

13.004

**Rapport annuel 2012
des Commissions de gestion et de la Délégation
des Commissions de gestion des Chambres fédérales**

du 24 janvier 2013

Madame la Présidente,
Monsieur le Président,
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 2012 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, Madame la Présidente, Monsieur le Président, Mesdames et Messieurs, l'assurance de notre très haute considération.

Le 24 janvier 2013

Au nom des Commissions de gestion des
Chambres fédérales :

Le président de la CdG-N,
Ruedi Lustenberger, conseiller national

Le président de la CdG-E,
Paul Niederberger, député au Conseil des
Etats

chargés de la protection de l'Etat et du renseignement au sens étroit du terme, mais s'étend régulièrement à d'autres domaines qui relèvent de la sécurité intérieure et extérieure et, dans des cas particuliers, des événements ne relevant pas du domaine de la sécurité tel que l'on l'entend traditionnellement, mais qui sont susceptibles de porter un grave préjudice aux intérêts du pays »¹⁴⁴.

Dans le cas de la crise diplomatique avec la Libye par exemple, la délégation avait décidé de faire toute la lumière sur les projets d'exfiltration des otages par une unité spéciale de l'armée suisse, non pas parce que l'objet relevait du renseignement ou de la sécurité intérieure, ce qui n'était pas le cas, mais parce qu'il s'agissait d'informations sensibles appartenant au domaine secret de l'Etat. Le Conseil fédéral n'avait d'ailleurs à cette occasion pas remis en cause la légitimité de la délégation d'exercer sa fonction de haute surveillance également dans ce domaine.

Autrement dit et comme l'affirme désormais l'art. 53 LParl, le domaine de surveillance de la délégation s'étend à toutes les affaires devant rester *secrètes*. C'est précisément ce que demandait l'initiative parlementaire de la CEP DMF il y a plus de 20 ans, en exigeant la création d'une délégation chargée d'exercer la haute surveillance « sur les activités de l'administration soumises à une obligation particulière de secret »¹⁴⁵. Il aura fallu ainsi près de deux décennies pour concrétiser dans la loi les aspirations du Parlement à une haute surveillance systématique des domaines sensibles de l'Etat.

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

4.3.1 Liquidation des cas en suspens dans le contrôle de qualité et réduction supplémentaire du volume des données

Dans son rapport d'inspection du 21 juin 2010¹⁴⁶ sur le système d'information relatif à la protection de l'Etat ISIS¹⁴⁷, 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. En raison des problèmes persistants découlant de la migration, en 2004, des données de l'ancien vers le nouveau système ISIS, l'assurance périodique de la qualité des données ISIS, inscrite dans la loi, a pris de plus en plus de retard. Au printemps 2010, ce retard se montait à environ 114 000 appréciations générales¹⁴⁸. Ce n'est qu'à partir de l'automne 2010, lorsque le SRC est parvenu à augmenter l'effectif de l'Assurance qualité, que les contrôles ont pu être repris en nombre. Simultanément, la radiation d'un grand nombre de personnes enregistrées avait permis de réduire le volume de données qui devaient encore être contrôlées.

¹⁴⁴ Précision du droit à l'information des commissions de surveillance, rapport de la CdG-E du 3.12.2010 (FF **2011** 1227)

¹⁴⁵ Evénements survenus au DMF, rapport de CEP du 17.11.1990 (FF **1990** 1229 ; 1521 ss)

¹⁴⁶ 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** 7003)

¹⁴⁷ Avant 2010, ISIS était l'acronyme construit sur la désignation allemande (*informatisiertes Staatsschutzinformationssystem*) du système d'information relatif à la protection de l'Etat. Depuis, cet acronyme désigne le **système d'information sécurité intérieure** (*Informationssystem Innere Sicherheit*).

¹⁴⁸ Rapport annuel 2011 des CdG et de la DélCdG des Chambres fédérales du 27.1.2012 (FF **2012** 6301 ; 6363 ss)

Jusqu'à fin 2011, le nombre de contrôles périodiques en suspens a pu être réduit à 21 000. A la fin du premier semestre 2012, ils étaient encore à peine 10 000 et le retard a finalement été entièrement comblé à la fin de l'année.

Le nombre de personnes enregistrées dans ISIS a culminé à 212 000 à l'automne 2010¹⁴⁹. Fin 2011, grâce au rattrapage de contrôles et aux suppressions recommandées par la DélCdG, le nombre d'enregistrements dans ISIS avait pu être réduit à quelque 55 000 personnes, dont 12 000 tiers. A la fin du premier semestre 2012, le nombre d'enregistrements dans ISIS n'atteignait plus tout à fait 50 000 personnes, les radiations ayant touché les personnes et les tiers dans une même mesure. Fin 2012, quelque 38 000 personnes et 7000 tiers faisaient encore l'objet d'enregistrements dans ISIS.

Fin 2011, l'Assurance qualité du SRC a également accéléré le contrôle des institutions enregistrées dans ISIS, faisant passer leur nombre à moins de 15 000 au début de 2012 à quelque 13 500 à la fin du premier semestre 2012 (à noter que les institutions tierces n'ont pas été mentionnées à part). A la fin de l'année, le nombre d'institutions enregistrées s'élevait à 11 000 environ.

Dans son arrêt du 18 mars 2009, statuant sur la demande de consultation d'un hebdomadaire suisse, le TAF avait demandé la radiation de tous les enregistrements pour lesquels un média a été enregistré comme objet en tant que tel¹⁵⁰. Le SRC a effacé une première partie de ces quelque 200 enregistrements en 2011. Fin 2012, il n'y avait plus qu'une centaine de médias enregistrés dans ISIS.

L'effort extraordinaire destiné à venir à bout des contrôles en suspens ayant été mené à bien et les radiations concernées ayant été faites, le SRC estime que le nombre des enregistrements dans ISIS devrait à nouveau repartir légèrement à la hausse.

4.3.2 Indicateurs ISIS

La recommandation 13 du rapport ISIS demandait au DDPS de définir des indicateurs permettant au département de procéder à un examen de plausibilité afin de déterminer si l'Assurance qualité fonctionne conformément aux prescriptions légales. Pour répondre à cette demande, le SRC a élargi les rapports trimestriels¹⁵¹ relatifs à l'évolution du volume de données ISIS, que la DélCdG avait demandés en mars 2010, en y incluant des informations supplémentaires. A partir du premier trimestre 2011, les rapports présentaient également des chiffres relatifs aux contrôles de qualité effectués et en suspens.

Selon le préposé à la protection des données ISIS (voir ch. 4.3.3), ces informations ont permis à la direction du SRC de dégager des tendances claires pour la liquidation des cas en suspens dans le contrôle de qualité. La DélCdG a pris connaissance de ces chiffres à la fin de chaque trimestre.

¹⁴⁹ Rapport annuel 2011 des CdG et de la DélCdG des Chambres fédérales du 27.1.2012 (FF 2012 6301 ; 6342 ss)

¹⁵⁰ 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 7003 ; 7051 s.)

¹⁵¹ *Ibid.* (FF 2010 7003 ; 7069)

Les indicateurs permettent de calculer le taux de suppression lors des appréciations générales. Ainsi, en 2012, environ 40 % des personnes examinées ont été radiées parce qu'elles ne revêtaient plus d'importance pour la sûreté de l'Etat. En outre, durant la même période, un tiers des institutions contrôlées a été radié, le taux de suppression trimestriel ayant varié entre 24 et 42 %.

Avant que le SRC s'attelle à la liquidation systématique des cas en suspens dans l'Assurance qualité à l'automne 2010, la part des tiers représentait nettement plus de 40 % de toutes les personnes enregistrées dans ISIS. Ainsi, pour près de la moitié des personnes faisant l'objet d'un enregistrement dans ISIS, le SRC ne disposait pas encore d'indices directs relatifs à leur pertinence pour la sûreté de l'Etat.

En 2011, comparée à l'ensemble des enregistrements ISIS, la part des tiers a diminué au fur et à mesure des radiations d'enregistrements relatifs à des personnes effectuées par l'Assurance qualité. Début 2012, cette part est passée sous la barre des 20 %. Simultanément, la proportion entre les personnes et les tiers nouvellement saisis s'est également améliorée. Elle a atteint environ 15 % en 2012. Cette tendance est plausible puisque l'objectif principal d'ISIS est d'enregistrer les personnes revêtant une importance pour la protection de l'Etat, mais pas celles qui ont des contacts avec elles, certes, mais dont le SRC ne parvient pas à évaluer la pertinence sous l'angle de la protection de l'Etat.

Le système ISIS ne permet pas de générer suffisamment d'indicateurs de manière automatique et une partie d'entre eux doit être calculée manuellement. Lors d'un entretien avec le préposé externe à la protection des données ISIS, ce dernier a recommandé à la délégation de veiller à ce que les fonctions statistiques correspondantes figurent dès le départ dans les spécifications de détail du futur système ISIS (voir ch. 4.3.11).

4.3.3 Travail du préposé à la protection des données ISIS

Tenant compte de la recommandation 1 du rapport ISIS de la DélCdG, le Conseil fédéral a institué un préposé externe à la protection des données chargé de surveiller la liquidation des cas en suspens par l'Assurance qualité. S'en tenant à la recommandation, le Conseil fédéral l'a chargé de lui faire rapport semestriellement.

Pour remplir la mission de préposé à la protection des données ISIS, le DDPS a pu s'attacher les services de l'ancien député au Conseil des Etats Hansruedi Stadler qui est entré en fonction début 2011. Cette année-là, la DélCdG s'est entretenue avec lui à deux reprises et a pris connaissance de son premier rapport semestriel. En mars et en octobre 2012, la délégation s'est entretenue avec lui de ses deuxième et troisième rapports semestriels respectivement.

Conformément à la recommandation de la DélCdG, le SRC était chargé de verrouiller l'accès à toutes les données saisies dans ISIS qui n'avaient pas fait l'objet d'une appréciation générale dans le délai prescrit. Les collaborateurs du SRC n'avaient le droit d'utiliser de telles données que sur autorisation préalable du préposé à la protection des données ISIS. En cas de consultation de la base de

données, ISIS indiquait à l'utilisateur quelles données étaient verrouillées sans toutefois l'empêcher d'y accéder¹⁵².

Le 19 mars 2011, lors de l'entretien avec le préposé à la protection des données ISIS, ce dernier a déclaré que l'Assurance qualité examinait hebdomadairement si les rapports écrits que la division Analyse rédigeait en se fondant sur des données ISIS contenaient des informations visées par le verrouillage. Dans de tels cas, plutôt rares, les informations incriminées étaient soumises après coup à l'approbation du préposé externe à la protection des données ISIS.

A fin 2012, l'Assurance qualité du SRC était parvenue à liquider tous les contrôles en souffrance. Le préposé externe à la protection des données ISIS a ainsi rempli le mandat qui faisait l'objet de la première recommandation de la DéICdG. La délégation estime qu'il a contribué de manière importante au rétablissement de la conformité légale des données saisies dans ISIS. Ses contrôles concomitants ont augmenté la confiance que la DéICdG place dans la qualité de ces données.

Pour la délégation, il est également important d'éviter que des négligences puissent se reproduire à l'échelon de l'assurance de la qualité. La liquidation des cas en suspens, entre octobre 2010 et fin 2012, a nécessité des efforts substantiels qui ont dû être fournis en plus des contrôles réguliers. Sans le personnel supplémentaire autorisé par le DDPS pour une durée limitée, le SRC ne serait pas venu à bout de la tâche.

En vertu des dispositions légales régissant l'assurance de la qualité, les données enregistrées dans ISIS doivent être réexaminées tous les trois ans. Cela signifie que, pour au moins une partie des enregistrements qui ont été contrôlés au cours de ces deux dernières années dans le cadre de la liquidation des cas en suspens, les contrôles périodiques à effectuer tous les trois ans arriveront progressivement à échéance dès fin 2013. La charge de travail supplémentaire sera sans doute moins élevée que lors de la liquidation des cas en suspens, étant donné que ceux-ci ont aussi donné lieu à des radiations (environ 40 % en 2012). Il n'empêche que, dès fin 2013, le SRC devra à nouveau effectuer un nombre de contrôles supérieur à la moyenne. Il faut donc qu'il se demande aujourd'hui déjà comment il parviendra à effectuer ces contrôles dans les délais sans le personnel supplémentaire qui avait été autorisé jusqu'à fin 2012 pour liquider les cas en suspens.

Dans son deuxième rapport, le préposé à la protection des données ISIS avait déjà fait état de cette difficulté. En mars 2012, la DéICdG a appris que le SRC avait fait appel au préposé à la protection des données ISIS dans le cadre de l'évaluation des besoins futurs en personnel de l'Assurance qualité. A la lecture du troisième rapport du préposé, la délégation a constaté que le DDPS avait octroyé à l'Assurance qualité trois postes supplémentaires dès 2013. Le SRC prévoit en outre d'avancer une partie des contrôles pour ne pas risquer un dépassement de délai à cause d'un nombre trop important d'appréciations générales à effectuer.

Il ressort du deuxième rapport du préposé externe à la protection des données que ce dernier s'était également penché sur les exigences légales minimales en vigueur en matière d'assurance de la qualité. Lors des travaux préparatoires relatifs à la révision

¹⁵² Rapport annuel 2011 des CdG et de la DéICdG des Chambres fédérales du 27.1.2012, ch. 4.3.3 (FF 2012 6301 ; 6364 s.)

de l'ordonnance sur les systèmes d'information du SRC (OSI-SRC)¹⁵³ du 9 décembre 2011, le SRC avait proposé d'assouplir les exigences en matière d'assurance qualité en modifiant l'ordonnance¹⁵⁴. En plus de l'accroissement de l'intervalle de temps entre les contrôles, il souhaitait que seuls les enregistrements jugés peu fiables soient encore soumis à un contrôle périodique. De l'avis du SRC, ces sacrifices consentis au détriment de la qualité auraient permis à l'Assurance qualité de juguler durablement les cas en suspens.

Pour sa part, le préposé à la protection des données ISIS a estimé que la proposition du SRC n'était pas compatible avec l'interprétation correcte de l'art. 15, al. 5, LMSI. Par ailleurs, l'OFJ, le PFPDT et la Surveillance SR sont parvenus à une conclusion similaire dans le cadre de la consultation des offices. Par la suite, le DDPS ayant renoncé à assouplir des dispositions relatives à l'assurance de la qualité des données ISIS, la révision de l'OSI-SRC approuvée par le Conseil fédéral n'a plus donné lieu à aucune contestation.

4.3.4 Nouvelle version du programme préventif de recherches photos passeport

Le rapport ISIS contient deux recommandations (2 et 12) au sujet du programme préventif de recherches fondé sur le contrôle des photos d'identité. La recommandation 2 demandait au DDPS 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. Le SRC a procédé à la radiation de ces données en décembre 2010 déjà¹⁵⁵.

La recommandation 12 de la DélCdG demandait au Conseil fédéral d'abandonner le programme de recherches ou, s'il devait décider de le poursuivre, de justifier son choix dans un rapport. Le Conseil fédéral a décidé de continuer le programme. Le DDPS a adressé le rapport demandé à la délégation le 31 mars 2011. Il ressort de ce rapport que le programme de recherches ne sert plus qu'à l'accomplissement d'une partie des tâches relevant de la LMSI et que la gestion des données a été rendue plus restrictive. Les informations relatives aux personnes dont les passeports ont été contrôlés à la frontière sont dorénavant stockées dans une base de données à part (le module informatique P4). La durée de conservation de ces données est limitée à cinq ans (art. 33 OSI-SRC). Selon l'art 31 OSI-SRC le droit d'être renseigné est régi par les art. 8 et 9 de la loi fédérale sur la protection des données (LPD)¹⁵⁶.

Le 25 avril 2012, la DélCdG a assisté, sur place, à une démonstration de la nouvelle base de données que le SRC venait de mettre en route le même mois. Le traitement manuel des documents de voyage photographiés à la frontière s'est avéré plutôt lourd. La délégation a constaté qu'un logiciel permettait toutefois de vérifier automatiquement si le porteur d'un passeport photographié à la frontière avait déjà été saisi dans ISIS.

¹⁵³ Ordonnance du 4.12.2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC ; RS **121.2**)

¹⁵⁴ Voir également compte-rendu de la DélCdG relatif au rapport de gestion du Conseil fédéral lors de la session d'été 2012, BO **2012** E 625

¹⁵⁵ Rapport annuel 2011 des CdG et de la DélCdG des Chambres fédérales du 27.1.2012, ch. 4.3.2 (FF **2012** 6301 ; 6363 s.)

¹⁵⁶ Loi fédérale du 19.6.1992 sur la protection des données (LPD ; RS **235.1**)

Il est ressorti du rapport du 31 mars 2011 que, pour le DDPS, une nouvelle version du programme préventif de recherches fondé sur le contrôle des photos d'identité s'imposait, car il permettait au SRC de se procurer une photo récente des personnes contrôlées. Cela étant, l'année passée, la DélCdG avait déjà constaté que, depuis le 11 octobre 2011, date de l'entrée en vigueur de l'ordonnance sur le système central d'information sur les visas (OVIS)¹⁵⁷ récemment édictée, les autorités suisses concernées avaient accès aux données relatives à toutes les personnes ayant présenté une demande de visa Schengen, photos d'identité incluses¹⁵⁸.

Le SRC a accès à ces données Schengen par le truchement du système d'information central sur la migration (SYMIC). Cet accès au SYMIC repose sur l'art. 9 de l'ordonnance SYMIC¹⁵⁹ qui dispose que le SRC est autorisé à accéder aux données relatives aux personnes pour lesquelles il envisage des mesures d'éloignement.

Lors de sa visite du 25 avril 2012, la DélCdG a également voulu se rendre compte par elle-même de la manière dont le SYMIC permet au SRC d'accéder aux photos des personnes qui ont présenté une demande de visa Schengen. Il est apparu que les collaborateurs disposant d'un accès au SYMIC ignoraient que celui-ci leur permettait d'avoir accès à des données et aux photos d'identité relatives à ces personnes. La DélCdG s'est donc demandé si les droits d'accès inclus dans le système électronique ne correspondaient pas à l'ordonnance SYMIC ou si l'ordonnance elle-même était défailante. Par lettre du 29 mai 2012, la DélCdG a prié le DDPS de clarifier cette question.

Le 11 juin 2012, le directeur du SRC a informé la DélCdG que le SYMIC permettait effectivement d'accéder aux données relatives aux demandes de visas, photos d'identité incluses. Il a précisé que ce système permettait d'accéder aux données relatives à toutes les personnes qui ont présenté une demande de visa Schengen auprès d'un service suisse, mais que le SRC ne disposait toutefois d'aucun accès en ligne aux données relatives aux demandes enregistrées par d'autres Etats dans le système central d'information sur les visas (C-VIS) et que, le cas échéant, il pouvait obtenir les informations relatives à ces visas en présentant une demande d'accès motivée à fedpol (art. 17 OVIS).

Dans le courant du mois d'octobre 2012, la DélCdG s'est entretenue avec le directeur du SRC du rapport sur les programmes de recherches préventifs à remettre au moins une fois par année au chef du DDPS (art. 24, al. 5, OSRC). Durant la période couverte par le dernier rapport en date (second semestre 2011 et premier semestre 2012), seuls 0,5 % des voyageurs qui ont fait l'objet d'un enregistrement dans le programme préventif de recherches fondé sur le contrôle des photos d'identité ont également été enregistrés dans ISIS. Depuis 2007 où elle atteignait encore 2 %, cette proportion n'a cessé de diminuer. De l'avis du directeur du SRC, cette tendance est probablement due à la décroissance du nombre de personnes enregistrées dans ISIS amorcée en 2011. Etant donné toutefois que la part des correspondances dans ISIS a commencé à baisser à partir de 2008, lorsque le traitement des données du programme préventif de recherches fondé sur le contrôle

¹⁵⁷ Ordonnance du 6.6.2011 sur le système central d'information sur les visas (OVIS ; RS **142.512**)

¹⁵⁸ Rapport annuel 2011 des CdG et de la DélCdG des Chambres fédérales du 27.1.2012, ch. 4.3.4 (FF **2012** 6301 ; 6364)

¹⁵⁹ Ordonnance du 12.4.2006 sur le système d'information central sur la migration (Ordonnance SYMIC ; RS **142.513**)

des photos d'identité a été accéléré en faisant appel à du personnel supplémentaire et que la masse des données stockées dans ISIS augmentait encore, force est de penser que cette explication est insuffisante.

En fin de compte, le SRC et les cantons fournissent un effort considérable pour enregistrer plus de 100 000 passages de frontière par an alors que plus de 99 % des informations ainsi traitées ne sont vraisemblablement pas pertinentes sous l'angle de la sécurité de la Suisse. De plus, dans de nombreux cas le SRC n'aurait pas besoin du programme préventif de recherches fondé sur le contrôle des photos d'identité pour pouvoir accéder aux informations sur les passeports de personnes qui veulent entrer en Suisse, puisqu'il dispose d'un droit d'accès au système d'information sur les visas Schengen et que pratiquement tous les ressortissants des pays concernés par ce programme préventif sont soumis à l'obligation du visa¹⁶⁰.

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, mais la question de l'opportunité et de l'efficacité reste d'actualité. La DélCdG va selon toute vraisemblance conclure cette partie de son contrôle de suivi du rapport ISIS au printemps 2013 par une appréciation dans ce sens.

4.3.5 Association à l'assurance de la qualité des utilisateurs chargés de l'analyse et des cantons

Dans le rapport ISIS, la DélCdG avait constaté que la saisie des données et les contrôles de qualité dans ISIS étaient effectués par des collaborateurs qui ne participaient pas à l'analyse ultérieure de ces données à des fins relevant de la sûreté de l'Etat. Au sein de l'ancien SRS, les analystes participaient directement au processus de saisie des données, ce que la délégation avait jugé pertinent¹⁶¹. Partant, elle s'était dite convaincue que le fait d'associer les spécialistes de l'analyse à la saisie des données déboucherait sur une amélioration considérable de la qualité des données ISIS.

La DélCdG avait également estimé qu'il était nécessaire que les organes de sûreté des cantons améliorent la qualité des communications qu'ils envoient au SRC, cela afin d'éviter à la source que des communications ne présentant aucune importance pour la sûreté de l'Etat ne lui soient transmises. Eu égard à ces deux constatations, la délégation avait exigé du SRC qu'il lui soumette deux rapports, l'un exposant la manière dont les compétences d'analyse du personnel peuvent être mises au service de l'appréciation, l'autre la manière dont les cantons peuvent contribuer à l'amélioration de la qualité des données ISIS (voir recommandations 4 et 5 du rapport ISIS).

Le 24 février 2012, la DélCdG a entendu plusieurs représentants du SRC au sujet des deux rapports susmentionnés, rédigés par le SRC.

Le rapport sur la manière dont les compétences des collaborateurs chargés de l'analyse peuvent être mises au service de la saisie et du traitement des informations

¹⁶⁰ Rapport annuel 2011 des CdG et de la DélCdG des Chambres fédérales du 27.1.2012, ch. 4.3.4 (FF 2012 6301 ; 6366 s.)

¹⁶¹ 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 7003 ; 7067 s.)

dans ISIS comporte deux pages. Ce rapport prévoit principalement de permettre aux collaborateurs chargés de la saisie des données et du contrôle préalable de leur pertinence sous l'angle de la sûreté de l'Etat de participer aux séances internes du SRC, au cours desquelles les analystes amènent leurs connaissances spécialisées. En outre, ces collaborateurs doivent pouvoir, d'une part, remettre une évaluation de la pertinence des données lorsque cela s'avère nécessaire pour la saisie des données ou les contrôles périodiques et, d'autre part, vérifier semestriellement, par sondage, l'utilité concrète des données confirmées lors de l'appréciation globale.

Ce rapport de deux pages annonce également l'examen de la pertinence de certaines données de moindre importance sous l'angle de l'analyse (comme l'indication du lieu d'origine). Il est ressorti de la discussion avec les représentants du SRC que ce genre d'examen est entrepris uniquement dans des cas particuliers et à l'initiative de la Section Analyse préliminaire. Il n'y a pas d'examen systématique des champs de données prévus dans ISIS. Il est également apparu que la désignation « analyse préliminaire » n'est pas adéquate pour le processus de saisie des données dans ISIS et que le terme « intégration » serait plus adapté pour décrire la saisie de données dans le système. Le SRC a examiné l'opportunité de renommer la section qui s'appelle « Saisie des données / Triage » depuis avril 2012.

Il ressort du rapport rédigé en réponse à la recommandation 5, que l'attribution des mandats aux organes de sûreté des cantons a été harmonisée et systématisée, ce qui a permis de simplifier la gestion des dossiers par le SRC et les cantons. L'autorité cantonale de surveillance dispose également de la liste des mandats qui ont été confiés à l'organe de sûreté du canton. Ainsi, à l'aide de cette liste, elle peut notamment consulter les données que la sûreté cantonale traite sur ordre du SRC (voir art. 35a OSRC).

4.3.6 Examen de l'allocation des ressources pour le traitement des données dans ISIS

La recommandation 3 du rapport ISIS demandait au SRC d'allouer les ressources en personnel aux diverses tâches relevant du traitement des données dans ISIS de sorte que seules soient saisies dans le système les informations dont la pertinence sous l'angle de la sûreté de l'Etat a effectivement été examinée et qui peuvent faire l'objet d'une appréciation régulière conformément aux prescriptions légales. Le DDPS était en outre invité à redéfinir l'engagement des ressources en personnel au sein du SRC dans le cadre d'un projet formel.

Au printemps 2012, le DDPS a accordé au SRC trois postes supplémentaires pour l'Assurance qualité à partir de 2013 (voir ch. 4.3.3) afin de relayer le personnel supplémentaire alloué jusqu'à fin 2012 pour liquider les cas de contrôle de la qualité en suspens. Le SRC a également modifié l'organigramme et les compétences des domaines chargés du traitement des données ISIS. Depuis le printemps 2012, les collaborateurs qui effectuent la saisie des données dans ISIS et ceux qui sont chargés d'en contrôler la qualité ne sont plus subordonnés au même supérieur direct commun. Une spécialisation des collaborateurs a également été introduite dans le domaine de la saisie des données : le triage des données et leur saisie dans ISIS ont été confiés à des collaborateurs distincts.

Le SRC a limité l'examen de l'allocation des ressources en personnel à sa division Gestion de l'information. Il n'a toutefois pas procédé à une analyse élargie des besoins, en y intégrant notamment la division Analyse qui, en fin de compte, utilise les données ISIS pour ses analyses de situation.

En revanche, à l'été 2010 déjà, le SRC avait chargé une société de consultants indépendante d'analyser les processus de travail de la division Gestion de l'information. Cette analyse a été achevée en février 2011 avec la remise d'un rapport d'une soixantaine de pages.

L'étude présentait au SRC un calcul de l'effectif nécessaire pour venir à bout, avant fin 2012, des cas en suspens dans le contrôle de qualité. A partir d'une analyse des liens fondamentaux au sein des processus de travail relatifs aux données ISIS, les consultants ont également mis différentes possibilités d'amélioration en évidence, sans toutefois vraiment remettre en question le modèle de gestion appliqué à l'exploitation d'ISIS que le SRC avait repris de l'ancien service de renseignement intérieur.

En revanche, à la demande du SRC, la société de consultants indépendante a soumis le rapport d'inspection ISIS de la DélCdG à une évaluation critique et formulé des recommandations contredisant l'avis du Conseil fédéral sur ledit rapport.

En ce qui concerne le traitement des données au sein du SRC, cette étude n'a en fin de compte déployé des effets tangibles que sur la subordination de l'Assurance qualité et la répartition des tâches entre les collaborateurs chargés de la saisie des données qui, comme indiqué précédemment, ont toutes deux été modifiées au printemps 2012.

4.3.7 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 relevant de la protection de l'Etat (ISIS01). La délégation voulait ainsi éviter qu'à l'avenir, des personnes dont le SRC, à l'instar d'autres services de la Confédération, doit s'occuper pour des raisons administratives fassent l'objet d'un enregistrement dans ISIS01. La DélCdG avait constaté ce problème lorsqu'elle avait elle-même consulté ISIS par sondage¹⁶².

Dans le rapport ISIS, la DélCdG avait expressément souligné que les données relatives à ces personnes devaient être enregistrées dans « ISIS02 Administration » et que seule la base de données ISIS01 pouvait contenir des informations relevant de la protection de l'Etat¹⁶³.

Conformément à la recommandation 6, le SRC enregistre dorénavant les données relevant de l'activité administrative uniquement dans ISIS02. Toutefois, la directive n'aura été entièrement mise en œuvre qu'une fois que toutes les données de nature purement administrative auront été transférées dans ISIS02. Actuellement, le SRC

¹⁶² 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** 7003 ; 7017 s.)

¹⁶³ *Ibid.* (FF **2010** 7003 ; 7051 s.)

est en train d'introduire un système de gestion des affaires qui succédera à ISIS02 et reprendra toutes les données correspondantes.

Depuis le 1^{er} juin 2011, le traitement des données dans ISIS02 est régi par une directive du directeur du SRC. En substance, cette directive prévoit notamment que, lors de leur radiation de la base de données relative à la protection de l'Etat, les rapports qui permettent de lever une suspicion documentée dans cette dernière doivent être saisis dans la base des données administratives, accompagnés du rapport sur lequel les soupçons se fondaient¹⁶⁴. Ce cas de figure se présente lorsque le contrôle de qualité conclut que la personne concernée est mise hors de cause par un rapport.

Lorsqu'une information n'est plus pertinente du point de vue de la protection de l'Etat, elle doit être supprimée, conformément à l'art. 15, al. 1, LMSI. La question se pose toutefois de savoir s'il est permis de copier préalablement dans ISIS02 des informations qui doivent être effacées d'ISIS01. La DélCdG continuera de s'intéresser à cette problématique en 2013.

4.3.8 Pas de saisie de données sans contrôle de pertinence

La recommandation 8 demandait au Conseil fédéral de préciser le droit d'exécution de sorte que, avant la saisie de toute nouvelle information, il soit obligatoirement procédé à une appréciation qui confirme ou infirme l'importance des personnes concernées du point de vue de la protection de l'Etat. Le Conseil fédéral a suivi cette recommandation et, le 9 décembre 2011, a complété l'OSI-SRC en reprenant son contenu pour ainsi dire littéralement (art. 29, al. 2, OSI-SRC).

L'accumulation dans ISIS d'un grand nombre d'informations non pertinentes découlait notamment des directives inappropriées régissant la saisie des données. Ainsi, un tiers devenait automatiquement pertinent pour la protection de l'Etat dès lors qu'il apparaissait dans plus de deux communications dans ISIS¹⁶⁵. Les directives relatives à l'enregistrement échelonné des activistes enclins à la violence¹⁶⁶ généraient elles aussi un automatisme semblable¹⁶⁷.

La DélCdG a estimé que ces mécanismes ne constituaient en fin de compte qu'une méthode inappropriée de déterminer l'importance d'une information tout en faisant l'économie de leur examen par les collaborateurs du renseignement lors de la saisie de cette information. Dans sa recommandation 9, la délégation avait par conséquent demandé que toutes les règles de cette nature soient abrogées et que toutes les directives régissant la saisie dans ISIS soient revues.

Suite aux résultats des inspections effectuées par la Surveillance des services de renseignement (Surveillance SR)¹⁶⁸, les règles inappropriées s'appliquant à la saisie

¹⁶⁴ Directive du directeur du SRC du 1.6.2011 (n'existe qu'en allemand), p. 2

¹⁶⁵ 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** 7003 ; 7023 s.)

¹⁶⁶ Richtlinien zur Abgestuften Erfassung von gewaltorientierten Aktivisten (ces directives n'ont pas été traduites en français).

¹⁶⁷ 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** 7003 ; 7032 s.)

¹⁶⁸ *Ibid.*, ch. 2.10 (FF **2010** 7003 ; 7036 ss)

ont été abrogées au printemps 2010 déjà. Durant la période jusqu'à l'été 2011, le SRC a rédigé plusieurs nouvelles directives relatives à la saisie des données dans ISIS ainsi qu'une liste de cas illustratifs. Les instructions pour la saisie ISIS, qui comprennent encore 225 pages, ont été révisées partiellement en avril 2012. La Surveillance SR, qui assure le contrôle sur place du respect des nouvelles prescriptions, estime que les nouvelles règles de saisie nécessitent des connaissances spécifiques importantes et doivent encore être consolidées dans la pratique.

4.3.9 Droit d'accès

Dans sa recommandation 11, la DélCdG avait proposé au Conseil fédéral de remplacer le droit d'accès indirect prévu à l'art. 18 LMSI alors en vigueur par un droit d'accès différé selon les modalités de l'art. 8 de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP)¹⁶⁹. Dans son message complémentaire « LMSI II réduite »¹⁷⁰ du 27 octobre 2010, le Conseil fédéral avait proposé une solution encore plus favorable pour le requérant, à savoir un droit d'accès en vertu des art. 8 et 9 LPD.

Le Conseil des Etats s'était rallié à la proposition du Conseil fédéral lors de la session d'été 2011. En revanche, lors de la session d'automne, le Conseil national a décidé de s'en tenir au statu quo. Durant la session d'hiver, suivant l'avis de sa Commission des affaires juridiques, le Conseil national s'est rangé à la proposition de compromis du Conseil des Etats et a accepté que le droit d'accès aux données enregistrées dans ISIS soit régi en application de l'art. 8 LSIP. La DélCdG a dès lors considéré sa recommandation 11 comme pleinement réalisée.

Dans son rapport ISIS, la DélCdG a mentionné un arrêt non publié du TAF, du 18 mars 2009, qui exigeait que la base de données « ISIS02 Administration » soit soumise au droit d'accès direct selon les modalités des art. 8 et 9 LPD¹⁷¹. Etant donné que les exigences formulées dans cet arrêt n'avaient pas encore été mises en œuvre, la délégation avait recommandé au Conseil fédéral (recommandation 10) de soumettre tous les fichiers d'ISIS, à l'exception des données « ISIS01 Protection de l'Etat », à un droit d'accès direct.

Le Conseil fédéral s'était déclaré prêt à examiner la recommandation 10¹⁷², en précisant toutefois son intention d'attendre la rédaction des dispositions relatives aux futurs systèmes d'information du SRC dans le cadre de l'élaboration de la future loi sur le service de renseignement.

En avril 2012, la Surveillance SR a informé la DélCdG que, en application de l'arrêt du TAF du 18 mars 2009, le SRC avait commencé à octroyer un droit d'accès direct

¹⁶⁹ Loi fédérale du 13.6.2008 sur les systèmes d'information de police de la Confédération (RS 361)

¹⁷⁰ Message complémentaire au message du 15 juin 2007 relatif à la modification de la loi fédérale institution des mesures visant au maintien de la sûreté intérieure (« LMSI II réduite ») du 27.10.2010 (FF 2010 7147)

¹⁷¹ 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 7003 ; 7051)

¹⁷² Traitement des données dans le système d'information relatif à la protection de l'état ISIS, rapport de la DélCdG des Chambres fédérales du 21.6.2010, avis du Conseil fédéral du 20.10.2010 (FF 2010 7079 ; 7095)

aux données enregistrées dans ISIS02, ce qui lui a été confirmé le 26 juin 2012, lors d'un entretien avec le PFPDT.

Les nouvelles dispositions de l'art. 18 LMSI sont entrées en vigueur le 16 juillet 2012 et accordent désormais un droit d'accès direct aux données enregistrées dans ISIS02. En effet, contrairement à ce qui est le cas des données enregistrées dans ISIS01, par exemple, les intérêts liés au maintien du secret ne peuvent pas être invoqués en ce qui concerne les données de nature administratives pour lesquelles le SRC est dorénavant tenu de renseigner la personne qui a fait valoir son droit d'accès aux données la concernant, et cela, en appliquant les normes générales du droit fédéral sur la protection des données. Cette obligation de renseigner ne peut pas non plus être différée lorsque ISIS02 ne contient aucune donnée relative à la personne qui fait usage de son droit d'accès. La révision LMSI II a donc déjà permis de réaliser l'objectif principal de la recommandation 10.

4.3.10 Renforcement de l'effectif de la Surveillance SR

Le 3 octobre 2008, les Chambres fédérales ont adopté la loi fédérale sur le renseignement civil (LFRC) élaborée par la DélCdG en réponse à l'initiative parlementaire Hofmann (Iv. pa. 07.404). Le 10 octobre 2008, la délégation a, par écrit, rendu le Conseil fédéral attentif au fait qu'en vertu de l'art. 8 LFRC, l'activité du renseignement extérieur devait dorénavant aussi être soumise à un contrôle administratif, à l'instar de celle du renseignement intérieur. En effet, en 2008, le Conseil fédéral avait encore refusé de soumettre le renseignement extérieur à un tel contrôle alors même que la DélCdG avait recommandé cette mesure dans son second rapport Onyx du 9 novembre 2007¹⁷³.

Dans sa lettre du 10 octobre 2008, la DélCdG a prié le Conseil fédéral de préciser, encore avant la fin de l'année, quelles ressources en personnel il entendait engager pour remplir cette mission de contrôle après le transfert, début 2009, du renseignement intérieur au DDPS. Le 12 décembre 2008, le Conseil fédéral a répondu à la DélCdG que deux collaborateurs de l'Inspectorat du DFJP seraient transférés au secrétariat général du DDPS début 2009 d'où ils continueraient d'exercer le contrôle sur le renseignement intérieur et qu'il avait en outre l'intention de débloquer deux postes supplémentaires pour étendre le contrôle administratif au renseignement extérieur dès que la LFRC serait en vigueur.

Le Conseil fédéral a mis la LFRC en vigueur avec effet au 1^{er} janvier 2010. En mars 2010, lors d'un entretien avec la Surveillance SRC, la DélCdG a constaté qu'ils n'étaient que trois et que la décision relative au quatrième poste de travail n'avait pas encore été prise. L'inspection sur ISIS ayant une nouvelle fois confirmé la nécessité de disposer d'un contrôle administratif opérationnel, la recommandation 15 avait pour objectif d'inciter le DDPS à renforcer l'effectif de la Surveillance SR, conformément aux assurances données par le Conseil fédéral. La DélCdG a considéré que l'objectif de la recommandation 15 avait été atteint dès lors que la Surveillance SR a été en mesure de pourvoir son quatrième poste en avril 2011.

¹⁷³ Légalité et efficacité du système d'exploration radio « Onyx », rapport du 9.11.2007 de la DélCdG des Chambres fédérales, avis du Conseil fédéral du 14.3.2008 (FF 2008 2319 ; 2323)

Au mois de janvier 2012, deux collaborateurs de la Surveillance SR ont déposé auprès de la DélCdG une requête en matière de surveillance. La délégation ne lui a toutefois pas donné suite puisque, statuant dans le cadre d'une procédure judiciaire, le TAF avait déjà tranché l'affaire en défaveur des deux auteurs de la requête.

En février 2012, le DDPS a informé la DélCdG qu'il avait suspendu les deux collaborateurs de la Surveillance SR. En avril 2012, lors de l'entretien annuel avec le chef de la Surveillance SR, la délégation a été informée que le chef du DDPS avait déjà mis un collaborateur supplémentaire à sa disposition pour une durée limitée. La Surveillance SR a pu pourvoir le dernier poste devenu vacant au cours du mois suivant.

4.3.11 Points en suspens à régler dans le système appelé à succéder à ISIS-NT

ISIS contient un champ de données qui consigne la date de la plus récente appréciation générale des informations relatives à chaque personne faisant l'objet d'un enregistrement. Lors de l'enquête qu'elle a menée sur ISIS, la DélCdG avait toutefois constaté que des dates avaient été enregistrées pour des appréciations qui ne pouvaient avoir été effectuées. Il est apparu que, pour éviter que l'Assurance qualité prenne encore plus de retard dans son travail, des dates fictives avaient été enregistrées pour des contrôles qui n'avaient pas été effectués et prolongeaient illégalement le délai jusqu'à la prochaine appréciation générale.

Pour exclure que de telles manipulations puissent se reproduire, la DélCdG avait recommandé au DDPS de configurer ISIS de sorte que la date de toutes les appréciations générales périodiques faites concernant une personne enregistrée puisse être présentée correctement dans le système (recommandation 14). Le Conseil fédéral s'était déclaré d'accord de tenir compte de cette recommandation dans le cadre du développement du système appelé à remplacer ISIS.

Le Conseil fédéral s'était également engagé à mettre la recommandation 16 du rapport ISIS en œuvre et à veiller à ce que seules des données qui remplissent toutes les exigences légales en matière de qualité soient transférées dans le futur système ISIS. Le SRC avait décidé de lancer le développement d'un tel système d'information en février 2010. Initialement, le SRC prévoyait non seulement d'achever ce développement, mais également de transférer toutes les données ISIS avant fin 2012. Depuis lors, cette planification s'est avérée irréaliste.

Depuis la liquidation des cas en suspens par l'Assurance qualité, il est possible d'admettre que les données enregistrées dans ISIS sont conformes aux exigences légales. Eu égard au retard pris par le SRC dans le développement du système appelé à remplacer ISIS, la recommandation 16 est devenue sans objet. Quant au contrôle de la mise en œuvre de la recommandation 14, la DélCdG se penchera sur les spécifications détaillées du futur système en 2013.

Dans la recommandation 17, la DélCdG avait exigé du DDPS qu'il lui soumette un rapport sur les solutions techniques actuelles et futures en matière d'exploitation de bases de données orientées personne. Ce rapport devait mettre en évidence le cadre juridique que la LMSI impose à ce système. La délégation avait exigé que sa rédaction soit confiée à des experts indépendants de l'administration et fondé sur l'état actuel des connaissances scientifiques.

Le 18 août 2011, le SRC a confié l'étude à la même société de consultants indépendante qui, en février 2011, avait déjà livré le rapport sur les processus de travail de la division Gestion de l'information (voir ch. 4.3.6). Après l'échéance du délai de remise du rapport contractuellement fixé à fin 2011, la DélCdG a prié le SRC de lui remettre une copie de l'étude. En février 2012, le directeur du SRC a répondu que le projet de rapport en sa possession se limitait beaucoup trop aux possibilités des systèmes d'informations actuels du SRC, raison pour laquelle il avait chargé la société de consultants de reprendre l'étude de manière à tenir également compte de l'évolution technique la plus récente.

Cette issue n'avait rien d'étonnant dans la mesure où le mandat que le SRC avait confié à la société de consultants portait principalement sur l'analyse des « systèmes actuels » et était resté très vague en ce qui concerne les technologies les plus récentes. En juin 2012, lorsque la délégation a pris connaissance du compte-rendu de l'étude, elle n'a pas vu en quoi ce rapport d'une trentaine de pages pouvait être utile pour le SRC. De plus, le rapport en question ne contient aucune analyse juridique fondée de l'interprétation à donner à la notion d'« enregistrement avec référence nominale » et n'aborde pas les conséquences de cette interprétation sur l'aspect technique de l'enregistrement et de la consultation des données relatives aux personnes. Par conséquent, le SRC a manqué une occasion de tirer des enseignements qui auraient pu lui être utiles pour l'élaboration de la future loi sur le service de renseignement.

4.4 Essai pilote du système d'information relatif à la sécurité extérieure ISAS

Lors de l'élaboration de la LFRC en réponse à l'initiative parlementaire Hofmann (Iv. pa. 07.404), la DélCdG avait repris telles quelles les dispositions de l'art. 99 LAAM dans l'art. 5 LFRC. En adoptant cet article, le Parlement avait assuré la continuité des bases légales régissant le traitement des informations sur l'étranger après la réorganisation du renseignement civil.

Avant la création du SRC, le service de renseignement extérieur exploitait déjà deux bases de données dans les domaines du terrorisme et de la prolifération. Dès 2007, en tenant compte des retours d'expérience, il a entrepris de développer un nouveau système pour les remplacer et dont il a achevé la première version apte à fonctionner durant le second semestre de 2009¹⁷⁴. Le SRC a commencé l'exploitation de ce système en juin 2010 sous la dénomination d'ISAS (Système d'information relatif à la sécurité extérieure) après y avoir transféré les données relatives à la prolifération et au terrorisme contenues dans les bases de données exploitées auparavant.

ISAS est un instrument de travail indispensable qui permet au SRC de remplir ses tâches au quotidien. En 2012, le nombre de personnes traitées dans ISAS a été comparable au nombre de personnes et de tiers traités dans ISIS. Dans ISAS le SRC y enregistre également des informations collectées en vertu de la LMSI. Or, selon l'interprétation de l'OFJ et de la DélCdG, il découle de l'art. 6 LFRC que les

¹⁷⁴ Projekte ISDACO und IASA NDB, rapport d'audit du CDF à l'attention de la DélFin et de la DélCdG du 10.8.2012, p. 10