pu introduire, fin 2012, un système de gestion électronique des affaires (« GEVER SRC ») appelé à remplacer ISIS02. Depuis, les documents administratifs ne sont plus enregistrés dans ISIS02, mais dans ce nouveau système. Les données administratives déjà enregistrées dans ISIS02 doivent être transférées dans GEVER SRC dans le cadre de la dissolution intégrale du système ISIS.

La question se posait toutefois de savoir si ISIS01 contenait des données administratives qui y avaient été enregistrées avant l'entrée en vigueur de la directive du directeur du SRC du 1er juin 2011 et qui n'avaient pas encore été découvertes et supprimées à la suite d'une appréciation générale. Comme l'a appris la DélCdG en octobre 2012, le SRC est parti du principe que toutes ces données et les personnes concernées avaient été identifiées dans ISIS01[103].

Selon les explications du SRC il était techniquement impossible, avant la migration des données relevant de la protection de l'Etat d'ISIS01 au nouveau système, de supprimer les données administratives qui avaient été enregistrées par erreur dans ISIS01 et qui s'y trouvaient encore. Ces données ne pourraient être déplacées dans GEVER SRC qu'après la migration.

99 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS), rapport de la DélCdG du 21.6.2010 (FF **2010** 7003, ici 7017)

100 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS), rapport de la DélCdG du 21.6.2010 (FF **2010** 7003, ici 7051)

101 Rapport annuel 2012 des CdG et de la DélCdG des Chambres fédérales du 24.1.2013, ch. 4.3.7 (FF **2013** 3073, ici 3151)

102 Rapport du SRC du 15.4.2013 sur l'état de la mise en œuvre de la recommandation 6 relative au traitement des données dans ISIS (données administratives), p. 2 [en allemand]

103 Courriel du SRC au secrétariat de la DélCdG du 21.10.2013

4.2.3 Conservation illicite dans la base de données « Administration » du système ISIS de copies des informations supprimées

En vertu de l'art. 15, al. 1, LMSI, le SRC est tenu d'effacer les informations qu'il a traitées et qui ne sont plus pertinentes pour la protection de l'Etat. Le SRC est appelé à déterminer si une personne doit être supprimée de la banque de données dans le cadre de l'examen global périodique (art. 15, al. 5, LMSI) ou en contrôlant, lors de la saisie d'une nouvelle information, l'importance que revêt une personne pour la protection de l'Etat (art. 29, al. 2, OSI-SRC ; cette disposition a été ajoutée en réponse à la recommandation 8 du rapport ISIS, cf. ch. 4.2.6).

La directive du directeur du SRC du 1er juin 2011 relative à ISIS02 (cf. ch. 4.2.2) prévoyait toutefois que les rapports qui permettaient de lever une suspicion documentée dans la banque de données relative à la protection de l'Etat – c'est-à-dire ISIS01 – devaient être saisis dans la base des données administratives, accompagnés du rapport sur lequel les soupçons se fondaient[104].

Concrètement, cela signifie qu'une copie de l'information qui a conduit à l'enregistrement d'une personne dans ISIS est enregistrée dans ISIS02 avant d'être effacée d'ISIS01 ; de même, ISIS02 contient toujours l'information ayant démontré l'absence de lien entre la personne et la protection de l'Etat. Ainsi, malgré leur suppression d'ISIS01, les deux informations n'ont pas été réellement effacées. Etant donné que toutes deux ont perdu l'importance qu'elles revêtaient pour la protection de l'Etat, la DélCdG s'est demandé si la directive du directeur du SRC ne contournait pas l'obligation de suppression visée à l'art. 15, al. 1, LMSI, vu que les données étaient simplement transférées dans une autre banque de données et y étaient enregistrées en tant que données administratives.

En avril 2013, la DélCdG a discuté de ce problème avec la Surveillance SR. Celle-ci a déclaré qu'elle organiserait, d'entente avec le chef du DDPS, une table ronde réunissant notamment l'OFJ et le PFPDT, afin d'aborder avec le SRC la question des bases légales applicables au traitement des données dans ISIS et de la légalité des réglementations internes du SRC.

Ladite table ronde a eu lieu le 10 juin 2013. Le 30 août 2013, la Surveillance SR a présenté ses résultats au chef du DDPS sous la forme d'un rapport. Elle y suggérait qu'il ne soit pas permis de copier dans ISIS02 les données relatives à une personne dont l'Assurance qualité devait effacer la mention dans ISIS01. De plus, il y aurait lieu d'effacer les copies de telles données qui avaient été enregistrées dans ISIS02 ou dans GEVER SRC sur la base de la directive du directeur du SRC.

Le 3 septembre 2013, le chef du DDPS a transmis le rapport à la DélCdG, informant cette dernière qu'il approuvait la recommandation de la Surveillance SR et qu'il avait demandé au SRC de la mettre en œuvre. En outre, il a accepté la deuxième recommandation concernant les données saisies à double dans les systèmes ISIS et ISAS (cf. ch. 4.3).

Le 9 septembre 2013, le directeur du SRC a remplacé sa directive du 1er juin 2011 par une nouvelle directive relative au traitement des données dans le système GEVER SRC. Aux termes de cette nouvelle directive, les rapports qui permettent de

104 Directive du directeur du SRC du 1.6.2011 relative au traitement des données dans la banque de données Administration (ISIS02), p. 2 [en allemand]

lever une suspicion documentée dans la banque de données ISIS01 ne doivent plus être enregistrés dans GEVER SRC, mais saisis temporairement dans ISIS, puis effacés conjointement avec les informations sur lesquelles les soupçons se fondent. Il est par contre possible d'enregistrer dans GEVER SRC une note indiquant que le SRC a traité, sur une certaine période, des données relatives à la personne ou à l'organisation concernée.

Dans la lettre qu'elle a envoyée au Conseil fédéral le 18 décembre 2013 à l'issue de son suivi, la DélCdG a salué la nouvelle directive du SRC, estimant que celle-ci correspondait désormais aux prescriptions légales.

4.2.4 Points en suspens à régler dans le système appelé à succéder à ISIS

Trois des recommandations du rapport ISIS de la DélCdG concernaient le système appelé à succéder à ISIS. Ainsi, la recommandation 16 visait à ne mettre en exploitation un nouveau système que s'il satisfaisait intégralement aux prescriptions légales. Par ailleurs, seules les données qui correspondaient à toutes les dispositions légales devaient être transférées. La DélCdG souhaitait ainsi empêcher que les erreurs commises fin 2004 (données de qualité insuffisante), lors de la mise en exploitation d'un nouveau système informatique pour ISIS, ne se reproduisent.

En outre, le Conseil fédéral a lié la mise en œuvre de deux autres recommandations à la mise en exploitation du système appelé à succéder à ISIS. Ce système vise à générer automatiquement des indicateurs sur la base desquels le DDPS pourra contrôler si l'assurance qualité fonctionne conformément aux prescriptions légales (recommandation 13) ; il doit également pouvoir montrer quand et à quelle fréquence une appréciation générale a été effectuée concernant une personne ou une institution (recommandation 14).

Considérant le calendrier du SRC, qui prévoyait de mettre en exploitation le nouveau système fin 2013, la DélCdG souhaitait savoir en temps utile si le système fonctionnerait conformément aux recommandations 13 et 14. Le SRC lui a présenté un court rapport sur ce point le 23 mai 2013.

Les fonctions statistiques prévues correspondent dans les grandes lignes aux informations que la Section Assurance qualité du SRC rassemblait jusqu'alors automatiquement ou manuellement. L'enregistrement entièrement automatisé des chiffres devrait permettre de faire disparaître les incohérences qui se produisaient régulièrement lorsque les statistiques étaient saisies manuellement.

Selon le rapport, le SRC a défini les indicateurs que le système devrait livrer en se fondant sur des entretiens avec le préposé externe à la protection des données, avec la Surveillance SR et avec des collaborateurs de la division Gestion de l'information du SRC. Le directeur du SRC et le chef du département, auxquels ces indicateurs devraient servir d'instruments de conduite, n'ont pas été impliqués.

Par ailleurs, le rapport indique que, désormais, toutes les appréciations générales pourront être identifiées par la date à laquelle elles ont eu lieu et par la personne responsable. Dans l'ancien système ISIS, seule la date de la dernière appréciation était mentionnée.

Selon la Surveillance SR, le SRC a rassemblé dans un même document les exigences légales sur lesquelles la future banque de données devra s'appuyer[105], conformément à la recommandation 16. L'objectif est de refléter la situation juridique en vigueur, c'est-à-dire les dispositions actuelles de la LMSI ; de plus, selon la Surveillance SR, cette liste fait partie des spécifications du projet IASA SRC[106]. Le système appelé à succéder à ISIS sera réalisé dans le cadre de ce projet.

La recommandation 16 visait également à ce que les données ISIS respectent toutes les prescriptions légales avant d'être transférées dans le nouveau système. Le SRC a affirmé avoir identifié les données administratives qui étaient encore enregistrées dans la banque de données relevant de la protection de l'Etat (ISIS01) ; de plus, il peut garantir que ces données seront transférées non pas dans le nouveau système, mais dans le système de gestion électronique des affaires « GEVER SRC » (cf. ch. 4.2.2). Si le SRC met à jour auparavant tous les médias qui sont encore enregistrés dans ISIS en tant qu'objets distincts (cf. ch. 4.2.1), la recommandation 16 peut être considérée comme mise en œuvre.

4.2.5 Deuxième version du programme de recherches fondé sur le contrôle des photos d'identité

Le programme préventif de recherches fondé sur le contrôle des photos d'identité a été introduit à l'époque de la guerre froide en tant qu'instrument de contre-espionnage et a notamment servi à surveiller les citoyens suisses qui se rendaient dans les pays d'Europe de l'Est. A la suite de l'affaire des fiches, l'utilisation de cet instrument a été limitée aux ressortissants de certains Etats étrangers franchissant la frontière suisse.

Il ressort du rapport ISIS de la DélCdG que ces contrôles ont à eux seuls entraîné l'enregistrement de quelque 52 000 personnes. Celles-ci ont été automatiquement enregistrées en tant que tiers dans ISIS, sans évaluation du risque concret qu'elles pouvaient représenter. La délégation a par conséquent émis des réserves quant à la légalité des enregistrements relatifs à ces tiers et a proposé de faire effacer tous les tiers saisis dans ISIS sur la seule foi du programme de recherches fondé sur le contrôle des photos d'identité (recommandation 2). Les données concernées ont été effacées en décembre 2010.

Dans son rapport, la DélCdG avait également recommandé au Conseil fédéral d'abandonner le programme préventif de recherches fondé sur le contrôle des photos d'identité (recommandation 12) ou, s'il devait décider de le poursuivre, de justifier son choix dans un rapport. Dans son avis du 20 octobre 2010, le Conseil fédéral a exprimé sa volonté de suivre la recommandation de la délégation et précisé que le SRC allait abandonner le programme préventif de recherches fondé sur le contrôle des photos d'identité tel qu'il était exploité à ce moment-là et utiliser les instruments existants (appareils à la frontière) dans un nouveau projet.

Avec la nouvelle version du programme préventif, le Conseil fédéral a donné suite aux critiques du rapport ISIS de la DélCdG sous l'angle juridique. Cette dernière

105 Rapport de la Surveillance SR du 6.3.2013, p. 23 [en allemand]
106 Système d'information et d'analyse *all source* du SRC

doute toutefois de plus en plus de l'opportunité et de l'efficacité du nouveau projet[107].

Début 2013, la DélCdG a effectué un état des lieux du programme préventif. Dans ses conclusions, elle a écrit au chef du DDPS que le programme n'était « ni adéquat ni efficace » et mobilisait « d'importantes ressources en personnel au SRC qui faisaient cruellement défaut dans d'autres domaines »[108]. Par conséquent, la DélCdG a recommandé au DDPS d'envisager sérieusement la possibilité de renoncer à ce programme.

Après avoir reçu une copie de la lettre de la DélCdG, la DélFin a écrit au chef du DDPS, le 22 février 2013, qu'elle soutenait clairement la position de la DélCdG.

En novembre 2013, la DélCdG a une nouvelle fois discuté de l'opportunité du programme préventif avec le chef du DDPS et le directeur du SRC. La délégation et le DDPS étaient unanimes à penser que le programme, sous la nouvelle forme que lui avait donnée le SRC, ne pouvait pas produire de résultat satisfaisant sous l'angle du rapport coût-utilité.

En réaction à la position de la DélCdG, qui recommandait encore une fois de mettre un terme au programme, le DDPS a souhaité savoir si le fait de le doter de nouveaux moyens techniques de saisie pouvait améliorer son opportunité. Il a alors été prévu de mener une étude de faisabilité sous la direction du Cgfr.

4.2.6 Remise en question de la mise en œuvre de la recommandation 8 en raison d'une modification d'ordonnance

Le 29 novembre 2013, le Conseil fédéral a approuvé la quatrième révision de l'OSI-SRC. Depuis la création du SRC, cette ordonnance fixe les règles applicables au traitement des données dans les différents systèmes d'information du SRC, notamment ISIS.

L'art. 29, al. 2, OSI-SRC prévoit dorénavant que les « collaborateurs chargés de la saisie des données examinent si une information permet de déduire la pertinence pour la protection de l'Etat de la personne ou de l'organisation à laquelle cette information se rapporte. Dans ce cas, ils saisissent les données dans ISIS ».

Le Conseil fédéral est ainsi revenu sur la modification de l'art. 29, al. 2, OSI-SRC qu'il avait effectuée le 9 décembre 2011 dans le cadre de la mise en œuvre de la recommandation 8 de la DélCdG[109] ; il avait alors repris presque mot pour mot, dans le droit d'exécution, la modification que la DélCdG avait demandée :[110]

107 Rapport annuel 2012 des CdG et de la DélCdG des Chambres fédérales du 24.1.2013, ch. 4.3.4 (FF **2013** 3073, ici 3146 ss)

108 Lettre de la DélCdG du 23.1.2013 à l'intention du chef du DDPS, p. 3

109 Rapport annuel 2012 des CdG et de la DélCdG des Chambres fédérales du 24.1.2013, ch. 4.3.8 (FF **2013** 3073, ici 3151)

110 Ce constat est uniquement valable pour la version allemande, car en français, la disposition ne correspondait ni littéralement ni en substance à la recommandation de DélCdG, qui demandait qu' « avant la saisie de toute nouvelle information, il soit obligatoirement procédé à une appréciation qui confirme ou infirme l'importance des personnes [ou institutions] concernées du point de vue de la protection de l'Etat ».

Dans son rapport consacré à ISIS, la DélCdG avait en effet critiqué que des données relatives à une personne figurent encore dans ISIS alors que, par exemple, le décès de cette personne avait été communiqué ou un organe de sûreté cantonal avait explicitement indiqué que cette personne était sortie d'un groupe extrémiste[111].

En fin de compte, la nouvelle formulation de l'art. 29, al. 2, OSI-SRC exige que l'on examine uniquement si une nouvelle information est suffisamment pertinente, avant d'en autoriser l'enregistrement. Or la recommandation 8 demandait que, pour toute nouvelle information, il soit obligatoirement procédé à une appréciation afin de déterminer si, en relation avec les autres enregistrements sur la personne concernée, l'information en question permettait éventuellement d'infirmer l'importance de la personne pour la protection de l'Etat, auquel cas la personne ne devrait pas rester enregistrée dans ISIS.

La nouvelle formulation de l'art. 29, al. 2, OSI-SRC annule la prescription selon laquelle une nouvelle information doit être examinée non seulement pour elle-même, mais également en vue des de ses conséquences pour l'évaluation de la pertinence pour la protection de l'Etat de la personne à laquelle cette information se rapporte. La DélCdG a peu d'indulgence pour ce genre de méprise d'ordre législatif et compte sur un rapide rétablissement de la situation.

4.2.7 Information du Conseil fédéral au sujet du contrôle de suivi

Le 18 décembre 2013, la DélCdG a informé le Conseil fédéral par écrit de l'état de son contrôle de suivi de l'inspection sur le système ISIS.

Dans cette lettre, la DélCdG a constaté que les principales lacunes relevées lors de son inspection avaient été comblées en temps utile. Selon elle, ce résultat positif a pu être obtenu grâce aux efforts du SRC, au soutien du chef du DDPS et au suivi du préposé externe à la protection des données.

La DélCdG a aussi signalé les derniers points en suspens concernant les informations relatives à la protection de l'Etat qui doivent encore être effacées de la banque de données ISIS. Elle a également informé le Conseil fédéral qu'elle n'était pas convaincue de l'opportunité de la nouvelle version du programme de recherches fondé sur le contrôle des photos d'identité, que le Conseil fédéral avait approuvée à la suite de l'inspection relative à ISIS. En outre, la délégation a rappelé au Conseil fédéral que la recommandation 8, à laquelle il avait répondu en 2011 en modifiant l'OSI-SRC, ne pouvait plus être considérée comme mise en œuvre en raison de la récente révision de cette même ordonnance.

Comme la DélCdG l'a écrit au Conseil fédéral, elle n'entend clore son contrôle de suivi que lorsque les dernières recommandations seront mises en œuvre.

111 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS), rapport de la DélCdG des Chambres fédérales du 21.6.2010 (FF **2010** 7030 ss)