Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS)

Rapport de la Délégation des commissions de gestion des Chambres fédérales

du 21 juin 2010

«Il manquait ainsi à l'activité d'acquisition d'informations tout caractère d'un instrument effectif de protection de l'Etat; elle devint ainsi une fin en soi, une inutile réserve d'informations, qui ne fut jamais exploitée dans un but quelconque.»

René Bacher

Rapport final du Préposé spécial au traitement des documents établis pour assurer la sécurité de l'Etat, du 2 mai 1996, p. 32.

Condensé

Une conclusion importante à laquelle la CEP-DFJP avait abouti en 1989 était que la protection de l'Etat devrait à l'avenir être mieux conduite au niveau politique et qu'il fallait empêcher la collecte d'informations erronées ou inutiles. Lorsque les fichiers contenant les fiches ont été relayées par le système d'information relatif à la protection de l'Etat (ISIS) en 1994, le Conseil fédéral a prévu par voie d'ordonnance un contrôle interne de la protection des données. La loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), adoptée en 1997, prescrivait explicitement que seules les informations exactes et utiles pour le travail des services de protection de l'Etat pouvaient être traitées. Une disposition supplémentaire, qui a été intégrée à la LMSI à l'initiative du Parlement, exigeait une appréciation périodique des données enregistrées. Il était prévu que ces règles restrictives garantiraient à l'avenir que seules seraient traitées les données pouvant effectivement fournir des renseignements sur les dangers menaçant la sûreté intérieure et extérieure.

Au début de 2005, le Service d'analyse et de prévention (SAP) a transféré les données ISIS dans le nouveau système ISIS-NT. La présente enquête de la Délégation des Commissions de gestion (DélCdG) établit que le SAP accusait déjà de sérieux retards dans le contrôle qualité avant le passage à ISIS-NT et que, à partir de là, il n'a plus effectué les appréciations périodiques jusqu'à la fin de 2008. De l'avis de la DélCdG, le SAP, qui a été intégré au nouveau Service de renseignement de la Confédération (SRC) au début de 2010, n'a en aucune manière satisfait aux exigences légales en matière d'assurance qualité.

En sa qualité d'organe de la haute surveillance parlementaire, la DélCdG doit pouvoir s'appuyer sur les contrôles de l'exécutif, chose impossible vu que le SAP n'a jamais fait les contrôles prescrits pour la majeure partie des 200 000 personnes et tiers enregistrés dans ISIS-NT. Les pièces que la DélCdG a examinées par sondage soulèvent des doutes quant à l'exactitude et la pertinence des données d'ISIS-NT. Un trop grand nombre des informations analysées par la délégation n'étaient en rien assez pertinentes pour être saisies dans le système, ou y ont été conservées trop longtemps. De plus, les directives du SAP régissant la saisie induisaient systématiquement le classement d'informations erronées, et la majorité des enregistrements des quelque 80 000 tiers figurant dans ISIS-NT ne remplissait pas les critères légaux.

L'état des données d'ISIS remet aussi fondamentalement en cause l'efficacité de la protection de l'Etat. La collecte, le traitement et la conservation de données erronées et inutiles entravent un travail efficace au service de la sûreté intérieure. Cette situation peut déboucher sur des actions inappropriées et des pannes, lesquelles mettent en fin de compte la sûreté de l'Etat en danger.

La DélCdG estime que le non-respect des prescriptions légales concernant l'assurance qualité tient à une mauvaise définition des priorités dans le projet ISIS-NT. Au lieu d'être éliminées avant la migration, des données qui avaient perdu leur pertinence ont été transférées dans le nouveau système et adaptées à la structure d'ISIS-

NT au prix d'un travail énorme. Comme le SAP et le DFJP n'avaient pas jugé utile d'adapter l'effectif du personnel pour la mise au net des anciennes données et la saisie des nouvelles communications, de sérieuses carences se sont faits jour après la mise en service d'ISIS-NT. Afin de pouvoir malgré tout saisir dans le système toutes les informations entrantes, le SAP a détourné le personnel de l'assurance qualité des appréciations générales périodiques pendant presque quatre ans pour l'affecter à la saisie des données.

Par la suite, le nombre des informations saisies a augmenté sans discontinuer et l'effacement des données ne présentant plus de pertinence, pourtant prescrit par la loi, a été oublié. Comme le travail requis par la gestion des données est directement proportionnel à la quantité d'informations, les priorités définies par le SAP ont en fin de compte rendu impossible un traitement des données conforme à la loi. Ce problème ne saurait être résolu par le seul renforcement des ressources de l'assurance qualité. Il faut que le critère de la qualité des données supplante celui de la quantité dans la recherche et la saisie d'informations.

La DélCdG constate en outre que le SAP a considéré dès le début le contrôle de la qualité comme une procédure administrative distincte de l'activité de protection de l'Etat proprement dite. Le personnel qui saisissait les données n'était finalement pas responsable de leur légalité. Des règles mécaniques ont permis aux collaborateurs concernés de saisir des données sans avoir à se préoccuper de l'importance des informations traitées. Au demeurant, les collaborateurs qui procédaient à l'appréciation des données ISIS dans l'optique du renseignement ne répondaient pas non plus de l'exactitude et de la pertinence des données saisies dans le système.

L'exécution des charges qui devaient distinguer la protection de l'Etat «réformée» après l'«affaire des fiches» a donc été déléguée à moins d'une demi-douzaine de collaborateurs de la Section Assurance qualité, qui n'avait toutefois pas la compétence d'interdire l'accès aux données dont la qualité ne pouvait pas être examinée conformément aux prescriptions légales. Il aurait donc appartenu au chef du SAP d'éviter que les données non conformes à la loi soient utilisables, de même que de pourvoir à ce qu'il soit remédié aux problèmes fondamentaux touchant à la qualité des données, dont il est établi qu'il avait connaissance.

Les constatations de la DélCdG se fondent en bonne partie sur les inspections que le DDPS a faites en 2009 dans le cadre du contrôle administratif prévu par la LMSI. La DélCdG juge exemplaire la collaboration entre la haute surveillance parlementaire et le département compétent.

L'enquête de la DélCdG a par ailleurs bénéficié des efforts déployés par la Commission de gestion du canton de Bâle-Ville pour examiner le traitement de données ISIS concernant des membres de son Grand Conseil. La requête de la CdG-BS a donné lieu à une réflexion approfondie sur les limites imposées par l'art. 3 LMSI au traitement des données en relation avec l'exercice des droits politiques, et a finalement ouvert la voie à un accord entre la Confédération et les cantons concernant la forme à donner à la surveillance exercée sur les organes cantonaux de protection de l'Etat.

Table des matières

Liste des abréviations

AFS	Archives fédérales
BO	Bulletin officiel
CAJ-N	Commission des affaires juridiques du Conseil national
CdG	Commission de gestion
CdG-BS	Commission de gestion du Grand Conseil du Canton de Bâle-Ville
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4.11.1950 (Convention européenne des droits de l'homme, RS *0.101*)
CFPD	Commission fédérale de la protection des données
CFPDT	Commission fédérale de la protection des données et de la transparence
Cst.	Constitution fédérale de la Confédération suisse du 18.4.1999 (RS *101*)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DélCdG	Délégation des commissions de gestion
DFJP	Département fédéral de justice et police
fedpol	Office fédéral de la police
FF	Feuille fédérale
ISIS	Système de traitement des données relatives à la protection de l'Etat
ISIS-NT	Système de traitement des données relatives à la protection de l'Etat – Nouvelle Technologie
LFRC	Loi fédérale du 3.10.2008 sur le renseignement civil (RS *121*)
LMSI	Loi fédérale du 21.3.1997 instituant des mesures visant au maintien de la sûreté intérieure (RS *120*)
LParl	Loi du 13.12.2002 sur l'Assemblée fédérale (RS *171.10*)
LPD	Loi fédérale du 19.6.1992 sur la protection des données (RS *235.1*)
LREC	Loi du 23.3.1962 sur les rapports entre les conseils (RO *1962* 811)
LTF	Loi du 17.6.2005 sur le Tribunal fédéral (RS *173.110*)
LSIP	Loi fédérale du 13.6.2008 sur les systèmes d'information de police de la Confédération (RS *361*)
ODM	Office fédéral des migrations
OFJ	Office fédéral de la justice
OMSI	Ordonnance du 27.6.2001 sur les mesures visant au maintien de la sûreté intérieure (RO *2001* 1829)
Ordonnance ISIS	Ordonnance sur le système de traitement des données relatives à la protection de l'Etat (RO *2001* 3173)
OSI-SRC	Ordonnance du 4.12.2009 sur les systèmes d'information du Service de renseignement de la Confédération (RS *121.2*)
OSRC	Ordonnance du 4.12.2009 sur le Service de renseignement de la Confédération (RS *121.1*)

PFPD	Préposé fédéral à la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
PKK	Partiya Karkerên Kurdistan (Parti des travailleurs du Kurdistan)
SAP	Service d'analyse et de prévention
SR	Service de renseignement
SRC	Service de renseignement de la Confédération
SRS	Service de renseignement stratégique
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
UE	Union européenne
WEF	World Economic Forum

Rapport

1 Introduction

La Délégation des Commissions de gestion (DélCdG) exerce la haute surveillance parlementaire sur les activités relevant de la sécurité de l'Etat et du renseignement. L'institution d'une délégation remonte à une commission d'enquête parlementaire chargée de clarifier des événements survenus au Département fédéral de justice et police (CEP DFJP).[1] La CEP DFJP avait déposé une initiative parlementaire (Iv. pa.) réclamant l'institution d'une Délégation des Commissions de gestion chargée de la haute surveillance dans le domaine des activités secrètes.[2] Le Parlement avait donné suite à l'initiative par le biais d'une révision de la loi sur les rapports entre les conseils (LREC)[3], qui est entrée en vigueur le 1er février 1992. Depuis lors, la DélCdG surveille les activités des services de renseignement intérieur et extérieur.

Le traitement des données est au cœur de l'activité de tout service de renseignement et fait par conséquent l'objet d'une attention particulière dans la haute surveillance de la DélCdG. Ces dernières années, la DélCdG s'est notamment penchée de façon récurrente sur les systèmes de données des services, faisant régulièrement écho de leur activité dans son rapport annuel.[4]

Vu sa préoccupation concernant la masse croissante des informations contenues dans la banque de données ISIS (système de traitement des données relatives à la protection de l'Etat) et à la suite d'une requête de la commission de gestion du Grand Conseil du Canton de Bâle-Ville (CdG-BS), la DélCdG a décidé, le 16 avril 2008, d'approfondir la surveillance qu'elle exerce sur le traitement des données dans ISIS à travers une inspection formelle et de rédiger un rapport. L'enquête porte sur l'exploitation du système ISIS-NT (nouvelle technologie) par le Service d'analyse et de prévention (SAP). Le SAP a introduit le système à la fin de 2004 et s'est chargé de son exploitation jusqu'à la fin de 2009. Le système ISIS-NT avait pris le relais de l'ancien système ISIS, qui avait été mis en service quelques années après l'affaire des fiches.

Aujourd'hui, l'exploitation d'ISIS-NT est du ressort du nouveau Service de renseignement de la Confédération (SRC), qui est né au début de 2010 de la fusion entre le SAP et le Service de renseignement stratégique (SRS). Dans le cadre de cette réforme, le droit d'exécution relatif à la protection de l'Etat a été abrogé et les dispositions pertinentes ont été reprises dans les ordonnances concernant le SRC. Comme le rapport concerne la période jusqu'à la fin de l'année 2009, il se réfère aux bases légales en vigueur à ce moment-là, se rapporte cependant systématiquement aux bases légales actuellement valables. Dans la mesure où cela se révèle pertinent, le présent rapport contient aussi des conclusions qui concernent le devenir du traitement des données dans ISIS-NT sous l'égide du SRS.

1 Iv. pa. 89.006 du 31.1.1989 «Evénements survenus au sein du DFJP. Commission d'enquête parlementaire».
2 Pa. Iv. 89.243 du 22.11.1989 «Constitution d'une délégation».
3 RO **1992** 641
4 Rapports annuels 2005 et 2007 des CdG et de la DélCdG des Chambres fédérales, respectivement du 20.1.2006 (FF **2006** 4043 4167 ss) et du 25.1.2008 (FF **2008** 4579 4670 ss).

L'inspection présentée ici a été menée par la DélCdG dans la composition suivante:

- Claude Janiak, député au Conseil des Etats, président
- Pierre-François Veillon, conseiller national, vice-président
- Therese Frösch, conseillère nationale
- Alex Kuprecht, député au Conseil des Etats
- Isabelle Moret, conseillère nationale
- Hansruedi Stadler, député au Conseil des Etats

En juin 2010, Paul Niederberger a pris le relais d'Hansruedi Stadler en qualité de député du Conseil des Etats au sein de la DélCdG. Il a pris part à la rédaction finale du rapport et à la décision de publication.

2 Traitement des données relatives à la protection de l'Etat entre 1994 et 2009

2.1 Du système provisoire à ISIS-NT (1994–2004)

Le 22 novembre 1989, la CEP DFJP a rédigé un premier rapport[5] présentant les carences dans le traitement des données relatives à la protection de l'Etat mises au jour par l'enquête. Le 29 mai 1990, elle a publié un rapport complémentaire[6] concernant différents fichiers relatifs à la protection de l'Etat et la légalité des moyens mis en œuvre dans la recherche d'informations.

Outre le non-respect de certains principes de l'Etat de droit dans la recherche d'informations, la CEP DFJP avait alors constaté un manque de conduite politique, avec notamment pour conséquence la collecte de données inexactes, inutiles et sans intérêt pour la protection de l'Etat. Selon le rapport de la CEP, les informations ont dans certains cas été récoltées de manière aléatoire et sans aucune systématique, puis utilisées de manière incorrecte. Sur quoi la CEP avait déposé une motion exigeant la définition de critères précis pour la saisie des informations, ainsi que la destruction des enregistrements périmés.

Avant l'entrée en vigueur des bases légales nécessaires, le DFJP a réglé le traitement des informations par voie de directives[7] et d'instructions, qui ont ensuite été relayées par l'ordonnance du 31 août 1992 sur le système provisoire de traitement des données relatives à la protection de l'Etat[8]. Sur la base de cette ordonnance, le système ISIS a été mis en service en 1994 à titre provisoire comme instrument d'enregistrement et de gestion électronique des données relatives à la protection de l'Etat.

L'ordonnance prévoyait différentes procédures afin de garantir que seules les données du système pertinentes pour la sécurité de la Suisse et présentant une utilité future fussent traitées. Les principes et critères prévus par l'ordonnance ont été

5 Rapport de la CEP DFJP du 22.11.1989 «Evénements survenus au DFJP» (FF **1990** I 593–847).
6 Rapport complémentaire de la CEP DFJP du 29.5.1990 «Evénements survenus au DFJP» (FF **1990** I 1469–1513).
7 Directives du DFJP du 9.9.1992 sur la mise en application de la protection de l'Etat (FF **1992** VI 150–165).
8 RO **1992** 1659

repris dans le projet de nouvelle loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[9], que le Conseil fédéral a transmis au Parlement avec le message y relatif[10] en mars 1994.

Dans son message relatif à la LMSI, le Conseil fédéral avait défini de manière précise les règles auxquelles la pratique du traitement de l'information devait se conformer. Il estimait que l'évaluation de l'exactitude et de l'importance des informations était un préalable indispensable au traitement des données. Selon le message, les données personnelles ne pouvaient être traitées que dans la mesure et les limites temporelles nécessaires à l'accomplissement des tâches prévues par la LMSI. Il fallait donc que le contrôle des données ne se limite pas à la saisie initiale, mais soit périodique, puisque c'était aux yeux du Conseil fédéral la seule manière d'éviter que des informations inexactes, superflues ou devenues inutiles soient conservées et utilisées. Vu que des données seraient supprimées à chaque contrôle périodique, le Conseil fédéral s'attendait à ce que seul un petit nombre d'enregistrements dussent encore être effacés à l'expiration de la durée maximale de conservation.[11]

Les délibérations parlementaires concernant la LMSI ont débuté à l'été 1995 et ont donné lieu à plusieurs modifications du projet de loi, l'une d'elle donnant notamment un tour concret aux prescriptions de garantie de la qualité proposées dans le message du Conseil fédéral. Un examen périodique des données ISIS a été prévu à l'art. 15, al. 5, LMSI, le Conseil fédéral fixant une durée de conservation maximale pour les différentes catégories de données. Cette précision a été ajoutée à la suite d'une proposition déposée à l'instigation de la DélCdG par la Commission des affaires juridiques du Conseil des Etats.[12]

La LMSI a été adoptée le 21 mars 1997. Elle est entrée en vigueur le 1er juillet 1998, après le rejet de l'initiative populaire «S. o. S. – pour une Suisse sans police fouineuse» le 6 juin 1998. Le 1er décembre 1999, le Conseil fédéral a remplacé l'ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat par l'ordonnance ISIS du 1er décembre 1999[13]; le 27 juin 2001, il a édicté l'ordonnance sur les mesures visant au maintien de la sûreté intérieure (OMSI)[14].

En 1999, les organes de sûreté des cantons ont été raccordés à ISIS. Les cantons ont pu dès lors interroger directement la banque de données, mais la saisie est restée de la compétence exclusive de la Confédération. Les travaux de mise au point du successeur du système ISIS ont débuté en juin 2001. Ce chantier répondait à des impératifs techniques, vu que le fabricant ne proposait plus de soutien pour le développement du programme utilisé.

Le nombre des personnes enregistrées dans ISIS est passé de quelque 50 000[15] en 2001 à environ 60 000 en 2004, cette dernière valeur reflétant l'état au 18 fév-

9 Loi fédérale du 21.3.1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS **120**).
10 Message du 7.3.1994 concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire «S. o. S. – pour une Suisse sans police fouineuse» (FF **1994** II 1123–1216).
11 FF **1994** II 1180
12 BO **1995** E 588 (Schoch Otto AR).
13 RO **1999** 3461
14 RO **2001** 1829
15 Réponse du Conseil fédéral du 5.9.2001 à la question ordinaire de Dardel, Jean-Nils «Personnes enregistrées dans les systèmes de données JANUS et ISIS» (01.1068).

rier 2004 tel que présenté par le SAP à la Commission des affaires juridiques du Conseil national (CAJ-N) dans la discussion relative au rapport sur l'extrémisme[16]. Selon cette source, ce nombre comprenait approximativement 2500 ressortissants suisses.[17]

A la fin de 2004, le nouveau système ISIS-NT (nouvelle technologie) était assez abouti pour que le SAP puisse lancer l'exploitation au début de 2005. A partir de ce moment, le SAP a enregistré toutes les nouvelles informations exclusivement dans ISIS-NT. Les données de l'ancien système ISIS avaient été transférées dans ISIS-NT pendant la dernière quinzaine de 2004.

Dans l'ancien système, ces données étaient organisées hiérarchiquement. Leur structure ne correspondait donc pas à celle d'une base de données relationnelle, système sur lequel s'était appuyée la conception d'ISIS-NT. Après la migration des données, un grand travail d'adaptation manuelle aux structures de classement d'ISIS-NT a encore été nécessaire. Cela sans compter qu'il a fallu que les utilisateurs du système s'adaptent au nouveau modèle, ce qui exigeait une approche radicalement différente, notamment pour la saisie des nouvelles données. Enfin, ces nouveautés techniques d'ISIS ont aussi requis l'adaptation des notions techniques dans l'ordonnance ISIS, qui a été révisée le 30 juin 2004 pour être en phase avec le nouveau système, et est entrée en vigueur le 1er septembre 2004.[18]

2.2 Règles régissant le traitement des données dans ISIS-NT

Pour qu'elles soient compatibles avec la structure relationnelle des données d'ISIS, il faut représenter les relations internes d'une communication comme des relations de banque de données dans le système. Par exemple, il faut commencer par identifier les personnes et les organisations dans une communication, puis relier ces objets avec la communication, mais aussi entre eux. Un objet inconnu du système donne lieu à un nouvel enregistrement.

L'enregistrement autonome dans ISIS-NT n'est possible que lorsque la personne concernée revêt en elle-même de manière univoque de l'importance pour la protection de l'Etat. Si une personne revêt de l'importance pour la protection de l'Etat uniquement de par son lien avec un objet, elle est réputée «tiers». Le contact avec une personne considérée comme une menace pour la sûreté peut conduire à l'enregistrement en tant que tiers. De même, le détenteur d'un véhicule peut être enregistré en tant que tiers si son véhicule est saisi dans le système à la suite d'un événement touchant à la protection de l'Etat.

Les personnes et les tiers sont tous deux saisis dans ISIS-NT en tant qu'objets et peuvent donc être reliés avec d'autres personnes, organisations ou communications par le truchement de relations de banques de données. Du point de vue technique, les tiers se distinguent uniquement par une mention supplémentaire qui les identifie comme tels.

16 Rapport du Conseil fédéral du 25.8.2004 sur l'extrémisme (donnant suite au postulat 02.3059 du 14 mars 2002 du groupe démocrate-chrétien; FF **2004** 4693).
17 Ces chiffres ont été publiés dans le rapport annuel 2005 des CdG et de la DélCdG du 20.1.2006 (FF **2006** 4043 4167).
18 RO **2004** 3495

Les informations versées dans ISIS sur la base des communications reçues sont soumises à un contrôle de la Section Assurance qualité après leur saisie. Selon l'ordonnance, elle doit examiner si l'indication des sources et la date de la prochaine appréciation générale ont été saisies correctement. Au-delà de ces informations de nature formelle, elle doit examiner si les informations sont fiables quant à leur teneur et si elles ont été appréciées correctement par rapport à d'éventuelles autres informations déjà saisies. Il convient d'appliquer le principe visé à l'art. 15, al. 1, LMSI, qui interdit le traitement de données imprécises ou non nécessaires à la protection de l'Etat. Une information peut être réputée pertinente uniquement si son traitement sert à l'accomplissement de la mission prévue à l'art. 2 LMSI, à savoir notamment détecter précocement et combattre les dangers liés au terrorisme, au service de renseignements prohibé, à l'extrémisme violent et au transfert illégal de technologie.

Au plus tard cinq ans après la saisie de la première communication concernant une personne, la Section Assurance qualité doit procéder à une appréciation générale sur la base des informations disponibles, pour déterminer si la personne présente toujours une menace pour la sûreté intérieure. Elle doit aussi examiner lesquelles parmi les communications enregistrées sur cette personne sont nécessaires à l'accomplissement de la mission de protection de l'Etat.

Si la conclusion découlant de l'appréciation générale est que la personne ne présente pas de risque plausible pour la sûreté intérieure, l'objet relatif à cette personne doit être effacé de la banque de données. Les communications relatives à cette personne ne sont toutefois pas effacées si elles restent utiles du fait d'une relation avec une autre personne qui demeure enregistrée. Ainsi, une liste de personnes par laquelle un canton a communiqué tous les extrémistes de gauche et de droite reste dans le système ISIS aussi longtemps qu'une seule personne figurant sur la liste revêt de l'importance pour la protection de l'Etat.

Lorsque l'enregistrement d'une personne est effacé, il n'est plus possible de trouver les informations relatives à cette personne qui demeurent dans le système par une recherche orientée personne. La recherche en texte intégral dans les communications, comme on la connaît par exemple sur l'internet, n'est plus possible, car les communications entrantes sont enregistrées sous forme d'image, procédé technique qui empêche la reconnaissance textuelle.

Un tiers peut rester enregistré en cette qualité pendant cinq ans au plus. Des informations nouvelles peuvent toutefois faire qu'un tiers peut revêtir en soi une importance nouvelle pour la protection de l'Etat, et voir ainsi le statut de son enregistrement modifié. Ce sont alors les règles générales applicables à l'effacement pour les personnes enregistrées qui s'appliquent.

La durée maximale de conservation des données relevant de la protection de l'Etat dans ISIS est de 15 ans. Dans la pratique du SAP, cette limite se réfère à la date de l'entrée des communications. Une personne qui a été enregistrée 15 ans auparavant comme présentant un risque pour la sûreté à la suite d'une communication peut toutefois rester enregistrée après l'effacement de cette information. Elle peut continuer de figurer dans ISIS aussi longtemps que des communications la concernant sont saisies dans le système. Les vieilles communications doivent cependant être effacées au fur et à mesure lorsqu'elles dépassent la durée maximale de conservation fixée à 15 ans.

2.3 Problèmes liés au passage à ISIS-NT (2005–2007)

Le 24 mai 2005, la DélCdG s'est penchée pour la première fois sur le traitement des données dans le nouveau système ISIS-NT. Dans le cadre de son enquête sur l'affaire Achraf[19], la DélCdG a fait une visite inopinée au SAP pour se faire expliquer par les collaborateurs de la Section Analyse préliminaire chargés de la saisie des informations dans la base de données les procédures de sélection, d'appréciation et de saisie des données dans le système ISIS.

Toutes les communications reçues par le SAP sont systématiquement numérisées dans un document après leur entrée et transmises à la Section Analyse préliminaire pour enregistrement. La section détermine si une communication doit figurer dans la banque de données «ISIS01 Protection de l'Etat» ou dans un autre des divers fichiers de données qui constituent le système ISIS, par exemple celui relatif aux actes administratifs (ISIS02). Le cas échéant, la Section Analyse préliminaire peut décider que la communication n'a pas lieu d'être saisie et qu'elle doit être détruite.

Selon les indications des intéressés, les collaborateurs de la Section Analyse préliminaire procèdent à une analyse matérielle de la communication reçue, tout au moins lorsque cela se révèle nécessaire pour l'exactitude de l'enregistrement. Cette étape comprend aussi la rédaction d'une brève synthèse de la communication, dont le contenu est accessible via une recherche dans ISIS.

Le travail d'enregistrement exige des connaissances concernant les personnes et les groupes que le SAP considère comme relevant de la sûreté de l'Etat car, au moment de l'enregistrement, des relations de type banque de données doivent être établies avec les objets figurant déjà dans le système.

L'appréciation finale de l'exactitude et de l'importance des informations d'une communication ne se fait toutefois pas au moment de la saisie. La décision de savoir si une communication a sa place dans ISIS est du ressort de la Section Assurance qualité. Le cas échéant, cette dernière doit effacer les communications saisies par la Section Analyse préliminaire qui ne satisfont pas aux conditions prévues par la LMSI.

Par sa visite au SAP, la DélCdG voulait par ailleurs établir si des retards avaient grevé le traitement de communications importantes en relation avec l'affaire Achraf. Lors de la visite, le chef du SAP a reconnu qu'il pouvait arriver que l'analyse préliminaire soit saturée et qu'il y avait en l'occurrence effectivement eu des retards dans la saisie. Il a estimé que le passage au nouveau système ISIS-NT avait accru le travail en souffrance, jugeant toutefois que la situation n'avait pas été dramatique.

La procédure est ainsi conçue que, pour la Section Analyse préliminaire, c'est l'efficacité de l'enregistrement qui est prioritaire. Une appréciation fondée quant au bien-fondé de la saisie d'une communication et de l'enregistrement de personnes conformément à la mission et aux critères définis par la LMSI est laissée aux soins de la Section Assurance qualité, qui n'intervient que dans un deuxième temps. L'organisation du traitement de l'information au sein du SAP assigne ainsi à la Section Assurance qualité un rôle crucial dans la garantie de la légalité du traitement des données dans ISIS.

19 Le dispositif de sécurité de la Suisse et le cas Mohamed Achraf – appréciation résumée sous l'angle de la haute surveillance parlementaire, rapport de la DélCdG du 16.11.2005 (FF **2006** 3577–3584).

L'utilisation subséquente des données, que ce soit pour établir des analyses de la menace ou pour échanger des informations avec l'étranger, se fonde par conséquent sur la prémisse qui veut que la qualité de toutes les données saisies dans ISIS est garantie par les règles de la LMSI.

Le 16 novembre 2005, la DélCdG a mené une discussion interne concernant le nombre des personnes enregistrées dans ISIS, avec pour toile de fond les chiffres livrés par le SAP, qui avaient soulevé différentes questions à la CAJ-N à l'occasion des délibérations concernant le rapport du Conseil fédéral sur l'extrémisme.

Organe de surveillance parlementaire compétent, la DélCdG décida de suivre systématiquement l'évolution du nombre des enregistrements dans le nouveau système ISIS-NT. Dans son programme annuel 2006, elle requit alors du DFJP une statistique actualisée d'ISIS, et consacra un chapitre entier du rapport annuel 2005 des Commissions de gestion et de la Délégation des Commissions de gestion au traitement des données dans ISIS.[20]

Le 3 mars 2006, la DélCdG a reçu le rapport exigé sur le traitement des données dans ISIS. Elle s'est penchée de manière approfondie sur les informations reçues le 29 mars 2006, à l'occasion d'une discussion avec des représentants du SAP.

Le rapport chiffrait le nombre des personnes enregistrées présentant un profil pertinent pour la protection de l'Etat à environ 100 000 au début de 2006. Selon le rapport, cette augmentation massive du nombre de personnes enregistrées par rapport à l'ancienne version d'ISIS tenait au fait que, pour des raisons techniques, tous les tiers avaient dû être saisis à nouveau, et qu'un grand nombre de tiers avaient été considérés comme revêtant en eux-mêmes une importance du point de vue de la protection de l'Etat. Le rapport chiffrait à environ 50 000 le nombre des tiers restants dont l'importance pour la protection de l'Etat n'était pas encore établie.

Le SAP expliquait alors que les données migrées dans ISIS-NT étaient appelées à être mises au net et que le chiffres fournis devaient donc être considérés comme provisoires. Il était prévu que le toilettage des données serait achevé à la fin de 2006, moment à partir duquel on disposerait de chiffres fiables.

D'après le rapport, la difficile migration des données de l'ancien système ISIS vers ISIS-NT s'était déroulée sans problème à la mi-décembre 2004. Lors de l'audition, il avait été souligné qu'aucune perte de données n'était à déplorer. Du côté de la DélCdG, la question avait été soulevée de savoir si les données qui ne méritaient pas d'être transférées avaient été écartées avant la migration. Réponse du SAP: pareil examen n'aurait pas permis de procéder à la migration dans le délai prévu (fin 2004), d'où la décision de ne pas opérer cette distinction.

Le rapport précisait en outre que la qualité et la pertinence des données ISIS du point de vue de la protection de l'Etat devaient être appréciées par la Section Assurance qualité (2,8 équivalents plein temps). Or l'assurance qualité mettait la priorité sur le contrôle et l'optimisation de la saisie des données et la mise au net des données transférées à partir de l'ancien système ISIS.

Les deux missions entraient en fait dans le domaine de compétence de la Section Analyse préliminaire. Mais, comme l'a révélé l'audition, le passage à ISIS-NT a posé de gros problèmes aux collaborateurs de la section. L'engagement des ressour-

20 Rapport annuel 2005 des CdG et de la DélCdG du 20.1.2006 (FF **2006** 4043 4167).

ces de l'assurance qualité pour la saisie était donc apparu être la mesure adéquate pour limiter le travail de correction subséquent dans ce domaine.

Selon le rapport, le SAP ne disposait pour l'année 2005 d'aucune statistique concernant l'exécution des appréciations générales périodiques prescrites par la loi. A un autre passage, le rapport évoquait cependant la reprise des appréciations générales au rythme usuel en 2006. Ce faisant, le rapport évitait de mentionner que les appréciations générales périodiques avaient été suspendues en 2005, manifestement pour maîtriser les problèmes posés par le toilettage des anciennes données et la saisie des nouvelles.

Le SAP avait par ailleurs intégré au rapport des valeurs empiriques remontant au temps de l'ancien système ISIS: selon ces valeurs, un tiers des personnes enregistrées avaient déjà été effacées à la première appréciation après cinq ans, un tiers avait fait l'objet d'une mise au net ponctuelle et un tiers seulement avait été retravaillé complètement pendant trois années supplémentaires. Lors de l'audition, la DélCdG avait en outre été assurée que l'appréciation générale des données prévue par la loi se déroulait «normalement».

Le 28 août 2006, la DélCdG a fait une autre visite inopinée au SAP.[21] Elle s'est entretenue avec des collaborateurs du service et, avec leur concours, a consulté ISIS par sondage. Dans un cas, la DélCdG a constaté qu'une personne avait été enregistrée sur la seule base d'une recherche effectuée par un autre service fédéral dans la banque de données Protection de l'Etat (ISIS01). Le SAP n'avait pourtant lui-même aucune information sur la personne et en avait informé le service concerné. La DélCdG a critiqué l'enregistrement dans ISIS01 car un tel enregistrement présupposait l'existence d'informations importantes pour la protection de l'Etat concernant la personne en question. Le chef du SAP a opposé que ladite personne n'avait pas été enregistrée comme suspect, mais dans le cadre d'une demande normale, ajoutant qu'il était bien possible que l'enregistrement aurait dû figurer dans la banque de données Administration (ISIS02).

La visite sur place a confirmé les déclarations antérieures du SAP, selon lesquelles le travail requis par la saisie avait augmenté substantiellement du fait de la structure relationnelle des données d'ISIS-NT. En outre, la Section Assurance qualité investissait selon ses propres dires beaucoup de temps dans l'amélioration de la saisie des données. A ce moment-là, la section était dotée de 4,6 équivalents plein temps répartis entre 5 personnes.

D'après le SAP, le système s'était stabilisé une année et demie après la mise en service, ouvrant une phase d'amélioration avec l'intégration de nouvelles fonctions qui s'étaient révélées nécessaires. Ces nouveautés comportaient des programmes d'automatisation des effacements et un module d'archivage. Le nombre des personnes enregistrées revêtant une importance en propre pour la protection de l'Etat était toujours estimé à 100 000, la part des ressortissants suisses étant de l'ordre de 4 %.

Sur mandat de la DélCdG, le DFJP a présenté le 1er février 2007 un nouveau rapport sur le traitement des données dans ISIS-NT, avec notamment des statistiques actualisées. A sa séance du 21 février 2007, la DélCdG a noté que la mise au net des données n'avait pas été achevée à la fin de 2006. Le nombre des personnes enregistrées avait augmenté à 112 000, celui des tiers, à 56 000. La proportion des personnes titulaires d'un passeport suisse était de 3,5 % et celle des personnes domiciliées

21 Communiqué de presse du 30.8.2006 de la DélCdG.

en Suisse, de 11 %. Le SAP n'avait pas voulu faire de pronostic fiable concernant l'évolution future de la base de données, tout en attendant un «tableau complètement nouveau» pour la fin de 2007.

Le 23 février 2007, la DélCdG a écrit au chef du DFJP que les derniers chiffres en date concernant les enregistrements dans ISIS étaient pour elle source de préoccupation, en l'invitant à expliquer pourquoi la mise au net des données n'avait pas été achevée à la fin de 2006, comme l'avait annoncé le SAP, et pourquoi le nombre des personnes enregistrées et des communications saisies dans le système avait continué d'augmenter.

Le 30 mars 2007, le chef du DFJP a répondu à la DélCdG que la mise au net des données avait connu des retards parce que les ressources limitées et le rythme élevé des affaires courantes n'avaient pas permis un traitement plus rapide[22]. Autrement dit, le chef du DFJP a déclaré que les ressources disponibles avaient été investies prioritairement dans la saisie de nouvelles données dans ISIS. La lettre du chef du DFJP reste par contre muette sur les ressources humaines par ailleurs disponibles pour les contrôles initiaux et les appréciations générales périodiques.

Dans sa lettre, le chef du DFJP prévoyait en revanche que la base de données serait définitivement mise à jour avant la fin de 2007, précisant qu'il avait donné son feu vert à un renforcement du SAP par six collaborateurs temporaires pour l'année en cours. Il poursuivait en soulignant qu'il n'était pas possible de déterminer les causes précises qui avaient induit une augmentation du nombre des personnes saisies dans ISIS-NT en 2006 tant que la mise au net des données n'était pas achevée. Le chef du DFJP se déclarait convaincu que les données ISIS étaient collectées, traitées et effacées dans les délais conformément aux sévères prescriptions légales[23], renvoyant aux contrôles pertinents de l'inspectorat du DFJP.

Le rapport de l'inspectorat du DFJP, dont la DélCdG a pris acte en date du 16 février 2007, n'analysait toutefois pas le fonctionnement de la Section Assurance qualité, mais se concentrait sur les problèmes liés à la mise au net et à la saisie de nouvelles données dans ISIS-NT. Le rapport constatait qu'ISIS-NT avait accru les exigences pour le personnel chargé de la saisie des données. Cela à double titre: le nouveau système exigeait des capacités d'analyse accrues et, par ailleurs, le volume des données à saisir était en augmentation constante, selon le rapport. Le rapport relevait en outre un déficit structurel de ressources dans le domaine de la saisie, déficit auquel un renforcement temporaire ne permettrait pas de remédier. Enfin, le rapport précisait que le système ISIS-NT était tout entier tributaire d'une saisie des données de haute qualité et en temps utile[24].

2.4 Requête de la CdG du Grand Conseil du canton de Bâle-Ville (2008)

Dans une lettre du 27 novembre 2007, la CdG du Grand Conseil du canton de Bâle-Ville a demandé à la DélCdG de s'exprimer sur l'organisation des compétences dans la surveillance de l'activité cantonale de sûreté. La CdG-BS tenait pour acquis

22 Lettre du 30.3.2007 du chef du DFJP à la DélCdG, p. 1.
23 Lettre du 30.3.2007 du chef du DFJP à la DélCdG, p. 2.
24 Rapport de l'inspectorat du DFJP du 16.2.2007 sur le traitement des données dans ISIS, p. 20 du texte allemand (non traduit).

qu'elle disposait de vastes compétences de contrôle de la sûreté cantonale dans le cadre de sa haute surveillance. Comme elle allait l'apprendre, l'autorité cantonale de protection de l'Etat et le SAP ne partageaient pas ce point de vue. A leur avis, aux termes de l'art. 23, al. 1, OMSI[25], la compétence de l'autorité cantonale se limitait à contrôler que les données relatives à la sûreté intérieure et les autres informations de police étaient traitées séparément. Les deux organes estiment que la DélCdG et le département responsable ont la compétence exclusive de la surveillance de l'activité des services de la sûreté cantonale.

La CdG-BS a en outre informé la DélCdG qu'elle était fondée à penser que le SAP traitait des informations sur six membres de son Grand Conseil. Elle a invité la DélCdG à examiner la légalité de cette activité, notamment à la lumière de l'art. 3 LMSI. Celui-ci prévoit que le traitement de telles informations relatives à la personne est licite uniquement lorsqu'une présomption sérieuse permet de soupçonner les personnes visées de se servir de l'exercice des droits politiques pour dissimuler la préparation ou l'exécution d'actes relevant du terrorisme, du service de renseignements ou de l'extrémisme violent.

A la demande de la CdG-BS, le préposé à la protection des données du canton de Bâle-Ville avait déjà essayé de vérifier auprès du service cantonal de protection de l'Etat si des données concernant les députés cantonaux avaient été traitées. Il avait toutefois été renvoyé au SAP, qui doit donner son accord pour qu'un organe de contrôle cantonal puisse consulter ISIS (art. 23, al. 2, OMSI). Le SAP a refusé un contrôle cantonal des données en question, aussi bien sur le principe que, par la suite, sur le cas concret des six députés cantonaux, en faisant valoir que les dispositions relatives à la protection d'informations provenant de relations avec l'étranger s'opposaient à la consultation (art. 17, al. 7, LMSI).

La requête de la CdG-BS est parvenue à la DélCdG après sa dernière séance de 2007. Après s'être constituée pour la nouvelle législature en décembre 2007, la DélCdG s'est saisie de la demande de la CdG-BS dès sa première séance de 2008, arrêtant comme première mesure une visite inopinée au SAP afin de vérifier sur pièces les indications de la CdG-BS.

Le contrôle a révélé, le 11 mars 2008, que deux des six députés au Grand Conseil bâlois figuraient dans la banque de données Protection de l'Etat d'ISIS. La DélCdG a en outre été fondée à penser que deux autres députés étaient enregistrés comme tiers au moment de la demande du préposé bâlois à la protection des données, en septembre 2007.[26] Leur enregistrement avait dû être effacé à la suite de la requête du canton de Bâle-Ville. La DélCdG n'a trouvé aucune information dans ISIS-NT concernant les deux derniers députés.

Le 16 avril 2008, la DélCdG a adressé une lettre au DFJP l'enjoignant de motiver l'enregistrement durable de deux membres du Grand Conseil du canton de Bâle-

25 Le Conseil fédéral a abrogé l'OMSI le 1.1.2010. Les dispositions de l'art. 23 OMSI sont depuis reprises à l'art. 35 de l'ordonnance du 4.12.2009 sur le Service de renseignement de la Confédération (OSRC; RS **121.1**).

26 En requérant que soit produite la correspondance entre le SAP et le préposé à protection des données du canton de Bâle-Ville, la DélCdG a constaté que le SAP, lorsqu'il a contrôlé le nom des six députés au Grand Conseil, avait marqué leur statut dans ISIS sur une copie de la demande d'accès du canton de Bâle-Ville. Selon ces indications, quatre noms figuraient dans ISIS.

Ville à la lumière de l'art. 3 LMSI. Elle a en outre requis un avis sur l'organisation des compétences dans le domaine de la surveillance de la protection de l'Etat.

Le même jour, la DélCdG a écrit au président de la CdG-BS pour l'informer de sa démarche visant à contrôler sur place si les députés du Grand Conseil mentionnés figuraient dans ISIS. Tout en précisant qu'il ne lui appartenait pas de donner des informations sur le traitement des données de personnes déterminées dans ISIS, la délégation a assuré le président qu'elle avait fait, dans les limites de ses possibilités, les démarches nécessaires pour mettre fin à d'éventuelles infractions.

Le 16 avril 2008 encore, la DélCdG a décidé d'examiner de façon systématique le traitement des données dans ISIS-NT dans le cadre d'une enquête formelle, en accordant une attention particulière aux causes de l'augmentation du nombre des enregistrements et au fonctionnement de l'assurance qualité.[27]

Le 22 mai 2008, la DélCdG s'est penchée sur les derniers chiffres en date concernant les données saisies dans ISIS-NT et sur les progrès réalisés dans la mise au net des données transférées dans le cadre de la migration fin 2004. La poursuite de l'augmentation des enregistrements a confirmé à la délégation qu'elle avait axé son enquête dans la bonne direction.

Après le rapport du SAP du 22 avril 2008, le nombre des personnes enregistrées était de 114 000, notamment du fait qu'un grand nombre de tiers étaient passés au statut de personnes revêtant en propre une importance du point de vue de la protection de l'Etat. Le nombre des tiers était descendu à 47 000. Parmi les personnes enregistrées dans ISIS-NT, 3,9 % étaient des ressortissants suisses. Le SAP n'a pu donner aucun chiffre concernant le nombre des enregistrements effacés par la Section Assurance qualité.

La délégation constatait que la mise au net des données n'avait pas non plus pu être achevée en 2007. Le SAP comptait alors devoir poursuivre ce travail jusqu'à la fin de 2008, estimant que les principales incohérences dans les données transférées seraient alors corrigées. La Section Assurance qualité se chargerait ensuite des erreurs subsistantes dans le cadre des appréciations générales périodiques prescrites par la loi.

A l'image des trois années précédentes, les déclarations du SAP concernant l'état des données dans ISIS se sont concentrées sur la maîtrise de la migration des données. Le nouveau modèle de données d'ISIS-NT s'est révélé nettement plus exigeant sous l'angle de la cohérence des données. Les données ISIS saisies avant la migration présentaient manifestement des carences à cet égard. Ce constat soulève la question du sérieux avec lequel le SAP avait traité l'assurance qualité dans l'ancien système ISIS. Lors de l'audition du 22 mai 2008, un représentant du SAP soucieux de mettre en valeur les avantages d'ISIS-NT sous l'angle de la qualité des données a déclaré que, sous l'ancien régime d'assurance qualité, personne n'aurait eu l'idée de vérifier l'entrée précédente pour voir si un processus (soit une communication) devait être effacé.

Depuis le passage à ISIS-NT, pour le SAP, la question de savoir si les données mises au net dans ISIS moyennant une somme considérable de travail étaient en soi pertinentes pour la sécurité de la Suisse et si elles respectaient les critères de la

27 La DélCdG a annoncé la décision le 3.7.2008 dans un communiqué de presse rendant compte des différentes activités en cours de la délégation.

LMSI a été complètement occultée par les difficultés liées à la maîtrise du nouveau système. Dans le même fil, le SAP estimait que, dans le nouveau système, l'assurance qualité revenait «quasiment à une garantie» permettant d'éviter que des données soient traitées sans respecter les objectifs et les limites fixés par la LMSI.

Le 14 juillet 2008, le DFJP a transmis à la DélCdG le résultat du contrôle qu'elle avait demandé concernant les deux députés du Grand Conseil du canton de Bâle-Ville enregistrés dans ISIS-NT. Le DFJP a jugé que l'enregistrement était justifié pour l'un des deux députés. Il a indiqué par ailleurs que l'enregistrement du deuxième député avait été effacé par la Section Analyse préliminaire à l'occasion d'une appréciation générale anticipée.

A sa séance du 26 août 2008, la DélCdG ne s'est pas montrée pleinement convaincue par les déclarations du DFJP. L'entrée concernant un député avait certes été effacée, mais aucune raison suffisante justifiant l'enregistrement de cette personne n'avait jamais existé. L'effacement de l'enregistrement n'a par ailleurs pas été opéré par le SAP de son propre chef après avoir constaté l'absence de tout lien entre la personne et la protection de l'Etat, mais du seul fait de l'intervention de la DélCdG. Sans la requête de la CdG-BS, la personne en question figurerait encore dans ISIS-NT.

La DélCdG a jugé utile de se procurer du matériel permettant de se faire une image concrète de la manière dont le SAP exécutait au terme prévu les effacements prescrits par la loi. Elle a donc exigé du DFJP, par lettre du 26 août 2008, qu'il lui fournisse l'intégralité des informations concernant les personnes domiciliées en Suisse dont l'enregistrement a été effacé par le SAP dans le cadre de l'appréciation générale périodique.

A cet effet, tous les champs de données importants tirés d'ISIS-NT concernant une personne enregistrée ont été imprimés sous forme de tableau (extrait intégral). Outre les données d'identité, un extrait intégral comprend les renvois aux relations de la personne concernée avec les communications reçues et avec d'autres personnes ou organisations.

Le cas du député qui est resté enregistré a donné lieu à d'autres éclaircissements au DFJP. En septembre 2008, l'Office fédéral de la justice (OFJ) a été chargé d'apprécier si les principes et les critères légaux avaient en l'occurrence été interprétés et appliqués correctement.

Dans son avis du 18 octobre 2008, l'OFJ a jugé les informations en question dans ISIS-NT comme étant peu solides et en partie non pertinentes pour la protection de l'Etat. Selon l'OFJ, l'analyse générale n'a donné aucun indice concluant montrant que la personne en question se livrerait à des activités faisant peser une menace sur l'Etat, et il n'existe aucune base fondant la poursuite du traitement des données.

A la suite de l'avis de l'OFJ, le SAP s'est vu contraint d'effacer l'enregistrement du député concerné dans ISIS-NT. Le SAP a ensuite communiqué l'effacement, exécuté le 3 novembre 2008, et remis à la DélCdG l'extrait intégral demandé, avec copie des communications effacées.

2.5 Conséquences de la pratique adoptée pour les enregistrements dans ISIS-NT

Le 18 novembre 2008, la DélCdG a eu une discussion concernant la pratique en matière d'enregistrement dans ISIS-NT avec le chef suppléant du SAP. Celui-ci a souligné qu'ISIS-NT n'était pas un casier judiciaire ou un répertoire de suspects, mais un outil qui vise à documenter l'activité déployée par le SAP pour la protection de l'Etat.

Lorsque, par exemple, une demande de renseignement qui émane de l'étranger concerne une personne sur laquelle le SAP n'a pas d'informations et qu'il ne peut par conséquent pas apprécier son importance pour la protection de l'Etat, le SAP enregistre quand même la personne en qualité de tiers. Même si le SAP communique à l'autorité étrangère qu'il n'a connaissance d'aucune information négative sur la personne, celle-ci fait néanmoins l'objet d'un enregistrement, ce que le chef suppléant du SAP estime fondé, car le SAP ne retrouverait plus les informations dans le système sans cet enregistrement et ne pourrait pas documenter qu'il avait envoyé une réponse à l'autorité étrangère concernant la personne en question.

De la même manière, le SAP a justifié le traitement des données relatives à un membre du Grand Conseil du canton de Bâle-Ville, bien que son importance pour la protection de l'Etat n'ait jamais pu être établie de façon concluante. Le fait que des informations liées à des organisations extrémistes kurdes aient régulièrement été mises en relation avec la personne en question aurait justifié un enregistrement, même si elle n'était pas considérée personnellement comme une menace pour la sûreté intérieure ou extérieure. Après que l'OFJ eut conclu dans l'intervalle qu'une poursuite du traitement de ces données n'était pas indiquée, le SAP a effacé l'enregistrement.

Le chef suppléant du SAP a par ailleurs défendu le point de vue selon lequel le traitement de données non pertinentes ou fausses n'était pas en soi une «atteinte grave à la personnalité» pour l'intéressé, surtout tant que le traitement restait une affaire interne et que l'information n'était pas utilisée contre lui. Reprenant l'exemple du député bâlois mentionné, le SAP a fait valoir que les informations contenues dans ISIS-NT n'avaient porté préjudice en aucune manière à la personne, qui a au demeurant été élue au Grand Conseil et dont l'activité économique n'a pas pâti d'une appréciation sécuritaire négative.

De même, le SAP ne voyait pas de problème à confirmer, sur demande d'un service de renseignement européen, que le député en question avait assisté à un procès à l'étranger en qualité d'observateur. Cela alors que la requête provenant de l'étranger décrivait une personne qui ne correspondait pas forcément avec les données personnelles du député. En fait, sur la foi de ses propres informations, le SAP ne savait pas si l'intéressé avait effectivement assisté à un procès en tant qu'observateur. Il avait fondé sa déclaration sur la seule demande du service étranger.

Le SAP a en outre informé le service étranger de relations non spécifiées du député avec un comité de soutien pour un groupe extrémiste. Au-delà d'une remarque sans détails ni indication de la source, la DélCdG n'a pourtant pas trouvé d'information dans ISIS-NT qui aurait étayé ce soupçon. Malgré les lacunes patentes qui grevaient les informations a sa disposition, le SAP a présenté le contenu de la communication au service partenaire comme étant consolidé.

Aux yeux du SAP, la transmission de ces informations non consolidées était indispensable à la sauvegarde d'intérêts importants liés à la sûreté de la Suisse ou de l'Etat destinataire; il a donc donné suite en s'appuyant sur l'art. 17, al. 3, let. d, LMSI. Comme l'a expliqué le chef suppléant du SAP, le bureau des liaisons du SAP, qui a compétence pour les transactions avec l'étranger, peut dans la plupart des cas fonder une transmission d'information à l'étranger en invoquant cette disposition.

Le chef suppléant du SAP a souligné que la saisie d'information dans ISIS-NT n'avait rien de mécanique, mais exigeait une réflexion sur le contenu souvent très riche des communications. Il a précisé que la saisie devait obéir à de volumineuses directives. Or un survol des 556 pages des directives de la Section Analyse préliminaire régissant le traitement des informations montre que les communications ne sont pas saisies dans ISIS-NT après une appréciation matérielle, mais selon des règles mécaniques.

Ainsi, les demandes de naturalisation ou d'asile sont saisies dans la banque ISIS01 (Protection de l'Etat) lorsque le requérant y est déjà enregistré pour une autre raison.[28] Cette règle est aussi appliquée lorsque le SAP reconnaît à l'intention de l'Office fédéral des migrations (ODM) que le requérant ne présente pas de menace pour la sûreté intérieure (v. exemple au chap. 2.9.10). Si la personne ne fait pas l'objet d'une entrée dans ISIS01, la demande est dans tous les cas saisie dans ISIS02 (Administration).

Font aussi l'objet d'un enregistrement dans la banque de données Protection de l'Etat ISIS01 les milliers de personnes enregistrées à la suite d'un contrôle des photos d'identité[29] à la frontière. Ces personnes sont enregistrées comme tiers sans égard de la menace concrète qu'ils pourraient présenter. Aux termes des directives, un tiers se voit de plus attribuer automatiquement en propre une importance pour la protection de l'Etat dès qu'il apparaît dans plus de deux communications. On reconnaît ici aisément un mécanisme qui débouche forcément sur une augmentation du nombre des personnes qui figurent dans ISIS-NT et sont perçues comme une menace pour la sûreté de la Suisse.

A l'arrivée d'une nouvelle communication, la Section Analyse préliminaire est en outre tenue d'identifier et de saisir tous les liens possibles avec des personnes déjà enregistrées. Le chef suppléant du SAP fonde cette pratique sur le fait que, s'agissant des personnes déjà enregistrées, pouvoir user de l'ensemble des informations

28 L'ODM transmet au SAP toutes les demande de naturalisation pour examen sous l'angle d'une possible menace pour la sûreté intérieure. De même, le SAP contrôle les demandes d'asile de toutes les personnes de certains pays. La liste de ces Etats est établie par le SAP et actualisée au besoin. En 2009, le SAP a examiné quelque 34 800 demandes de naturalisation et 2250 dossiers de demande d'asile.

29 Les contrôles des photos d'identité remontent à un programme lancé en 1968 pour appuyer la défense contre l'espionnage et fondé sur l'interrogation des visiteurs en provenance des pays de l'Est (v. chap. VI.8 du rapport de la CEP DFJP). Pour pouvoir interroger les personnes sur d'éventuels contacts avec des services de renseignement étrangers, le passeport des visiteurs transitant par des postes de douane sélectionnés a été photographié par la police frontalière et les documents photographiques ont été conservés dans une archive dédiée au contrôle des photos d'identité (v. chap. II 2.3 du rapport complémentaire de la CEP DFJP). Le 12 février 1990, le chef du DFJP a stoppé, dans le cadre d'un train de mesures d'urgence, la saisie des passeports des ressortissants suisses et d'étrangers domiciliés en Suisse. Le programme de saisie des photos d'identité a depuis été prolongé pour les titulaires d'un passeport de certains Etats.

disponibles présente un intérêt accru pour le service. A ses yeux, ces informations supplémentaires peuvent être utilisées non seulement pour étayer le plus rapidement possible l'importance d'une personne du point de vue de la protection de l'Etat, mais aussi pour l'exclure en temps utile. Cette intention est toutefois remise en cause lorsque les règles de saisie du SAP font passer une personne du statut de tiers à celui de personne revêtant une importance directe du point de vue de la protection de l'Etat dès que plus de deux communications concernent l'intéressé. Dans ce cas, une information à décharge entraîne l'enregistrement au lieu de l'effacement de la personne concernée.

Comme le montrent les exemples présentés plus haut et les mécanismes d'enregistrement des tiers, une entrée dans ISIS-NT n'est pas forcément un indice fiable d'une appréciation matérielle de la pertinence de l'enregistrement, comme l'exige l'art. 15, al. 1, LMSI.

En cours d'audition, le chef suppléant du SAP n'a pas exclu que des erreurs étaient possibles lors de la saisie et qu'un fait pouvait se révéler par la suite moins pertinent pour la sûreté de l'Etat qu'il ne l'avait été jugé initialement. Il a toutefois présenté ce risque comme acceptable, vu que cette possibilité permet précisément de porter une nouvelle appréciation sur les données après un certain temps, et donc de les effacer le cas échéant.

2.6 Cas en souffrance dans l'assurance qualité

A l'occasion de sa séance du 18 novembre 2008, la DélCdG s'est aussi informée des tâches et des capacités de la Section Assurance qualité. Selon la conception des processus de traitement des données dans ISIS-NT, la Section Assurance qualité, qui intervient après la saisie d'une information par la Section Analyse préliminaire (v. explications au chap. 2.3), garantit que la saisie a été effectuée dans les formes, l'opération visant avant tout à vérifier que les informations ont été représentées conformément aux structures des banques de données.

Selon les prescriptions légales, la Section Assurance qualité doit aussi veiller à ce que les informations qui ne sont pas vraiment importantes du point de vue de la protection de l'Etat ne soient pas saisies dans le système. Lors des appréciations générales périodiques, la section doit identifier les informations qui ne sont plus utiles et les effacer.

La gestion des banques de données et la formation des collaborateurs de la Section Analyse préliminaire font aussi partie des tâches de la Section Assurance qualité. Deux personnes se sont occupées des questions techniques et de la formation, notamment de la rédaction des directives régissant la saisie. Une autre s'est occupée de la banque de données HOOGAN, dans laquelle le SAP traitait les données des personnes qui ont affiché un comportement violent lors de manifestations sportives organisées en Suisse ou à l'étranger. Seulement un peu plus de la moitié des capacités de la section (3,7 sur 6,7 équivalents plein temps) ont été engagées pour l'assurance qualité proprement dite des données ISIS.

Lors d'auditions antérieures, la DélCdG a entendu à plusieurs reprises que, à la suite du passage à ISIS-NT, l'assurance qualité devait concentrer son activité sur le contrôle des communications nouvellement enregistrées. Or voici qu'on lui dit que, en raison de la forte augmentation des communications reçues, il y avait «quelques

cas en suspens» au contrôle des entrées. Si les cas en souffrance n'avaient pas été si nombreux, a précisé le chef du contrôle qualité, le contrôle aurait probablement permis d'effacer quelques enregistrements immédiatement après leur saisie.

Ces cas en suspens n'ont toutefois pas pu être chiffrés lors de l'audition. En revanche, la DélCdG a reçu pour la première fois une indication précise concernant les cas en souffrance dans le domaine des appréciations générales périodiques prescrites. L'exécution des appréciations générales a dû «être mise temporairement en veilleuse en raison du nouveau système ISIS-NT», car les capacités de la Section Assurance qualité étaient mobilisées par d'autres tâches, selon l'interlocuteur de la DélCdG, qui a précisé que la section avait enfin juste pu reprendre ses appréciations générales périodiques.

2.7 Coordination des enquêtes du DDPS et de la DélCdG

En mai 2008, le Conseil fédéral a décidé de rattacher le SAP au Département fédéral de la défense, de la protection de la population et des sports (DDPS). Par cette décision, le Conseil fédéral a anticipé une requête formulée par le conseiller national Hofmann, ancien président de la DélCdG, à travers une initiative parlementaire demandant le rattachement des services de renseignement civils à un même département.[30] Donnant suite à l'Iv. pa. Hofmann, le Parlement a adopté, le 3 octobre 2008, la loi fédérale sur le renseignement civil (LFRC)[31], qui prévoit notamment un renforcement de la surveillance départementale sur les services de renseignement.

Dans la perspective de l'intégration du SAP au DDPS, la DélCdG est intervenue auprès du Conseil fédéral pour que le transfert ne donne pas lieu à des lacunes dans la surveillance des services de renseignement. La délégation a en outre demandé une mise en œuvre rapide des prescriptions de la LFRC.

Par lettre du 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 à compter du début de 2009 et qu'ils continueraient d'exercer le contrôle du SAP. Le Conseil fédéral prévoyait en outre deux postes supplémentaires pour l'extension du contrôle au renseignement extérieur après l'entrée en vigueur de la LFRC.

Le nouvel organe de surveillance du DDPS, doté de trois personnes, a commencé son travail avec le transfert du SAP début 2009. Le traitement des données dans ISIS-NT figurait en haute priorité dans le plan de contrôle 2009 du chef du DDPS. En accord avec DélCdG, le chef du DDPS a décidé de soumettre ISIS-NT à une inspection interne. Lors de la discussion du 29 janvier 2009, il a en outre accédé à la demande de la délégation, qui proposait d'ordonner une inspection supplémentaire portant sur l'utilité d'ISIS-NT et son adéquation aux besoins des différents utilisateurs. Ce mode opératoire permettait à la DélCdG d'appuyer sa haute surveillance sur les contrôles de la surveillance départementale et d'utiliser ces résultats en temps utile dans sa propre enquête sur ISIS.

30 Iv. pa. 07.404 du 13.3.2007 «Transfert des tâches des services de renseignement civils à un département».
31 Loi fédérale du 3.10.2008 sur le renseignement civil (LFRC; RS **121**).

2.8 Questions récurrentes sur la qualité des données dans ISIS-NT (2009)

Le 19 mai 2009, la DélCdG a discuté du rapport annuel du SAP concernant le traitement des données dans ISIS-NT. Le nombre des personnes enregistrées revêtant une importance directe pour la protection de l'Etat était monté à 117 000, celui des tiers à quelque 66 000.

L'augmentation observée pour les tiers tenait au fait que le SAP avait engagé deux personnes supplémentaires au service extérieur, qui ont pu saisir dans ISIS-NT les cas en suspens découlant du contrôle des photos d'identité en 2008. Il en a résulté environ 20 000 nouveaux enregistrements de tiers, ce qui a porté le nombre des tiers enregistrés à la suite d'un contrôle des photos d'identité à la frontière à 39 000. Vu qu'une part de ces ressortissants étrangers sont entrés et sortis plusieurs fois de Suisse, environ 229 000 passages à la frontière ont été enregistrés dans ISIS-NT. Un représentant du SAP a commenté cet accroissement du nombre des tiers de la manière suivante: dès que le SAP a plus de personnel, le service produit plus. Autrement dit, le nombre des personnes enregistrées dans ISIS-NT qui revêtent potentiellement une importance pour la protection de l'Etat a gonflé avec l'effectif du personnel du SAP.

La proportion des ressortissants suisses enregistrés dans ISIS-NT était passée de 3,9 à 5 %. Le rapport expliquait cet accroissement de l'ordre de 1000 personnes par le fait que, pour beaucoup de personnes, seul le lieu d'origine avait été saisi, mais non la nationalité suisse, et que cette erreur dans les données transférées avait été identifiée et corrigée dans le cadre de la mise au net des données. Globalement, la proportion des personnes enregistrées domiciliées en Suisse était de 12,2 %.

Selon le rapport, la mise au net des données avait été achevée fin 2008. Or il est apparu dans la discussion que le SAP ne pouvait pas garantir intégralement la saisie correcte de ces données, mais qu'il estimait que les erreurs restantes pouvaient être identifiées et corrigées dans le cadre de l'activité normale de saisie de la Section Analyse préliminaire. Trois des personnes engagées temporairement pour la mise au net des données ont été entre-temps mises au service de la Section Assurance qualité, dont le personnel fixe a toutefois été réduit à 4,7 équivalents plein temps, contre 6,7 l'année précédente, selon les indications du rapport.

Le rapport laisse apparaître que les appréciations générales périodiques avaient été «temporairement suspendues» jusqu'à l'automne 2008. Le rapport n'en postulait pas moins que les données dans ISIS étaient gérées de manière uniforme selon un «standard de qualité élevé». Dans l'audition, le SAP a expliqué avoir «seulement réduit un peu le personnel» affecté aux appréciations générales périodiques, car la priorité allait à la mise au net des données et au contrôle des saisies courantes.

Depuis le premier rapport en mars 2006, le SAP avait évité de s'exprimer clairement sur la conformité légale de l'exécution des appréciations générales périodiques sous l'angle de la pertinence des personnes enregistrées pour la protection de l'Etat. Sur la base des effacements communiqués, la DélCdG savait que le SAP avait repris les contrôles à l'automne 2008, à la suite du mandat de la délégation demandant, en août 2008, au SAP de lui communiquer les enregistrements effacés selon la procédure ordinaire. Le SAP restait toutefois muet sur le nombre des appréciations périodiques qui avaient été faites dans le délai prescrit (entre fin 2004 et l'automne 2008) et si tous les contrôles en suspens avaient été faits.

Lorsque la DélCdG s'est par la suite penchée sur les échanges de courrier électronique de l'automne 2008 entre le SAP et le Centre de services informatiques du DFJP (CSI-DFJP), il est apparu que le SAP n'avait pas pu procéder à des appréciations générales jusque-là. D'après un message du 27 octobre 2008, des obstacles techniques ont empêché le déroulement correct des appréciations générales, sans lesquelles les effacements qui devaient être communiqués à la DélCdG selon son mandat du 26 août 2008 ne pouvaient pas être opérés dans le système. Le CSI-DFJP a donc été chargé de résoudre ces problèmes dans les meilleurs délais. Le chef suppléant de la division Gestion de l'information du SAP a justifié l'urgence en développant l'argumentation suivante: «La DélCdG attend déjà les premiers effacements réalisés dans le cadre de l'appréciation générale pour la fin du mois [octobre 2008]. Je serais heureux si nous pouvions leur livrer quelques résultats …»[32]. Ainsi, le SAP n'avait repris les contrôles prescrits par la loi que vers la fin de 2008, sous la pression de la DélCdG.

2.9 Analyse des effacements ISIS communiqués

2.9.1 Enseignements à tirer des effacements communiqués

Pendant la période allant d'octobre 2008 à fin décembre 2009, le SAP a communiqué à la DélCdG une partie des effacements opérés par la Section Assurance qualité dans ISIS-NT dans le cadre des appréciations générales périodiques. Comme elle l'avait spécifié dans son mandat du 26 août 2008, il s'agissait des enregistrements de personnes qui possédaient la nationalité suisse ou avaient leur domicile en Suisse. Pour chacune de ces personnes, la DélCdG a reçu un extrait intégral comprenant toutes les données enregistrées qui les concernaient.

Comme la livraison de ces données occasionnait un travail supplémentaire non négligeable pour la Section Assurance qualité – au demeurant déjà surchargée –, la DélCdG a limité la durée de son mandat à fin 2009. Les communications sont ainsi restées dans le cadre temporel fixé pour l'inspection, soit jusqu'à l'intégration du SAP dans le nouveau service du renseignement civil.

Pendant les 15 mois considérés, la Section Assurance qualité a effacé les enregistrements d'environ 450 personnes dans le cadre des appréciations générales périodiques effectuées.[33] De ce nombre, quelque 240 remontaient à la période précédant les années 2000, et environ 200 à la période comprise entre 2000 et la migration vers ISIS-NT à la fin de 2004. Seul un très petit nombre des effacements portaient sur des enregistrements postérieurs à 2004.

La DélCdG a examiné les échantillons dans la perspective de la conformité des mesures d'assurance qualité prises par le SAP pour les données ISIS avec les prescriptions de la loi et de l'ordonnance. Il s'agissait notamment des procédures suivantes: le rythme des appréciations générales périodiques d'une personne, la première devant intervenir 5 ans après la saisie de la première communication, puis tous les trois ans; l'effacement, aux termes de l'ordonnance, des enregistrements des person-

32 Courrier électronique du chef suppléant de la division Gestion de l'information du SAP au chef suppléant de la section Développement du CSI-DFJP, du 27.10.2008 (en langue allemande).

33 Près de 50 autres enregistrements ont été effacés par la Section Assurance qualité durant ce laps de temps parce que la Section Analyse préliminaire les avait saisis à tort.

nes qui figurent dans le système depuis au moins trois ans en qualité de tiers à la première appréciation générale périodique; enfin, la durée de conservation des communications dans le système, qui ne doit pas dépasser 15 ans.

Les cas examinés par la DélCdG permettent de se faire une idée de la façon dont le SAP a suivi les procédures prescrites. Ils donnent aussi des indications sur la manière dont le SAP a apprécié les informations entrantes sous l'angle matériel et du point de vue de leur importance pour la sécurité de la Suisse. Dans tous les cas communiqués, l'effacement signifie que la personne enregistrée a perdu son importance pour la sécurité de l'Etat ou qu'elle n'en a jamais revêtu. On peut d'une part se poser la question de savoir si le critère de l'importance d'une information n'a pas été apprécié de façon laxiste au moment de l'enregistrement. D'autre part, on peut aussi examiner dans quelle mesure, le cas échéant, des informations supplémentaires ont conduit à une nouvelle appréciation, notamment lorsque ces informations indiquent de manière explicite que la personne concernée ne présente pas une menace pour la sécurité de la Suisse.

2.9.2 Appréciations générales périodiques avant 2005

Toutes les personnes enregistrées avant 2000 devaient, selon les règles régissant l'assurance qualité, faire l'objet d'au moins une appréciation générale périodique avant fin 2005. Une personne enregistrée en 1996 devait par exemple être contrôlée en 2001 et en 2004.

Dans les extraits intégraux communiqués à la DélCdG, seuls un peu plus de la moitié des cas enregistrés dans ISIS avant 2000 présentent un champ indiquant un contrôle dans la période comprise entre début 2000 et fin 2004. On peut donc en déduire que, dans les autres cas, l'appréciation générale périodique n'a pas été faite comme elle le devait.

2.9.3 Appréciations générales périodiques à partir de 2005

Pour aucune des personnes dont l'enregistrement avait été effacé entre l'automne 2008 et fin 2009 la DélCdG n'a pu trouver, dans l'extrait intégral, d'indice montrant qu'elles auraient fait l'objet d'une appréciation générale périodique après la migration vers ISIS-NT. Un contrôle était pourtant prescrit entre début 2005 et l'automne 2008 tout au moins pour les cas les plus anciens, qui devaient être appréciés à un intervalle maximal de trois ans.

Par contre, on trouvait dans tous les extraits intégraux communiqués comme effacés un champ qui indiquait le 31 décembre 2004 comme date de la dernière appréciation générale périodique. Cette date contredit cependant une information du SAP de 2006, selon laquelle toutes les données ISIS avaient été transférées à la fin de 2004 sans faire l'objet d'un contrôle préalable (v. chap. 2.3).

La DélCdG a en outre noté que le champ en question ne figurait précisément pas dans un extrait requis par la délégation le 11 mars 2008 pour le contrôle concernant les deux membres du Grand Conseil du canton de Bâle-Ville. L'extrait intégral suivant concernant un de ces mêmes députés établit par le SAP avant son effacement

contenait l'information indiquant qu'un contrôle avait été effectué le 31 décembre 2004.

Il faut en conclure que le visum du contrôle de fin 2004 a dû être intégré dans les données de la personne concernée après coup dans le courant de 2008. Cette modification de date ne peut en aucun cas avoir été faite dans les règles par la Section Assurance qualité, et donne à penser que le même procédé a été appliqué aux autres cas communiqués, autrement dit que la date du 31 décembre 2004 a été saisie après coup comme jour du dernier contrôle.

Dans la période observée par la DélCdG, le SAP a procédé à 360 effacements en rythme annuel. Dans ce laps de temps, le SAP a concentré ses contrôles et les effacements sur les personnes qui correspondaient au mandat d'effacement de la DélCdG. Les ressortissants étrangers domiciliés en Suisse, qui représentaient à peu près 90 % des cas enregistrés dans ISIS, n'ont été supprimés du système que dans une faible proportion (5 % des effacements).

Les prescriptions légales prévoient une appréciation générale périodique après cinq ans, puis tous les trois ans. Il s'ensuit que la Section Assurance qualité devrait contrôler chaque année entre un cinquième et un tiers de tous les enregistrements. Avec un effectif ISIS de 116 000 personnes revêtant une importance du point de vue de la protection de l'Etat et de 66 000 tiers, cela représente entre 36 000 et 60 000 contrôles par année.

Avec 360 effacements par année, le SAP atteint au mieux un taux d'effacement annuel de 1 %. Or le SAP avait rapporté à la DélCdG en 2006 qu'il fallait compter avec l'effacement d'environ un tiers des enregistrements contrôlés dans le cadre de l'appréciation générale périodique. Selon ces chiffres, de deux choses l'une: soit le SAP n'a pas fait un nombre suffisant de contrôles, soit il les a faits de manière trop superficielle.

2.9.4 Respect de la durée maximale de conservation

ISIS ayant été mise en service en 1994, les premières communications enregistrées ont atteint leur durée maximale de conservation (15 ans) en 2009. Si l'enregistrement se fonde sur une seule communication, la personne concernée ne doit pas rester enregistrée dans ISIS après la fin de la période de conservation prescrite. Différents cas examinés par la DélCdG satisfaisaient à cette condition. Dans quelques cas, le SAP n'a pas réussi à respecter le délai de trois mois dans lequel doit intervenir l'effacement à l'échéance de la durée de conservation.

Selon les règles, les tiers peuvent rester enregistrés en tant que tels au plus tard jusqu'à la première appréciation générale, soit une durée maximale de cinq ans. Dans différents cas, l'effacement est toutefois intervenu plusieurs années, voire une décennie après l'enregistrement en tant que tiers.

2.9.5 Appréciation de la pertinence du point de vue de la protection de l'Etat

La LMSI autorise en principe uniquement le traitement des informations nécessaires à l'accomplissement de la mission de protection de l'Etat (art. 15, al. 1, LMSI).

Cette prescription implique une appréciation des informations avant leur classement dans ISIS. Dans la pratique, il peut arriver que les informations collectées se révèlent par la suite inexactes ou sans intérêt pour la sûreté de la Suisse. Dans ce cas l'appréciation générale périodique doit donner lieu à l'effacement des informations concernées, voire de l'enregistrement de la personne concernée.

Il ne fait aucun doute que l'intention du législateur veut qu'une personne ne figure plus dans ISIS après communication de son décès ou de son retrait d'un groupe extrémiste. Dans les cas communiqués par le SAP, on trouve cependant plus d'une dizaine d'exemples de personnes qui sont restées enregistrées pendant plusieurs années après que le décès avait été dûment noté dans le système. Dans trois cas, l'effacement n'est intervenu qu'une dizaine d'années après le décès. Un de ces cas est emblématique en ce que le défunt n'avait pas seulement été oublié dans ISIS, mais que deux contrôles ultérieurs ont confirmé l'importance de la personne du point de vue de la protection de l'Etat.

Dans d'autres cas, le classement d'une communication spécifiant de manière explicite qu'une personne était sortie d'un groupe extrémiste ou qu'elle n'y était plus active n'a pas entraîné l'effacement immédiat de l'enregistrement dans ISIS. Les cas examinés par la délégation donnent l'impression que, face à une nouvelle communication concernant une personne déjà enregistrée, le SAP a pour principe de saisir les informations supplémentaires sans soumettre la communication à une appréciation. Il semble au fond que l'idée était que les contrôles nécessaires seraient rattrapés à l'occasion de la prochaine appréciation générale périodique. Dans le cas d'une communication signalant la sortie d'un groupe, il a fallu attendre deux contrôles pour que le SAP reconnaisse que la personne en question ne présentait plus une menace pour la sûreté de la Suisse et qu'il efface enfin l'enregistrement, huit ans après la communication à décharge.

Un grand nombre d'enregistrements faisaient suite à des requêtes émanant de l'étranger. L'enregistrement se faisait même lorsque la requête n'était pas motivée par des informations complémentaires sur la personne et que le SAP lui-même ne pouvait pas ajouter d'informations touchant à la protection de l'Etat à l'intention du service requérant. Même lorsque les renseignements pris auprès des cantons spécifiaient explicitement que la personne ne revêtait pas d'importance pour la protection de l'Etat, les informations à décharge ont été saisies dans ISIS, cela sans appréciation de l'importance de la personne pour la sûreté de l'Etat, et donc sans possibilité d'effacement. Avec ce genre de pratique, on conçoit aisément comment une personne intègre peut acquérir de l'importance du point de vue de la protection de l'Etat par le truchement de l'échange international d'informations entre les services du renseignement.

Dans de nombreux cas, des listes de personnes établies par les cantons sur mandat du SAP ont été à l'origine d'un enregistrement dans ISIS. Par ces listes, les organes cantonaux de protection de l'Etat ont par exemple communiqué au SAP, dans le cadre d'un mandat concret, des procédés, personnes ou institutions qui présentaient un rapport plus ou moins proche – ou lointain – avec l'objet du mandat. Plusieurs exemples montrent comment toutes les personnes figurant sur une liste ont été enregistrées dans ISIS-NT sans égard aux informations détaillées disponibles. Même dans les cas où le canton fournissait des informations très fouillées et souvent très nuancées, la pratique du SAP en matière de saisie a fait que même des personnes qui étaient explicitement désignées comme inoffensives ou plus du tout actives ont fait l'objet d'un enregistrement dans ISIS-NT.

Dans plusieurs cas, la DélCdG a constaté que les personnes à l'origine d'une manifestation autorisée et pacifique ont été enregistrées comme tiers. Dans certains cas, le titulaire de l'autorisation de manifester a même été enregistré en tant que personne revêtant en propre une importance pour la protection de l'Etat, alors que les informations disponibles attestaient que la personne concernée n'était pas membre des organisations ou groupes violents repérés à la manifestation ou visant des buts politiques analogues.

Dans la plupart des cas examinés, la DélCdG a constaté que le niveau d'information n'était pas fondamentalement différent entre le moment de la saisie et de l'effacement. Soit aucune information nouvelle n'était venue s'ajouter, soit les informations nouvelles présentaient le plus souvent une faible pertinence pour l'appréciation de l'importance de la personne sous l'angle de la protection de l'Etat. Du point de vue de la DélCdG, dans de nombreux cas, le SAP aurait pu purement et simplement éviter l'enregistrement moyennant un examen plus minutieux de la première communication.

2.9.6 Le cas A. L.

En 2008, A. L. a adressé une demande d'accès au préposé fédéral à la protection des données et à la transparence (PFPDT). Du fait de la demande d'accès, le SAP a soumis les données d'A. L. à une appréciation générale (anticipée) et a effacé son enregistrement le 13 mai 2009. Le SAP a communiqué cet effacement à la DélCdG.

Il ressort des documents y relatifs que, en avril 1998, le service du renseignement d'un pays voisin de la Suisse a demandé des renseignements sur deux personnes nord-africaines qui pouvaient appartenir à des groupements islamistes extrémistes et avoir eu des contacts en Suisse. Dans les enquêtes étrangères figuraient notamment des numéros de téléphone suisses. Un de ces numéros s'est révélé être le raccordement d'A. L. et de son époux, à la suite de quoi la sûreté du canton de Bâle-Ville a reçu pour mandat de rédiger un rapport sur A. L.

Le rapport du 23 juin 1998 concluait qu'A. L. était apparue de manière récurrente comme porte-parole de groupes marginaux et que ses activités devaient immanquablement l'avoir mise en contact avec des étrangers d'origine islamique. Cela étant, le rapport précisait qu'A. L. était une personne bonne et généreuse, sans la moindre inclination criminelle. Enfin, il ajoutait qu'A. L. et son époux vivaient une union très libre: sans que cela pose la moindre difficulté, ils passaient souvent des périodes prolongées éloignés l'un de l'autre et avaient chacun leurs propres activités.

En juillet 1998, le service étranger a été informé que l'un des numéros de téléphone transmis pour éclaircissements était celui du couple L., qu'A. L. était connue pour son engagement en faveur de personnes de pays du tiers monde, ce qui pouvait expliquer un contact avec les suspects de terrorisme, et que, enfin, la Suisse ne disposait d'aucune information concernant les deux personnes nord-africaines.

Tant le rapport de la sûreté du canton de Bâle-Ville que la réponse au service étranger ont été classés dans ISIS. A cette occasion, A. L. et son mari ont été enregistrés en tant que tiers dans le système.

Le 5 septembre 2002, la sûreté du canton de Bâle-Ville a établi, sur mandat du SAP, une liste de personnes connues comme activistes dans les manifestations antimondialisation. A. L. figurait sur cette liste. Selon une note, son intégration à la liste

tenait à l'arrivée à Bâle de personnes qui voulaient se rendre au sommet du G8 à Gênes le 19 juillet 2001. Dans le contexte de cet événement, la liste contenait en outre, à la colonne «Délits violents», la mention «Dénonciation pour émeute et entrave à l'accomplissement d'un acte officiel». Comme la DélCdG l'a appris d'A. L., cette dénonciation n'a jamais été notifiée à l'intéressée et manifestement les autorités n'y ont pas donné suite. Son intégration à la liste était en outre assortie de la mention que A. L. était enregistrée dans ISIS en tant que tiers. A la suite de cela, le SAP a modifié le statut d'A. L. dans ISIS, la faisant passer de tiers à celui de personne revêtant en propre une importance du point de vue de la protection de l'Etat, précisant dans son enregistrement qu'elle était soupçonnée d'appartenir au «bloc noir».

Un simple examen superficiel aurait à lui seul dû montrer qu'A. L. n'était pas une menace pour la sûreté intérieure de la Suisse. Son arrière-plan et son âge rendaient son appartenance au bloc noir extrêmement improbable, puisque les membres dudit bloc étaient, selon la propre appréciation du SAP, en majorité de sexe masculin et avaient en moyenne 20 ans.[34]

En fait, les informations de 1998, qui déniaient à A. L. toute importance pour la protection de l'Etat, auraient dû s'opposer à l'inscription du soupçon de participation à des manifestations violentes dans son enregistrement. D'autant que des représentants du SAP ont souligné de manière réitérée qu'une appréciation correcte de la pertinence du point de vue de la protection de l'Etat requérait aussi de collecter les informations à décharge.

Comme l'ont montré les investigations de la DélCdG, le soupçon d'appartenance au bloc noir ne résultait pas d'une appréciation des informations que le SAP avait accumulées sur A. L., mais de l'application, par la Section Analyse préliminaire, des directives relatives à la saisie graduée dans ISIS des activistes inclinés à la violence, que le SAP avait adoptées le 15 juillet 2002 et qui continuaient de s'appliquer.

Les directives font une distinction entre les activistes de catégorie A, B et C en fonction du nombre de communications et de dénonciations liées à la personne, ainsi que des indications concernant des actions violentes commises par la personne en question. Le système mis ainsi en place prévoit manifestement que deux communications de la sûreté cantonale en l'espace de quatre ans et une dénonciation non vérifiée pour émeute et une entrave à l'accomplissement d'une action officielle remplissent les conditions pour classer A. L. comme activiste de catégorie B, avec pour conséquence son passage du statut de tiers à celui de personne revêtant une importance autonome du point de vue de la protection de l'Etat, l'enregistrement étant assorti de la mention «soupçon bloc noir».

Dans liste des activistes du 5 septembre 2002 figurait aussi M. H., pour qui rien de concret n'avait été cependant retenu à charge. Comme elle avait été contrôlée par la police, M. H. a été classée activiste A par le SAP et donc saisie dans ISIS comme tiers. La saisie suivante est intervenue en janvier 2005, après un nouveau contrôle de M. H. par la police au cours d'une manifestation, ce qui a entraîné, en application des directives du SAP et comme pour A. L., son enregistrement dans ISIS en tant que personne revêtant en propre une importance pour la protection de l'Etat, assorti de la mention «soupçon bloc noir». Comme dans le cas d'A. L., l'âge de M. H.

34 Rapport du Conseil fédéral du 25.08.2004 sur l'extrémisme, FF **2004** 4693 4724.

rendait pourtant ce soupçon peu plausible. L'enregistrement de M. H. a été effacé en mai 2009, après sa demande d'accès déposée auprès du PFPDT.

En septembre 2007, la sûreté du canton de Bâle-Ville a fait état d'un incendie dans le centre de détention en vue du refoulement Bässlergut. Le rapport cite un article de presse dans lequel A. L. commentait l'événement dans la perspective de son engagement pour les détenus en instance de renvoi. C'est manifestement pour cette seule raison que la communication a été reliée à A. L. lors de son enregistrement dans ISIS, alors que rien n'indiquait qu'A. L. ait quoi que ce soit à voir avec l'incendie.

Dans les dossiers, rien n'indique que l'appréciation générale – prescrite par la loi – de l'enregistrement d'A. L. ait jamais été faite avant la demande d'accès. Le premier contrôle aurait dû intervenir au plus tard en juin 2003, le deuxième en juin 2006. L'enregistrement de M. H. n'a pas non plus été contrôlé conformément aux prescriptions de l'ordonnance.

Enfin, il convient de relever que, lorsque la DélCdG s'est renseignée sur la dangerosité d'A. L. à l'occasion de sa visite dans le canton de Bâle-Ville, la réponse fut qu'elle ne revêtait aucune importance pour la protection de l'Etat.

L'enregistrement du mari d'A. L. comme tiers a aussi été effacé en mai 2009, selon toute vraisemblance à la suite de sa demande d'accès. Il était resté enregistré dans ISIS durant onze ans, soit plus du double du temps légalement autorisé.

Le 5 juin 2009, le SAP a adressé une lettre à A. L. afin de la renseigner ultérieurement conformément à l'art. 18, al. 6, LMSI. Aux termes de cette disposition, les personnes enregistrées ayant déposé une demande de renseignements seront renseignées au plus tard à l'expiration de l'obligation de conserver les données, conformément à la loi fédérale sur la protection des données (LPD)[35], dès lors que les intérêts liés au maintien de la sûreté intérieure n'exigent plus le secret (v. chap. 4.2). Le SAP s'est toutefois contenté de rendre compte des données ISIS d'A. L. de manière abrégée, au lieu de lui fournir des renseignements complets, comme l'exige la LPD.

Le 30 juin 2009, A. L. et M. H. se sont adressées à la DélCdG pour obtenir un droit d'accès sans restriction aux dossiers que la protection de l'Etat avait constitués sur leurs personnes. Le 15 juin 2009, le président de la DélCdG leur a répondu que la délégation n'avait pas compétence pour fournir directement des informations aux personnes concernées, mais qu'elle allait en revanche examiner, à l'occasion de son inspection, la manière dont les données d'A. L. et M. H. ont été traitées dans ISIS. La DélCdG a sollicité et obtenu l'accord d'A. L. et de M. H pour la publication des présentes constatations.

Comme le SAP a donné des renseignements incomplets selon l'art. 8 LPD, la DélCdG estime qu'A. L. et M. H peuvent exiger du SRC, qui a repris les tâches du SAP le 1er janvier 2010, une décision formelle au sens de l'art. 5 de la loi fédérale sur la procédure administrative (PA)[36] en relation avec l'art. 25 LPD. Les personnes concernées peuvent recourir auprès du Tribunal administratif fédéral (TAF) contre cette décision.

35 Loi fédérale du 19.6.1992 sur la protection des données (LPD; RS **235.1**)
36 Loi fédérale du 20.12.1968 sur la procédure administrative (PA; RS **172.021**)

2.9.7 Cas de trafic nucléaire

Vers le milieu des années 90, le Ministère public de la Confédération a ouvert des enquêtes pour contravention à loi sur l'énergie atomique dans deux affaires distinctes. Les actes de procédure ont été saisis dans ISIS. Les deux personnes concernées sont décédées en 1998. Les enregistrements ont été effacés respectivement à la fin de 2008 et au milieu de 2009, soit plus de dix ans après le décès des personnes concernées.

Dans le premier cas, le prévenu avait remis un récipient contenant une substance radioactive à un partenaire commercial. Il avait ensuite exigé de cette personne, au moyen d'une fausse lettre de menace d'un groupe extrémiste étranger, de renoncer à toute prétention financière à son égard. Les investigations ont montré que la radioactivité du matériau était trop faible pour causer des atteintes à la santé. Le prévenu, qui avait alors plus de 70 ans, avait été condamné à une amende et une peine d'emprisonnement avec sursis. Il n'y avait toutefois pas de quoi fonder sérieusement une menace pour la sûreté de l'Etat en rapport avec la prolifération nucléaire ou le terrorisme.

Les documents du dossier ont tous été classés dans ISIS, y compris un certificat interne du SAP du 29 mai 2002, indiquant que les documents étaient «encore nécessaires à des fins de prévention policière». Ce contrôle avait été fait lors de la répartition des dossiers de la police fédérale entre les deux unités nouvellement créées, soit la Police judiciaire fédérale (PJF) et le SAP. L'appréciation générale suivante, intervenue le 11 mars 2003, avait confirmé l'importance de la personne concernée pour la protection de l'Etat, cela environ cinq ans après son décès.

L'autre cas, qui remonte à septembre 1993, avait fait plus de bruit: le Ministère public de la Confédération avait ouvert une enquête judiciaire contre une personne qui avait déposé environ 13 kg d'uranium faiblement radioactif sur l'aire autoroutière de Kemptthal, tout en alertant la police cantonale zurichoise de manière anonyme. Auparavant, la personne avait demandé conseil au sous-chef d'état-major du renseignement et mis au point avec lui le mode opératoire.[37]

Les documents y relatifs du Ministère public de la Confédération ont été saisis dans ISIS à des fins de protection de l'Etat. Lorsque, en 1998, la personne décéda, un rapport a été enregistré dans ISIS sur la cause de la mort. Le SAP a ensuite saisi d'autres rapports de différentes sources publiques sur les relations de la personne avec le régime d'apartheid de l'Afrique du Sud. Un de ces rapports mentionnait même les contacts de l'ancien sous-chef d'état-major du renseignement avec l'Afrique du Sud, ce qui a entraîné son enregistrement dans ISIS en qualité de tiers.

2.9.8 Liste d'extrémistes de droite

En septembre 2000, la sûreté d'un canton de Suisse orientale a remis au SAP un rapport sur l'extrémisme de droite à l'échelle locale. Seize personnes y figuraient, qui s'étaient signalées d'une manière ou d'une autre en relation avec des activités d'extrême-droite. L'éventail allait du meneur établi qui entretenait des contacts intensifs avec d'autres personnalités de même obédience dans d'autres cantons, à la

37 Rapport de la DélCdG du 12 novembre 1999: Le rôle des Services de renseignements suisses dans le cadre des relations entre la Suisse et l'Afrique du Sud (FF **2000** 505 524).

personne qui, lors d'une arrestation pour conduite en état d'ébriété, avait entonné des chants d'extrême droite et vilipendé les étrangers. Une autre personne ne s'était plus signalée depuis un contrôle d'identité remontant à 1993, toujours selon le rapport.

Le SAP a enregistré dans ISIS toutes les personnes mentionnées dans le rapport, cela quand bien même le rapport concluait clairement dans son appréciation générale qu'il n'y avait plus de scène locale de skinheads et qu'une aggravation de la situation n'était pas en vue. A la fin de 2008, le SAP a effacé les enregistrements de la moitié des personnes mentionnées dans le rapport. Aucune information nouvelle n'était venue s'ajouter pour quiconque au fil des années, et l'appréciation générale périodique prescrite en 2005 n'a pas été faite.

2.9.9 Associations islamiques

En mai 2000, le service de protection de l'Etat d'un canton romand a établi un rapport concernant un centre islamique implanté sur son territoire. Les membres dirigeants du centre cités dans le rapport ont été saisis dans ISIS en tant que tiers. Dans un rapport d'ensemble sur les institutions islamiques réalisé en novembre 2004 sur mandat du SAP, une des personnes est citée à nouveau, étant précisé qu'il ressort clairement du rapport que rien ne pouvait être retenu contre elle. En 2007, la personne figure dans un nouveau rapport adressé au SAP. Le document analysait le courant religieux auquel appartenait le centre en question et concluait qu'aucun des fidèles de ce groupe religieux n'était connu pour des activités extrémistes. Cette information avait aussi été saisie par le SAP. L'enregistrement de cette personne a été effacé en novembre 2009.

Dans un autre cas remontant à mars 2004, la sûreté cantonale surveillait la réunion d'une organisation qui figurait sur la liste d'observation. Dans ce contexte, les véhicules garés dans la zone de la réunion, où se trouvaient une mosquée et un centre islamique, ont été contrôlés. Ont été communiqués au SAP les détenteurs des véhicules qui, selon le rapport du canton, étaient garés à proximité du lieu de la réunion et pouvaient correspondre au profil des participants. Pour l'une des personnes, qui avait été enregistrée en tant que tiers, le canton a transmis une nouvelle communication en février 2006. La personne était cette fois décrite comme un membre du comité d'une association islamique, le rapport précisant que les représentants du comité étaient connus comme personnalités respectables et ne pouvaient être mis en relation avec un mouvement extrémiste. La personne est néanmoins restée dans ISIS et son enregistrement n'a été effacé qu'en août 2009.

2.9.10 Contrôle des photos d'identité

Dans le cadre de ce programme de recherches préventif fondé sur le contrôle des photos d'identité, les titulaires d'un passeport d'un certain nombre d'Etats font l'objet d'un enregistrement lors de leur passage par certains postes frontière.

Les paragraphes qui suivent décrivent le cas du ressortissant d'un Etat nord-africain qui, en 2000, a été enregistré dans ISIS à la suite de l'un de ces contrôles[38]. D'autres entrées du même type ont suivi dans les années 2001 et 2002. Par la suite, la personne concernée, domiciliée en Suisse et mariée à une ressortissante suisse, a déposé une demande de naturalisation. Comme il ressort de l'avis saisi dans ISIS en septembre 2003, le SAP n'avait aucune objection à formuler.

Selon les informations saisies dans ISIS, la personne a fait l'objet d'une appréciation par la Section Assurance qualité et a été naturalisée. Néanmoins, elle est restée enregistrée jusqu'en mars 2009, et ce non comme tiers, comme l'enregistrement initial à la suite d'un contrôle de photo d'identité l'aurait laissé supposer, mais comme personne revêtant en propre une importance pour la protection de l'Etat.

Un autre étranger domicilié dans un canton limitrophe gérait une affaire commerciale juste de l'autre côté de la frontière. Son enregistrement dans ISIS a aussi fait suite à un contrôle de photo d'identité. Trois passages de frontière présumés conduire dans le pays d'origine en Afrique du Nord ont été enregistrés dans ISIS entre août 1998 et août 1999, alors que les trajets quotidiens de la personne concernée à l'occasion desquels elle traversait la frontière pour se rendre à son travail n'ont fait l'objet d'aucune surveillance.

2.9.11 Contacts avec l'entourage de «Carlos»

En 1995, les services de protection de l'Etat ont systématiquement interrogé les ressortissants suisses ayant eu des contacts avec des personnes sur lesquelles le Ministère public de la Confédération enquêtait en raison d'un soutien présumé à I. R. Sanchez («Carlos»), terroriste internationalement recherché. Plusieurs des personnes interrogées ont été saisies dans ISIS comme personnes revêtant une importance du point de vue de la protection de l'Etat.

Le Ministère public de la Confédération a suspendu sa procédure relative au cas «Carlos» le 20 juin 2000 pour absence de preuves.[39] Néanmoins, quatre des personnes interrogées n'ont pas été effacées d'ISIS à l'occasion de l'appréciation générale périodique de décembre 2001. Le contrôle prescrit en 2004 n'a manifestement pas eu lieu. Il a fallu attendre février 2009 pour que la Section Assurance qualité du SAP efface les quatre enregistrements.

2.10 Résultats des contrôles effectués au titre de la surveillance du DDPS (2010)

Après le transfert de l'obligation de surveillance du SAP au DDPS au début de 2009, le chef du DDPS a ordonné deux enquêtes internes sur ISIS-NT (v. chap. 2.7). Les inspections ont été assurées par la nouvelle surveillance des services de renseigne-

38 Du point de vue de la DélCdG, l'enregistrement d'une personne du seul fait qu'elle a été l'objet d'un contrôle de photo d'identité est contraire aux dispositions de la LMSI et de son ordonnance d'exécution (v. chap. 6.3).

39 Communiqué de presse du 21.6.2000 de la police fédérale et du Ministère public de la Confédération: Attentats terroristes commis sous la direction de «Carlos» au début des années 80: enquêtes de police judiciaire suspendues.

ment du DDPS (Surveillance SR), qui a repris la mission de surveillance du SAP de l'inspectorat du DFJP au début de 2009.

Le 24 mars 2010, la Surveillance SR a présenté à la DélCdG les résultats de ses inspections concernant la légalité et l'utilité d'ISIS. Le rapport d'inspection du 22 février 2010 sur la légalité du traitement des données dans ISIS-NT montre que les incohérences dans l'assurance qualité, que la DélCdG avait relevées dans son travail d'analyse des effacements ISIS qui lui avaient été communiqués, n'étaient que la pointe de l'iceberg. Finalement, le rapport de la Surveillance SR est arrivé à la conclusion que, sur des points essentiels, la gestion de la banque de données Protection de l'Etat d'ISIS-NT ne satisfaisait pas aux dispositions de la LMSI.[40]. Comme la Section Assurance qualité n'était pas à même d'assumer sa mission en temps utile et ne parvenait pas à rattraper son retard dans le traitement des affaires, il n'était pas possible d'assurer une qualité des données satisfaisant aux prescriptions légales, précise le rapport.

Selon le rapport, ISIS contenait environ 16 000 communications qui n'avaient pas encore été contrôlées depuis leur saisie. L'appréciation générale périodique prescrite était pendante pour 76 000 personnes enregistrées dans l'ancien système ISIS, soit avant 2005. Le retard dans les appréciations générales périodiques pour la période ultérieure à la migration vers ISIS-NT concernait 40 000 personnes supplémentaires, comme le montre le deuxième rapport d'inspection.[41]

L'enquête révèle que la date de la dernière appréciation générale a été fixée après coup au 31.12.2004 pour toutes les personnes dont les données avaient été transférées vers ISIS-NT. Comme la Surveillance SR l'a découvert, cette appréciation n'avait en fait jamais été faite. Ce fait est venu confirmer le soupçon de la DélCdG: la modification inexplicable intervenue dans les données d'un député au Grand Conseil du canton de Bâle-Ville (v. chap. 2.9.3) avait été appliquée en automne 2008 à toutes les personnes reprises dans ISIS-NT.

Le rapport constate en outre que le contrôle initial consécutif à la saisie des données n'intervenait dans la pratique que par sondage. Pour assurer un contrôle intégral, il aurait fallu que la Section Assurance qualité puisse suivre sans défaut le travail de la Section Analyse préliminaire, ce que la Surveillance SR a jugé totalement impossible compte tenu de l'effectif du personnel. Comme il ressort d'une notice explicative interne, la Section Assurance qualité se concentrait essentiellement sur les aspects formels lors du contrôle initial. Bien qu'il soit prescrit légalement, l'examen de la légalité des informations saisies n'était manifestement pas une préoccupation prioritaire de l'activité de contrôle.

Le rapport de la Surveillance SR critique aussi la pratique adoptée par le SAP, qui consistait à faire passer les tiers dans la catégorie des personnes revêtant une importance pour la protection de l'Etat lorsqu'ils étaient mentionnés dans plus de deux communications. De l'avis de la Surveillance SR, cette pratique est arbitraire et ne correspond ni au sens et ni à l'esprit de la LMSI, car un soupçon de menace pour l'Etat quasi automatique fondé sur une règle purement mathématique n'est pas à même de remplacer une appréciation matérielle. Si une institution est citée trois fois

40 Rapport d'inspection de la Surveillance RS du DDPS du 22.2.2010 sur l'examen de légalité du traitement des données dans le système ISIS-NT Protection de l'Etat du SAP, p. 31 du texte allemand (non traduit).

41 Rapport d'inspection de la Surveillance RS du DDPS sur l'analyse de l'application du système de données ISIS, du 23.9.2009, p. 54 du texte allemand (non traduit).

dans différents contextes (pour préciser que différentes personnes y travaillent, p. ex.), elle devient automatiquement pertinente pour la sûreté de l'Etat. Cette pratique explique aussi l'augmentation inflationniste des institutions qui font l'objet d'un enregistrement (plus de 10 000), alors que le rapport fait état de 77 organisations sur la liste d'observation.

Selon le rapport, les entorses aux prescriptions légales applicables à ISIS-NT tiennent en grande partie au fait que, au cours du projet, les exigences légales n'ont jamais été analysées sous l'angle d'une exécution correcte dans le système ISIS-NT lui-même et dans son organisation et ses procédures. Les besoins en ressources, tant quantitatifs que qualitatifs, nécessaires à un traitement des données en temps utile et conforme aux exigences légales n'ont notamment jamais été identifiés. Le rapport précise que la proposition au Conseil fédéral concernant la modification de l'ordonnance ISIS du 30 juin 2004 mentionne certes la charge supplémentaire de travail découlant pour la Section Assurance qualité de l'introduction du nouveau système ISIS-NT, mais précise que les postes supplémentaires nécessaires n'ont jamais été arrêtés.[42]

Le rapport souligne que les directives régissant le travail de traitement de la Section Analyse préliminaire n'ont été adaptées aux nouvelles conditions qu'en 2008, soit trois ans après l'introduction d'ISIS-NT. Aucune formation aux prescriptions légales pour les collaborateurs de la Section Assurance qualité n'a été faite dans le cadre du projet. Une sensibilisation aux limites de l'art. 3 LMSI n'est intervenue qu'à la suite de la requête de la CdG-BS à la DélCdG. De plus, les utilisateurs des informations ISIS ne connaissent pas assez bien les critères et la grille utilisés par les sections Analyse préliminaire et Assurance qualité pour apprécier les informations, comme l'a révélé un sondage auprès des collaborateurs de la Section Analyse et de l'organe de pilotage (Steuerungsstelle). Les chefs de domaine de l'organe de pilotage attribuent les mandats de collecte d'informations et doivent pouvoir apprécier leur légalité.

La Surveillance SR contredit dans son rapport la déclaration générale du SAP selon laquelle ISIS n'est pas «un répertoire de suspects, mais une banque de données visant à documenter l'activité déployée par le SAP pour la protection de l'Etat». Le SAP avait utilisé la même expression face à la DélCdG et, selon le rapport de la Surveillance SR, aussi dans le cadre d'une séance d'information publique sur ISIS le 23 octobre 2009.

Si la banque de données Administration ISIS02 et la banque de données ISIS06, dans laquelle sont enregistrées les personnes qui ont fait l'objet d'un contrôle de sécurité servent bien un pur objectif administratif, la généralisation de la déclaration du SAP à la banque de données Protection de l'Etat ISIS01 minimise les faits, relativise les carences des contrôles de qualité et suggère qu'en fin de compte tout un chacun pourrait figurer dans la banque de données. Le rapport souligne au contraire que la banque ISIS01 est un répertoire de suspects, et qu'il faut en conséquence y enregistrer uniquement les personnes et les institutions qui sont concrètement soupçonnées de déployer des activités qui menacent la sûreté de l'Etat.

42 Sur proposition du Conseil fédéral du 16.6.2004, le DFJP s'est contenté de constater que davantage de ressources en personnel étaient nécessaires pour la saisie et le traitement des données dans ISIS-NT. Le besoin supplémentaire, qui n'était pas encore chiffrable, serait compensé au sein du département.

Le rapport de la Surveillance SR a aussi analysé le degré de réalisation des objectifs initiaux du projet ISIS-NT. La conception de 2003 prévoyait une saisie préalable dans le système d'information électronique et, sur cette base mais dans une procédure totalement distincte, le traitement opérationnel de l'information. Selon cette conception, la saisie électronique immédiate de toutes les communications arrivant au SAP devait permettre aux utilisateurs de la Confédération et des cantons d'accéder sans délai et en tout lieu à l'ensemble des documents du SAP.

Comme l'a constaté la Surveillance SR, le projet initial, qui prévoyait des processus électroniques pour l'intégralité des flux de travail, a dû être abandonné. La procédure électronique d'attribution des mandats a certes été introduite à l'interne, mais les formulaires papier ont été conservés parce que le système n'était pas à même de prendre en charge les exigences initiales. L'interface électronique prévue pour les contacts avec les cantons n'ayant pas encore été réalisée, les mandats aux cantons se faisaient toujours sur papier dans toute la Suisse.

La Surveillance SR a constaté un retard important dans la réalisation du module des Archives fédérales suisses (AFS), qui devait permettre le transfert électronique des données effacées aux AFS. Selon la Surveillance SR, les données effacées s'accumulent aujourd'hui dans une «corbeille», à laquelle les agents auparavant autorisés n'ont plus accès, mais dont les droits d'accès sont toujours gérés par le SAP. En fin de compte, selon le rapport, le but d'ISIS-NT, qui était d'assurer une gestion électronique des données systématique et contrôlée sur l'ensemble du cycle de vie des données relatives à la protection de l'Etat, n'a pas été atteint.

Le 24 mars 2009, la DélCdG a assisté à une présentation du rapport de l'autre inspection, qui se penchait sur l'utilité et l'efficacité d'ISIS-NT. Le document contient une analyse statistique des protocoles d'utilisation d'ISIS faite par le CSI-DFJP et fournit des informations quantitatives sur le comportement des utilisateurs d'ISIS-NT.

Il ressort de ces chiffres que, comparativement au SAP, les cantons utilisent très peu ISIS-NT.[43] Au sein du SAP lui-même, la Section Analyse préliminaire compte presque huit fois plus d'accès à ISIS-NT que les unités qui utilisent le système à des fins de renseignement.

Selon le rapport, une partie des accès de la Section Analyse préliminaire sert aussi à d'autres utilisateurs d'ISIS qui, au sein du SAP, recherchent des informations dans le système et les font imprimer. Le fait que des informations ISIS soient conservées sur papier par des collaborateurs du SAP pour la réalisation de leur travail opérationnel est toutefois jugé problématique par le rapport. Sous cette forme, ces données sont retirées du cycle des appréciations générales périodiques, mais peuvent encore être utilisées au sein du SAP après leur effacement dans ISIS-NT.

43 Les accès à ISIS se répartissent de la façon suivante: 67,3 % pour le SAP, 2,0 % pour les organes de protection de l'Etat des cantons et 30,6 % pour le Service spécialisé du DDPS chargé des contrôles de sécurité relatifs aux personnes, lequel ne peut opérer que des consultations ponctuelles pour déterminer si une personne figure ou non dans ISIS.

2.11 Investigations auprès du CSI-DFJP

Le 24 mars 2010, la DélCdG a conduit une audition avec le CSI-DFJP, qui était responsable de la mise au point et de l'exploitation technique d'ISIS-NT. La DélCdG a interrogé le responsable du projet informatique sur certains aspects techniques en rapport avec le passage à ISIS-NT. La délégation a en outre demandé des tirages d'une partie des échanges de courrier électronique entre le SAP et le CSI-DFJP.

La délégation a découvert que certaines données de l'ancien système ISIS n'avaient pas été représentées correctement dans la structure d'ISIS-NT au moment de la migration. Suite à une erreur, certaines informations concernant les contrôles effectués par la Section Assurance qualité ont été perdues, et d'autres informations ont été copiées dans le mauvais champ de données. Le problème a été discuté pour la première fois en février 2006 entre le SAP et le CSI-DFJP. Dans la mesure du possible, les données enregistrées dans le mauvais champ ont été copiées dans le bon.

A l'automne 2008, le SAP a décidé d'enregistrer la date de la migration comme date de la dernière appréciation générale périodique pour toutes les personnes dont les données ont été transférées à la fin de 2004. Le 22 octobre 2008, agissant sur mandat du SAP, le CSI-DFJP a ensuite fixé la date de la dernière appréciation générale périodique au 31 décembre 2004 pour près de 90 000 personnes et tiers enregistrés dans ISIS-NT.[44] Il a du même coup attribué le chiffre 1 comme statut d'appréciation, ce qui signifiait qu'une appréciation générale avait été effectuée pour toutes ces personnes.

En réalité, les contrôles visés à l'occasion de la migration dans ISIS n'avaient jamais eu lieu. Exemple emblématique: si l'on en croyait les informations ISIS concernant un membre du Grand Conseil de Bâle-Ville après la mutation, le SAP avait déjà effectué un contrôle périodique, alors que le député n'avait en réalité même pas fait l'objet du contrôle initial après son enregistrement en octobre 2004.

Le SAP a par la suite décrit dans son rapport du 27 avril 2009 à l'intention de la DélCdG les mutations opérées: en substance, avant la reprise des appréciations générales périodiques, le centre de calcul du DFJP devait procéder aux adaptations nécessaires dans ISIS (uniformisation du statut des contrôles)[45]. Ce faisant, le SAP a toutefois omis de préciser que ce traitement uniformisé entraînait des enregistrements matériellement erronés dans deux champs de données pour des milliers de personnes enregistrées dans ISIS.

Le SAP estimait cependant que le fait de saisir une date incorrecte et d'accorder un visum à une appréciation générale qui n'avait jamais eu lieu n'était en soi pas problématique, vu qu'un utilisateur chevronné d'ISIS-NT, en s'appuyant sur deux autres champs, était à même de déceler que la date du 31 décembre 2004 se rapportait à un contrôle fictif. Or, premièrement, le système ne signale ainsi aucun collaborateur comme responsable de (la non-exécution de) l'appréciation générale, mais inscrit dans le champ un identifiant imaginaire; deuxièmement, le contenu d'un autre champ indique que la mutation n'a pas été faite manuellement par le SAP, mais selon une procédure automatique par le CSI-DFJP.

44 Courrier électronique du 22.10.2008 du chef du projet informatique au chef de la gestion de l'information du SAP (en langue allemande).

45 Rapport du SAP du 27.4.2009 sur le traitement des données dans ISIS-NT, p. 2 du texte allemand (non traduit).

Le SAP a justifié la mutation en bloc par le fait que les procédures programmées dans ISIS-NT pour le calcul de la date de la prochaine appréciation générale périodique n'avaient pas donné les résultats escomptés pour les données transférées dans ISIS-NT. La disposition régissant le calcul était l'art. 16, al. 1, de l'ordonnance ISIS[46], qui prévoit une appréciation générale au plus tard cinq ans après la saisie de la première communication, et trois ans après la dernière appréciation générale.

A l'origine, le système calculait la date des contrôles en se fondant sur celle de l'enregistrement d'une personne. La première appréciation générale devait être faite dans les cinq ans, puis les deux contrôles suivants respectivement après huit et onze ans. Le cas échéant, les contrôles ultérieurs devaient suivre à un intervalle de trois ans.

Cette méthode de calcul a toutefois donné lieu à des problèmes lorsque les délais prescrits par l'ordonnance ne pouvaient pas être tenus. Lorsque, par exemple, les données d'une personne avaient fait l'objet d'une appréciation générale périodique en 2004, l'appréciation suivante devait avoir lieu en 2007. Si, en raison des retards accumulés, la Section Assurance qualité ne pouvait pas faire l'appréciation avant 2009 par exemple, la procédure automatisée du système fixait déjà la prochaine échéance en 2010. Ce n'était manifestement pas le but recherché, mais la procédure prévue par l'ordonnance n'était pas non plus conçue pour ne pas être respectée.

Comme la DélCdG l'a découvert dans l'échange de courriers électroniques entre les deux organes, le SAP avait mandaté le CSI-DFJP en novembre 2008 pour modifier dans ISIS-NT le mécanisme qui calculait la date de la prochaine appréciation générale périodique. Ainsi, la date des contrôles ultérieurs ne devait plus être calculée à partir de la date de l'enregistrement de la personne concernée, mais en fonction de celle de la dernière appréciation générale périodique en date.

Comme l'ancienne procédure fondait la date de l'appréciation générale sur celle de l'enregistrement, le système n'était pas tributaire des informations concernant le moment du contrôle précédent. Par contre, la nouvelle procédure exigeait que soit saisie la date du dernier contrôle. En fixant la dernière appréciation au 31 décembre 2004, la mutation a permis de créer une nouvelle base – fictive – pour le calcul des délais.

Avec le mode de calcul original, la date de la prochaine appréciation restait toujours dans les délais prévus par l'ordonnance. Or la nouvelle formule de calcul exigée par le SAP ne livrait des résultats corrects que dans la mesure où le contrôle précédent avait été fait dans les délais prescrits. A contrario, lorsque le contrôle précédent n'était pas fait dans les délais, la nouvelle formule calculait automatiquement pour la prochaine appréciation générale périodique une date répercutant le retard. Dans le contexte des «retards chroniques de l'assurance qualité pour les contrôles périodiques»[47], la proposition du SAP faisait que, pour des dizaines de milliers de personnes, le non-respect d'un délai de contrôle entraînait ipso facto le non-respect du délai du contrôle suivant.

46 Le 1.1.2010 le Conseil fédéral a abrogé l'ordonnance ISIS du 30.11.2001. Les dispositions de l'art. 16 de l'ordonnance ISIS ont été reprises à l'art. 32 de l'ordonnance du 4.12.2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC; RS **121.2**).

47 Courier électronique du 19.11.2008 du chef de la division Gestion de l'information du SAP au chef du projet informatique (en langue allemande).

Lorsque le CSI-DFJP a émis des réserves vis-à-vis du SAP concernant la légalité des mode de calcul proposé et exigé une confirmation écrite attestant que le mandat de programmation ne serait pas contraire aux prescriptions légales, la réaction du SAP oscilla entre irritation et indignation. Le SAP a déclaré au CSI-DFJP que les modifications souhaitées avaient pour seul objectif «de représenter dans ISIS le mode de calcul explicitement prévu par l'ordonnance»[48], et que le mandat ne dissimulait aucunement les cas en suspens au niveau de l'assurance qualité car, prétendait-il, ces affaires en souffrance étaient connues de la DélCdG. Le SAP ajoutait que si le CSI-DFJP devait persister à recevoir une confirmation écrite de la légalité du mandat, le chef de la division Gestion de l'information du SAP «exigerait préalablement une requête écrite exposant les motifs d'un tel acte de défiance»[49].

L'interprétation au pied de la lettre de l'ordonnance ISIS invoquée par le SAP impliquait toutefois que des intervalles de temps non conformes à l'ordonnance entre les contrôles qualité périodiques étaient admis. Comme le SAP campait sur sa position, le CSI-DFJP a procédé aux travaux de programmation demandés. A l'audition du 19 mai 2009, le SAP a parlé d'un «problème technique» qui aurait entraîné des «erreurs de calcul dans les durées» et a assuré la DélCdG que le problème avait été résolu entre-temps. Rétrospectivement, force est de constater que l'affirmation du SAP était doublement fausse: avant les modifications, les dates des contrôles étaient calculées correctement; comme les délais n'avaient pas pu être respectés, la modification permettait de prolonger les nouveaux délais en contrevenant à l'ordonnance.

3 Protection de l'Etat dans les cantons

3.1 Surveillance de la DélCdG

Les cantons exécutent la LMSI suivant les directives de la Confédération, par exemple sur la base de la liste d'observation approuvée par le Conseil fédéral (art. 11, al. 2, LMSI) ou de mandats directs du SAP. Les informations que les cantons se procurent en s'appuyant sur la LMSI sont des données de la Confédération. La Confédération indemnise partiellement les cantons pour leur travail; en 2009, elle a notamment versé un total de 8,4 millions de francs pour les 84 équivalents plein temps dans les organes de sûreté des cantons.[50]

La haute surveillance de la DélCdG sur la protection de l'Etat s'étend ainsi à l'exécution de la LMSI par les cantons. En dehors de son enquête sur ISIS, la DélCdG s'est penchée pendant la législature en cours sur la collaboration entre la Confédération et les cantons dans deux affaires distinctes et a interrogé des employés cantonaux.[51] Pour l'inspection relative à ISIS, la DélCdG avait déjà décidé en 2008 de faire une visite aux services de la sûreté de Bâle-Ville et d'autres cantons.

48 Courier électronique du 19.11.2008 du chef de la division Gestion de l'information du SAP au chef du projet informatique (en langue allemande).
49 Courier électronique du 19.11.2008 du chef de la division Gestion de l'information du SAP au chef du projet informatique (en langue allemande).
50 Rapport du Conseil fédéral sur sa gestion en 2009 du 17.2.2010, volume I, p. 107.
51 Les investigations de la DélCdG portaient sur le travail de la sûreté pendant la phase préparatoire de la manifestation du 6.10.2007 à Berne et la tentative de recrutement d'un informateur.

Par ses visites dans les cantons, la DélCdG visait à comprendre le processus de traitement des données au niveau cantonal. La délégation voulait en outre établir par quelles interfaces les informations des cantons étaient versées dans ISIS et comment elles étaient ensuite utilisées par les cantons.

La DélCdG avait aussi l'intention d'en savoir plus sur la surveillance exercée par les autorités cantonales sur leurs services de sûreté. Elle a appris à cette occasion que les membres compétents de l'exécutif cantonal n'avaient encore jamais jeté un œil sur le travail de leurs organes de protection de l'Etat jusqu'à sa visite.

3.2 Visite de la DélCdG dans le canton de Bâle-Ville

Le 30 janvier 2009, la DélCdG a fait une visite au ministère public du canton de Bâle-Ville, qui est responsable des organes cantonaux de protection de l'Etat. Le conseiller d'Etat en charge du Département cantonal de la justice et de la sécurité s'est aussi mis à disposition pour tout renseignement. Avant la réorganisation de l'administration du 1er janvier 2009, le ministère public était rattaché au Département cantonal de la justice.

Comme la police cantonale, le ministère public du canton de Bâle-Ville fait partie du Département cantonal de la justice et de la sécurité, mais n'y est subordonné qu'administrativement. Au sein du ministère public, la protection de l'Etat (Unité spécialisée 9) est rattachée au commissariat de la police judiciaire. Elle est toutefois séparée des autres unités spécialisées du commissariat et directement subordonnée au commissaire en chef de la police judiciaire, qui est aussi procureur général.

A l'occasion de sa visite, la DélCdG a été informée que, le 18 décembre 2008, le Grand Conseil avait réduit à une très courte majorité le budget de l'Unité spéciale 9 d'un tiers, ce qui menaçait le service de la suppression de deux postes. Le directeur de la justice et de la sécurité a déclaré à la DélCdG son intention de retourner devant le Grand Conseil pour mettre en lumière les déficits sécuritaires qui iraient de pair avec cette coupe budgétaire[52], avec pour objectif de convaincre le Parlement de faire machine arrière et d'annuler la réduction budgétaire.[53]

Le canton de Bâle-Ville ne dispose pas de loi sur la protection de l'Etat. Les services du canton n'assument par conséquent pas de mission cantonale de protection de l'Etat. La base légale du travail de l'Unité spéciale 9 est la LMSI, qui définit du même coup le contenu de la mission de la sûreté cantonale. Au SAP incombe ainsi la tâche de direction.

La liste d'observation (art. 11, al. 2, LMSI) sert de mandat cadre général à l'intention des services cantonaux de protection de l'Etat. Ceux-ci livrent spontanément au SAP les informations qu'ils jugent pertinentes sur les organisations et groupes de la liste. Comme cela a été expliqué à la DélCdG, près de 40 % de ces organisations déploient des activités dans le canton de Bâle-Ville, d'où un manque patent de ressources pour assurer l'observation systématique de tous ces groupes.

52 Communiqué de presse du 13.3.2009 du Département de la justice et de la sécurité du canton de Bâle-Ville: «Sûreté cantonale: une coupe budgétaire entraîne un déficit sécuritaire».

53 Le 10.3.2009, le Conseil d'Etat a décidé de soumettre un crédit supplémentaire au Grand Conseil pour annuler la réduction budgétaire. Le Grand Conseil a approuvé le crédit supplémentaire le 14.10.2009.

Le SAP confie en outre des mandats spécifiques, mais pas en très grand nombre. Un mandat de ce type est parvenu à la sûreté cantonale après que, en octobre 2004, plusieurs candidates et candidats d'origine turque ou kurde ont été élus au Grand Conseil du canton de Bâle-Ville. Un journal qui, selon le SAP, était proche du Parti des travailleurs du Kurdistan (PKK, Partiya Karkerên Kurdistan) et des organisations qui lui ont succédé, a célébré l'élection comme un succès pour la cause kurde. L'article a amené le SAP à requérir de l'Unité spéciale 9 un rapport sur les personnes mentionnées dans l'article. La sûreté du canton de Bâle-Ville a présenté une synthèse des informations dont elle disposait sur ces personnes dans un rapport daté du 11 novembre 2004.

Un autre mandat est confié annuellement à tous les cantons dans le cadre des directives du SAP concernant les renseignements intégrés en rapport avec le World Economic Forum (WEF). Ce mandat prévoit que chaque canton présente au SAP un rapport de situation en relation avec le WEF et qu'il lui communique notamment les tentatives et les autorisations de manifestations. Dans son rapport sur la manifestation anti-WEF du 27 janvier 2007, l'Unité spéciale 9 a aussi mentionné les personnes qui avaient demandé l'autorisation au nom de l'«Alliance bâloise anti-WEF». Comme il ressort du rapport, cette alliance s'était formée à la demande de la police pour discuter des modalités de la manifestation. Plusieurs membres du Grand Conseil faisaient partie des demandeurs.

Comme il était ressorti de la consultation d'ISIS par la DélCdG à la suite de la requête de la CdG-BS, le rapport relatif aux élections au Grand Conseil de l'automne 2004 a débouché sur le premier enregistrement dans ISIS de quatre députés en tant que tiers. Le rapport sur la manifestation anti-WEF de janvier 2007 a ensuite entraîné une communication supplémentaire pour l'une des personnes concernées.

Il est ressorti de la visite à Bâle-Ville que le canton, qui établit des rapports à l'intention du SAP conformément aux mandats de ce dernier, n'a aucune influence sur les enregistrements dans ISIS. La sûreté cantonale n'émet même pas de recommandation concernant l'enregistrement d'une personne ou d'une organisation, la décision appartenant entièrement et exclusivement au SAP.

L'Unité spéciale 9 ne gère pas de banque de données en propre. Ses rapports sont conservés dans un système électronique distinct de celui de la police judiciaire. Ils sont effacés après cinq ans de conservation, comme l'exige l'art. 19, al. 1, de l'ordonnance ISIS[54]. Comme les informations ne présentent la plupart du temps plus d'importance pour la sûreté du canton après ce laps de temps, cette règle est acceptable aux yeux des services compétents.

ISIS est principalement utilisée comme source de référence, mais ne peut pas remplacer le fichier de données du canton, sans lequel l'Unité spéciale 9 ne pourrait pas, à ses propres dires, travailler correctement. Il n'est à son sens pas praticable de devoir fouiller dans les données d'ISIS toute une journée pour faire une simple appréciation de la situation. ISIS est par ailleurs d'un apport très limité pour la mise en réseau nationale des informations qui y sont enregistrées par le SAP sur communication des cantons, a précisé notre interlocuteur. Et d'ajouter que, par le passé, l'actualité des données n'était pas garantie en raison des retards accumulés par le

54 Le 1.1.2010 le Conseil fédéral a abrogé l'ordonnance ISIS du 30.11.2001. Les dispositions de l'art. 19 de l'ordonnance ISIS ont été reprises à l'art. 33 OSI-SRC.

SAP dans la saisie, et que le système tend rapidement à la saturation lorsque l'on ouvre plusieurs rapports en même temps pour consultation.

La sûreté du canton de Bâle-Ville estime que la mise en réseau des informations des différents cantons répond à une nécessité. Le système ISIS n'est à ses yeux toutefois pas en mesure de porter une communication du canton A nouvellement saisie à la connaissance du canton B, par exemple concernant un domaine qui présente un intérêt commun pour les deux cantons. Comme l'a appris la DélCdG, la réunion des chefs cantonaux de la sûreté organisée sur une base semestrielle par le SAP ne suffit pas à satisfaire à ce besoin de partage d'informations.

Le contrôle qualité interne de la sûreté bâloise exige que chaque rapport soit visé par le commissaire en chef, qui examine tout d'abord si le rapport se fonde sur un mandat concret ou s'il existe un rapport avec la liste d'observation. Il vérifie en outre si toutes les informations réunies dans le rapport sont pertinentes du point de vue de la protection de l'Etat. Ainsi, une condamnation antérieure remontant à l'adolescence ne doit pas être communiquée à Berne. Néanmoins, aux yeux du canton, l'appréciation définitive de l'importance des informations fournies pour la sûreté de l'Etat est toujours du ressort du SAP. Il n'y a pas de surveillance du procureur en chef, instance suprême du ministère public du canton, ou du conseiller d'Etat compétent, vu qu'aucun des deux ne peut consulter les dossiers de la sûreté sans l'aval du SAP.

La sûreté doit se tenir à une forme très générale lorsqu'elle informe la CdG du Grand Conseil de son activité. C'est à l'occasion de l'une de ces informations que la CdG-BS a pris connaissance du fait que l'article publié dans la presse kurde avait donné lieu à l'enregistrement de membres du Grand Conseil. Lorsque la CdG-BS a requis un droit d'accès, le SAP a intimé l'ordre à la sûreté bâloise de ne pas l'accorder, sous peine d'une dénonciation pour violation du secret de fonction.

Le canton estime toutefois que l'accès aux dossiers de la sûreté n'était en soi pas suffisant pour garantir une surveillance systématique des services de protection de l'Etat. La surveillance cantonale devrait pouvoir avoir accès aux mandats du SAP et au contenu de la liste d'observation confidentielle du Conseil fédéral pour pouvoir contrôler la légalité du traitement des données. C'est à ses yeux une condition absolue pour être en mesure d'apprécier le moindre rapport.

3.3 Visite de la DélCdG dans le canton de Genève

Le 30 mars 2009, la DélCdG a rendu visite aux services de sûreté intérieure du canton de Genève, qui sont hébergés à l'état-major de la police cantonale, elle-même rattachée au Département des institutions (Département de la sécurité, de la police et de l'environnement depuis décembre 2009). Les organes chargés de la protection de l'Etat disposent d'un grand centre de situation et de deux unités distinctes. La première, la Brigade de la sûreté intérieure, s'occupe des tâches prévues par la LMSI, tandis que la seconde, la Brigade du renseignement communautaire, se charge des missions de sûreté cantonale qui ne sont pas couvertes par la LMSI. Les services de protection de l'Etat sont dirigés par le sous-chef d'état-major renseignements, qui est directement subordonné au chef d'état-major de la police cantonale.

La sûreté du canton de Genève travaille sur la base de mandats concrets du SAP (119 en 2008). Agissant de sa propre initiative, elle procède par ailleurs à des investigations sur la base de la liste d'observation et fournit des informations au SAP. La

liste d'observation est considérée comme un cadre très général. La Confédération n'y fixe pas de priorités et elle ne signale pas non plus spécialement aux cantons les thèmes importants de portée nationale.

Avant transmission d'un rapport au SAP, le sous-chef d'état-major en charge du renseignement l'examine pour déterminer si le mandat du SAP est rempli et si le contenu présente un degré de pertinence suffisant sous l'angle de la protection de l'Etat. Il n'y a toutefois pas de contrôle de l'exécutif au niveau du Conseil d'Etat. Ce dernier a d'ailleurs besoin de l'assentiment du SAP pour consulter les données relevant de la protection de l'Etat que le canton se procure en vertu de la LMSI.

Comme il appartient au SAP de décider de la saisie ou non d'un rapport dans ISIS, le canton part de l'idée que le personnel du SAP chargé de l'opération possède les compétences et connaissances analytiques et juridiques nécessaires. Lorsqu'une communication est rejetée car jugée non pertinente, ce qui est arrivé dans certains cas, les informations sont effacées à Genève. Il convient de préciser que le SAP n'est pas en mesure de fournir pour chaque rapport une information sur son exactitude, sa pertinence et sa saisie dans ISIS, comme le souhaiterait le canton.

La sûreté intérieure genevoise gère sa propre banque de données en se fondant sur l'art. 16, al. 2, LMSI. Elle y classe aussi les rapports qu'elle établit à l'intention du SAP. Plusieurs centaines de personnes y figurent. Elle a expliqué à la DélCdG que la durée de conservation de 5 ans prescrite par l'ordonnance pour toutes les données ne répondait pas toujours aux besoins, estimant qu'un effacement différencié en fonction de l'importance des informations serait plus adapté.[55]

Pour la sûreté intérieure genevoise, sa propre banque de données est l'instrument de travail principal. Elle estime que les informations y sont plus complètes que dans ISIS et qu'elle est plus simple à utiliser, considérant qu'ISIS est lourde et peu conviviale. Enfin, du fait que la majorité des cantons contributeurs sont alémaniques, ISIS contient à ses yeux un grand nombre d'informations qui n'ont qu'une pertinence limitée pour la protection de l'Etat en Suisse romande en général, et à Genève en particulier. D'autant que les informations sont majoritairement saisies en allemand. Toutefois, ISIS reste un système nécessaire au travail des services de sûreté intérieure du canton de Genève.

3.4 Visite de la DélCdG dans le canton de Berne

Pour sa troisième visite, la DélCdG s'est rendue au Commandement de la police du canton de Berne le 29 juin 2009. Du point de vue organisationnel, la sûreté cantonale est rattachée à la Division de la police judiciaire, dans laquelle elle est subordonnée à l'une de ses unités organisationnelles (la Brigade spéciale 2, devenue la Brigade spéciale 4 le 1er février 2010). La sûreté cantonale remplit exclusivement des

55 Jusqu'à sa révision en 2004, l'ordonnance ISIS ne prévoyait pas de délai unique d'effacement des données pour les cantons. Les données pouvaient être conservées jusqu'à ce que le SAP eût informé les cantons de l'effacement desdites données dans ISIS, conformément à l'art. 15, al. 1, LMSI. Selon la proposition du DFJP du 16.6.2004, limiter à 5 ans la conservation des données pour les cantons devait permettre d'éviter que ceux-ci ne conservent des données ou dossiers déjà effacés au niveau fédéral. Force est toutefois de constater qu'en faisant preuve de célérité dans la transmission des informations relatives à l'effacement des données – comme le prévoit la LMSI –, le SAP aurait pu atteindre cet objectif sans la révision de l'art. 19 de l'ordonnance ISIS.

tâches en application de la LMSI, avec pour directives concrètes la liste d'observation et les mandats ponctuels du SAP (au nombre de 150 en 2008).

Avant leur transmission au SAP, les «produits» de la sûreté qui contiennent des données personnelles sont examinés sous l'angle de leur légalité par la Division de la police judiciaire, en l'occurrence le chef de la Brigade spéciale compétente. Les rapports sans données personnelles sont transmis directement au SAP. Il n'a été fait état d'aucun cas dans lequel le SAP aurait rejeté un rapport. Il arrive en revanche que le SAP demande des informations supplémentaires.

Le SAP est non seulement l'organe supérieur du point de vue hiérarchique, mais il dispose de plus vastes informations et de meilleures capacités d'analyse que la sûreté cantonale. Celle-ci a donc intérêt à recevoir des avis en retour du SAP lorsque, sur mandat de ce dernier, le canton a mené des investigations qu'il a consignées dans un rapport à son intention. Or tel n'est pas le cas en règle générale. La sûreté bernoise a néanmoins réussi à faire en sorte que la fluidité de l'information en provenance du SAP s'améliore, comme elle a pu le constater ces derniers temps.

Ni l'exécutif ni le législatif du canton de Berne n'exercent de surveillance régulière sur la sûreté cantonale. Le conseiller exécutif compétent et la CdG cantonale se limitent à prendre acte du rapport sur la sécurité intérieure établi chaque année à l'intention du SAP.

Depuis l'intégration de la police municipale de Berne à la police cantonale, la sûreté bernoise dispose de deux fichiers de données appelés à être importés dans une nouvelle banque de données de la sûreté cantonale. Aux termes de l'art. 16, al. 2, LMSI, le règlement d'exploitation du système cantonal doit être soumis au DDPS pour approbation. Avant cela, le préposé cantonal à la protection des données doit donner son aval au dispositif de protection de l'information et des données.

ISIS est surtout utilisée comme outil de référence pour les rapports rédigés par la sûreté cantonale et ceux des autres cantons. Le système permet ainsi de faire une recherche à l'échelle de la Suisse concernant certains faits ou personnes revêtant de l'importance sous l'angle de la LMSI. Il est toutefois considéré comme peu convivial. Les fonctions de consultation ne permettent pas, selon le canton, de procéder à des analyses limitées à certaines parties du canton. De plus, ISIS est peu utile pour identifier les liens entre les informations de plusieurs cantons. La sûreté tend par conséquent à rechercher les informations sur la situation dans un canton voisin directement auprès du service cantonal compétent, qui peut aussi donner des renseignements sur de nouveaux rapports qu'il a livré au SAP et qu'il serait possible de trouver dans ISIS.

4 Contacts de la DélCdG avec le PFPDT

4.1 Le PFPDT et le droit d'accès indirect

Aux termes de l'art. 18, al. 1, LMSI, toute personne peut demander au Préposé fédéral à la protection des données et à la transparence (PFPDT) qu'il vérifie si des données la concernant sont traitées conformément au droit dans ISIS. Après vérification, le PFPDT communique au requérant une réponse au libellé toujours identique selon laquelle aucune donnée la concernant n'a été traitée illégalement ou que, dans

le cas d'une éventuelle erreur dans le traitement des données, il a adressé au SAP la recommandation d'y remédier.

Sur la base de cette communication, la personne concernée ne sait toutefois pas si des informations la concernant figurent dans ISIS ou non. Elle a seulement la certitude que le PFPDT a vérifié l'objet de sa requête et que, en cas de fait non conforme au droit, il a émis une recommandation demandant la correction des irrégularités.

L'art. 18 LMSI ne fonde donc pas vraiment un droit d'accès, mais permet à la personne concernée d'enclencher un contrôle administratif indépendant. Le requérant n'a aucun droit de recours contre la communication du PFPDT. Il peut toutefois demander que le président de la cour du TAF compétente en matière de protection des données examine la communication du PFPDT. Le TAF contrôle la communication du PFPDT ou l'exécution de la recommandation émise par ce dernier. Le TAF a repris cette tâche en 2007 de la Commission fédérale de la protection des données et de la transparence (CFPDT), qui avait pris le relais de la Commission fédérale de la protection des données (CFPD) à l'entrée en vigueur de la loi sur la transparence[56], le 1er juin 2006.

Dans les années 1998 à 2007, le PFPDT a traité 185 demandes d'accès indirect à ISIS, leur nombre se répartissant assez également sur les dix années. Ensuite, on observe soudainement un pic de 148 demandes pour la seule année 2008, à la suite de l'«affaire des fiches bâloise».[57] En 2009, 34 nouvelles demandes ont été faites, ce qui porte le nombre total de requêtes à 367 à fin 2009.

4.2 Exceptions au droit d'accès indirect

Le 20 août 2001, la DélCdG s'est informée pour la première fois de l'exécution de la LMSI dans le domaine de la protection des données par le Préposé fédéral à la protection des données (PFPD), qui deviendra le PFPDT à l'entrée en vigueur de la loi sur la transparence. A partir de 2005, l'échange de vues s'est fait à un rythme annuel, ce qui a permis à la délégation de suivre de première main l'évolution de la pratique du droit d'accès indirect prévu à l'art. 18 LMSI.

Le 22 avril 2005, le préposé à la protection des données a informé la DélCdG que la CFPD avait émis plusieurs recommandations concernant le traitement du droit d'accès indirect.[58] Elle a notamment recommandé au préposé de documenter ses contrôles de manière appropriée, de vérifier la légalité de l'ensemble des opérations de traitement de données constatées et de contrôler notamment la conformité de l'application de l'ordonnance avec le droit supérieur.

Dans la discussion du 22 avril 2005, le PFPDT a montré à la DélCdG à quel point il était difficile, sous le régime du droit d'accès indirect, de vérifier si les données concernant une personne avaient été traitées dans ISIS conformément au droit. Il peut certes dans certains cas vérifier les informations enregistrées sous l'angle de leur plausibilité, mais il est en règle générale impossible de contrôler le degré de véracité des enregistrements sans informations complémentaires de la part du requé-

56 Loi fédérale du 17.12.2004 sur le principe de la transparence dans l'administration (LTrans; RS **152.3**).
57 16e rapport d'activités 2008/2009 du PFPDT, p. 44.
58 Décision de la CFPD du 15.3.2004, publiée dans la JAAC 70.95.

rant. Or celui-ci ne peut pas consulter les faits enregistrés dans ISIS. Il s'ensuit que la rectification ou l'effacement de données fausses sont loin d'être assurés sous le régime du droit d'accès indirect.[59]

Comme la délégation l'a appris à l'occasion de la discussion de 2005, le SAP avait systématiquement omis d'appliquer l'art. 18, al. 6, LMSI jusqu'au contrôle du PFPDT en 2004.[60] D'après cette disposition, les personnes ayant déposé une demande de renseignements sont informées des données les concernant enregistrées dans ISIS lorsque la durée de conservation des données est écoulée et qu'elles doivent être effacées. Ce n'est que suite à l'intervention du préposé à la protection des données que cinq personnes ont été informées par le SAP en novembre 2004. A ce jour, le SAP a appliqué au total 14 fois l'art. 18, al. 6, LMSI pour donner suite à une demande de renseignements ultérieure.

Le 28 juin 2006, le PFPDT a renseigné la DélCdG sur des recommandations supplémentaires que la CFPD avait émises dans une décision du 15 février 2006[61]. La décision concernait l'application de l'art. 18, al. 6, LMSI. Cette disposition autorise le PFPDT à fournir de manière appropriée des renseignements aux personnes qui en font la demande, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et qu'il n'existe pas d'autre moyen pour empêcher que ces personnes soient lésées gravement et de manière irréparable.

Par sa décision du 15 février 2006, la commission de recours a invité le PFPDT à interpréter l'art. 18, al. 3, LMSI en ce sens que la personne concrètement concernée puisse être informée qu'elle ne figure pas dans ISIS. La CFPD motivait l'abandon de la pratique restrictive appliquée par le PFPDT en se fondant sur une interprétation conforme à la Constitution qui satisfaisait en outre à la Convention européenne des droits de l'homme (CEDH).[62] Le 7 septembre 2006, le directeur de fedpol, auquel le SAP était subordonné, a recouru contre cette décision de principe de la CFPD devant le Tribunal fédéral (TF). Le TF a rejeté le recours sur tous les points, refusant même d'entrer en matière sur certains d'entre eux.[63]

La DélCdG a en outre appris le 28 juin 2006 que la CFPD avait constaté dans sa décision du 15 février 2006 que le droit d'accès indirect ne satisfaisait pas aux exigences posées par le droit à un recours effectif tel que prévu à l'art. 13 CEDH. La CFPD était arrivée à la conclusion que le législateur devait améliorer cette voie de droit pour éviter que la Cour européenne des droits de l'homme, statuant sur un recours, ne qualifie la disposition de contraire à la CEDH. Comme le PFPDT l'a expliqué à la délégation, la Cour européenne des droits de l'homme a aussi rendu un arrêt dans un cas suédois qui viendrait à l'appui des conclusions de la CFPD concernant le droit d'accès indirect.[64]

Le 2 mai 2007, à l'occasion de la discussion suivante, le PFPDT a informé la DélCdG qu'il avait adapté sa pratique dans l'application de la disposition d'exception en fonction de l'arrêt de la Cour européenne des droits de l'homme. Selon cette

59 Rapport annuel 2005 des CdG et de la DélCdG du 20.1.2006 (FF **2006** 4043 4168).
60 12e rapport d'activités 2004/2005 du PFPD, p. 33.
61 La décision a été notifiée le 23.5.2006 et publiée dans Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht (ZBl) 2007, p. 392 (non traduit).
62 Convention du 4.11.1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH; RS **0.101**).
63 Arrêt 1A.188/2006 du TF du 8.2.2007.
64 Arrêt de la Cour européenne des droits de l'homme du 6.6.2006, Segerstedt-Wiberg et autres/Suède, nº 62332/00.

conception, il est signalé aux demandeurs qu'ils ont la possibilité de fournir des informations complémentaires qui permettent au PFPDT d'apprécier si des raisons suffisantes justifient que l'on informe la personne du fait qu'elle ne figure pas dans ISIS.

4.3 Développement du droit d'accès

Le 16 avril 2008, le PFPDT s'est entretenu avec la DélCdG de la conformité des modalités du droit d'accès avec la CEDH en relation avec le projet de loi sur les systèmes d'information de police de la Confédération (LSIP)[65]. Sur proposition de la CAJ-N, le Parlement, s'écartant du droit d'accès indirect proposé par le Conseil fédéral, a opté pour un système de réponse différée. Selon l'art. 8 LSIP, la réponse est différée lorsque les données traitées concernant le demandeur sont liées à des intérêts prépondérants pour la poursuite pénale qui exigent le maintien du secret ou lorsqu'aucune donnée la concernant n'est traitée. Dans ce cas, le demandeur peut exiger que le PFPDT procède à une vérification. Contrairement à ce que prévoit l'art. 18 LMSI, les autorités doivent motiver une limitation du droit d'accès, décision qui peut elle-même être attaquée sur la base des dispositions de la loi sur la protection des données.

Concernant ISIS, le PFPDT s'est prononcé dès le début pour un droit d'accès direct en application des art. 8 et 9 LPD, tout en défendant le point de vue selon lequel la forme du droit d'accès prévue par la LSIP permettrait également d'organiser la transmission de renseignements sur les données ISIS en conformité avec la CEDH. Il forme le vœu que cet aspect soit traité à l'occasion de la prochaine révision LMSI II. La CFPD avait posé la même exigence dans sa décision du 15 février 2006.

Le 31 mars 2009, le PFPDT informé à nouveau la DélCdG de l'évolution de la pratique concernant l'application de l'exception prévue au droit d'accès indirect à l'art. 18, al. 3, LMSI. A partir de 2006, le PFPDT a estimé dans quelques cas que les conditions étaient remplies pour communiquer à des personnes qui l'avaient demandé si elles figuraient ou non dans ISIS. Après la mise au jour en 2008 du fait que des membres du Grand Conseil de Bâle-Ville faisaient l'objet d'un enregistrement dans ISIS, le nombre des demandes a fortement augmenté, en particulier en provenance du canton de Bâle-Ville. En l'occurrence, sur proposition du SAP, le PFPDT, estimant qu'il était justifié de faire preuve de largesse dans l'application de l'art. 18, al. 3, LMSI, a communiqué à 45 demandeurs du canton de Bâle-Ville qu'ils ne figuraient pas dans ISIS. Dans une demi-douzaine de cas, le PFPDT a même donné aux demandeurs une information sommaire concernant le contenu des communications enregistrées dans ISIS, ce dont les médias se sont ensuite partiellement fait l'écho.[66]

Une partie des demandeurs a recouru au Tribunal administratif fédéral (TAF), exigeant un accès sans restriction à leurs données ISIS. Le TAF n'a pas accédé à ces demandes. Dans un cas, il a constaté que, aux termes de l'art. 3, al. 2, LMSI, il n'était pas autorisé d'enregistrer une personne dans ISIS au motif qu'elle s'était

65 Loi fédérale du 13.6.2008 sur les systèmes d'information de police de la Confédération (LSIP; RS **361**).

66 V. notamment l'article de Kaspar Surber «Nouvelle affaire des fiches» dans la WOZ du 7.8.2008 (en allemand).

portée demandeuse pour l'organisation d'une manifestation autorisée.[67] Le cas montré du doigt par le TAF a été transmis à la DélCdG dans le cadre des effacements que le SAP a dû communiquer à la délégation sur mandat de cette dernière. L'effacement de l'enregistrement en tant que tiers a été fait le 1er avril 2009.

Sur la base des documents à sa disposition, la DélCdG a constaté que le SAP avait reçu le dossier en mai 2008 avec la demande d'accès. Aux termes de l'art. 18, al. 5, LMSI, le SAP devait soumettre l'enregistrement du requérant à une appréciation générale à la suite de la demande. Bien que la DélCdG ait souligné l'importance du respect de l'art. 3 LMSI en relation avec la requête de la CdG-BS, le SAP n'a pas effacé l'enregistrement à l'occasion de ce contrôle. Si le demandeur n'avait pas saisi le TAF en s'appuyant sur l'art. 18, al. 2, LMSI, il serait resté enregistré illégalement dans ISIS.

Dans l'échange de vues avec la DélCdG, le PFPDT s'est clairement distancié de la conception du SAP selon laquelle la LMSI autoriserait des enregistrements «positifs», qui contiendraient des informations à décharge des personnes concernées. En dernière analyse, un enregistrement de ce type sape l'esprit de l'art. 3 LMSI. Il convient d'insister sur le fait que seules les personnes et les événements revêtant une importance pour la protection de l'Etat peuvent être saisis et traités dans ISIS. Le PFPDT a en outre estimé que se posait aussi la question de savoir si les cantons étaient suffisamment formés et encadrés pour pouvoir faire la distinction entre les informations pertinentes pour la sécurité de l'Etat et les informations qui ne le sont pas. Dans ce contexte, le PFPDT a eu le sentiment que les cantons envoyaient de nombreux rapports de police à Berne sans trop les filtrer, et que ces rapport étaient ensuite entrés dans ISIS sans distinction, quand bien même ils ne présentaient pas la qualité nécessaire sous l'angle de la protection de l'Etat.

4.4 Droit et aspects techniques des banques de données

Le 31 mars 2009, le PFPDT a aussi discuté avec la DélCdG de la question de la nature des données dont le classement est autorisé dans les différentes banques de données d'ISIS. Selon l'ordonnance, le système d'information ISIS compte plusieurs fichiers de données. Seule la banque de données ISIS01 contient les informations relevant à proprement parler de la protection de l'Etat. La banque ISIS02 contient les données relatives à l'administration des affaires du SAP. Les données que le SAP traite concernant des personnes qui ont fait l'objet d'un contrôle de sécurité sont classées dans ISIS06. L'ordonnance prévoit le même droit d'accès indirect pour toutes ces banques de données. Sur ce point, la pratique du SAP est conforme à l'ordonnance ISIS. Cependant, le PFPDT a estimé que le droit d'exécution n'était à cet égard pas conforme à la loi.

Dans un arrêt du 18 mars 2009[68], le TAF a aussi conclu qu'il était problématique de soumettre la banque de données Administration du SAP (ISIS02) au seul droit d'accès indirect prévu à l'art. 18 LMSI. Il a par conséquent recommandé au SAP de sortir la banque de données ISIS02 du système ISIS et de la soumettre au droit d'accès indirect selon la loi sur la protection des données (LPD) à l'occasion de la prochaine révision. Comme il le précise dans sa réponse du 8 septembre 2009 au

67 Arrêt non publié du TAF du 18.3.2009 (A-5922/2008).
68 Arrêt non publié du TAF du 18.3.2009 (A-5919/2008).

TAF, le SAP a accueilli favorablement la recommandation sur le principe, précisant toutefois que le moment de l'opération serait tributaire de la planification informatique du SRC.

Dans la même décision, le TAF critique en outre le fait que le SAP ait aussi enregistré des articles de journaux dans ISIS01 sous le nom de l'éditeur, estimant qu'il n'était pas conforme à la loi qu'un établissement d'édition fasse l'objet d'un enregistrement au seul motif qu'un de ses journaux a publié des informations que le SAP entend saisir. Selon l'arrêt, il devrait être possible d'enregistrer un article de journal dans la banque de données sans pour autant enregistrer le journal lui-même comme objet. Dans le cas contraire, il faudrait implémenter une restriction de la fonction de recherche empêchant de trouver les articles d'un journal donné dans la banque de données Protection de l'Etat d'ISIS. Selon le PFPDT, le SAP avait accepté la recommandation en se déclarant disposé à anonymiser les noms des journaux et d'autres médias dans ISIS.

Comme la DélCdG, le PFPDT a constaté que, depuis la migration sur ISIS-NT, les tiers étaient classés selon une nouvelle technique. Dans l'ancienne ISIS, le nom d'un tiers figurait uniquement dans la brève synthèse de la communication et ne pouvait pas être trouvé par une recherche orientée sur une personne enregistrée. Pour faciliter la recherche avec la fonction de texte intégral, les noms des tiers étaient caractérisés par une séquence spéciale de caractères («D>»). Dans ISIS-NT, les tiers sont enregistrés comme un objet en propre, et peuvent donc être trouvés par une recherche orientée personne comme des individus revêtant une importance directe du point de vue de la protection de l'Etat. Pour qu'un tiers obtienne un statut différent, il faut seulement adapter la mention qui l'identifie comme tiers.

Le modèle de données relationnel fait que le SAP s'attache à identifier tous les objets d'une communication et à les représenter dans les structures de la banque de données d'ISIS-NT, avec pour conséquence que, selon de PFPDT, une recherche orientée personne dans le nouveau système permet de trouver comme tiers des personnes mentionnées accessoirement dans un rapport de police, qui ne présentent en réalité aucun intérêt pour la protection de l'Etat.

Sur la base des éléments dont il disposait sur la pratique du SAP, le PFPDT a estimé que le risque existait qu'un tiers devienne une personne revêtant en propre de l'importance pour la protection de l'Etat du fait d'une éventuelle nouvelle communication, quelle que soit la qualité de cette dernière. Des événements tout à fait banals qui n'auraient clairement pas dû être traités en relation avec l'art. 3 LMSI pourraient ainsi faire qu'une personne soit considérée comme un danger pour la sûreté de la Suisse et fasse l'objet d'un enregistrement. Le PFPDT en est venu à s'interroger sur le moyen qui permettrait à la loi de conserver son effet original dans un contexte où les possibilités techniques sont en constante évolution.

5 Clarifications juridiques par la DélCdG

5.1 Contrôle cantonal et haute surveillance

A la suite de la requête adressée par la CdG-BS à la DélCdG demandant à cette dernière de s'exprimer sur l'organisation des compétences dans la surveillance de l'activité cantonale de sûreté, la délégation a de son côté demandé au DFJP, par lettre du 16 avril 2008, de lui fournir un avis concernant les compétences des can-

tons en matière de contrôle et de haute surveillance dans le domaine de la protection de l'Etat (v. chap. 2.4).

L'avis a été émis par l'OFJ; daté du 25 juin, il a été transmis par le DFJP à la DélCdG le 14 juillet 2008. Il ressort des investigations de l'OFJ que l'accès aux données que les autorités cantonales ont collecté en vertu de la LMSI requiert dans tous les cas l'approbation préalable du SAP, même lorsque le requérant est l'organe de surveillance cantonal compétent.

L'OFJ s'est appuyé sur l'art. 23, al. 2, OMSI, lequel prévoit expressément la chose. La disposition s'appuie elle-même sur l'art. 17, al. 1, LMSI, qui dispose que le Conseil fédéral règle par voie d'ordonnance la transmission de données à des destinataires accomplissant une tâche de service public en Suisse. Comme la compétence réglementaire de la Confédération dans le champ d'application de la LMSI est exclusive, poursuit l'OFJ, la Confédération peut aussi régler la transmission de données pour la surveillance. Les droits de surveillance cantonaux visés à l'art. 16, al. 3, LMSI ne sont toutefois pas abrogés, mais simplement limités. Pour les personnes à qui les cantons confient des tâches d'exécution de la LMSI, c'est donc le droit cantonal régissant la fonction publique qui s'applique, et elles sont donc aussi soumises à l'autorité cantonale de surveillance.

Du point de vue de l'OFJ, les autorités cantonales conservent des droits de surveillance dans l'exécution de la LMSI, mais ils sont limités. Aux termes de l'art. 23, al. 1, OMSI, l'organe de contrôle cantonal vérifie que les processus administratifs contrôlés correspondent aux prescriptions juridiques applicables, notamment que les données relatives au maintien de la sûreté intérieure sont traitées séparément des autres informations de police. Mais il est aussi possible de contrôler comment et où les informations ont été traitées et avec quels moyens elles ont été acquises. L'OFJ estime donc qu'un contrôle matériel des données collectées effectué par l'organe de surveillance cantonal ne peut se faire qu'avec l'assentiment du SAP.

Selon l'OFJ, une haute surveillance par le Parlement cantonal ou ses organes est aussi possible, bien que la chose ne soit pas précisée par la LMSI. D'après l'art. 47, al. 2, de la Constitution fédérale (Cst.)[69], il convient de laisser la plus grande autonomie aux cantons pour leur organisation, même dans l'exécution du droit fédéral.

Après analyse de l'avis de l'OFJ, la DélCdG a informé la CdG-BS de ses investigations par lettre du 10 octobre 2008, à laquelle elle a joint copie de l'avis. La délégation a par ailleurs invité la cheffe du DFJP à mettre l'avis à la disposition de tous les conseillers d'Etat responsables de la sûreté, tant que le SAP serait encore rattaché à son département.[70]

Sur demande, une copie de l'avis a été transmise à un professeur de l'Université de Bâle qui était chargé par le Département de la justice du canton de Bâle-Ville d'examiner sous l'angle juridique les possibilités existant pour la surveillance cantonale dans le domaine de la sûreté. Dans son rapport annuel 2008, la DélCdG a publié un résumé détaillé de l'avis.[71]

69 Constitution fédérale de la Confédération suisse du 18.4.1999 (Cst.; RS **101**)

70 Comme la cheffe du DFJP l'a communiqué à la DélCdG par lettre du 13.1.2009, elle a jugé qu'il n'était pas opportun de le faire, vu que tous les travaux en relation avec le transfert du SAP au DDPS n'étaient pas encore achevés.

71 Rapport annuel 2008 des CdG et de la DélCdG des Chambres fédérales du 23.1.2009 (FF **2009** 2215 2267 s.).

Le 18 décembre 2008, le Grand Conseil du canton de Bâle-Ville a décidé de réduire d'un tiers le budget de la sûreté cantonale. Cette décision s'inscrivait dans le contexte du traitement des données de députés au Grand Conseil dans ISIS, sujet qu'avait soulevé la CdG-BS.[72]

Le 23 décembre 2008, le président du gouvernement et chef du Département de la justice du canton de Bâle-Ville a saisi le DFJP, émettant différentes objections contre l'avis de l'OFJ du 25 juin 2008, en faisant notamment valoir que le SAP ne pouvait pas refuser à un organe de surveillance cantonal l'accès à des données qui avaient été fournies par des services du canton. Il a en outre demandé un examen du projet d'ordonnance cantonale sur la protection de l'Etat.[73]

Après que l'OFJ eut pris position sur les propositions du gouvernement cantonal, le chef du Département de la justice et de la sûreté du canton de Bâle-Ville a institué un groupe de travail afin sonder la marge de manœuvre qu'offrait la législation fédérale pour une possible surveillance cantonale sur la protection de l'Etat et d'élaborer un nouveau projet d'ordonnance cantonale.[74]

Le 26 juin 2009, le chef du Département de la justice et de la sûreté du canton de Bâle-Ville a transmis le projet du groupe de travail au chef du DDPS, afin de lui donner l'occasion de s'exprimer sur la compatibilité de l'ordonnance avec le droit fédéral. Le SAP s'est ensuite adressé à l'OFJ le 10 août 2009 pour lui demander de clarifier quelques questions juridiques en relation avec le projet d'ordonnance du canton de Bâle-Ville.

Le 8 septembre 2009, le Conseil d'Etat du canton de Bâle-Ville a adopté l'ordonnance cantonale sur la sureté, sans toutefois la mettre en vigueur. Selon le communiqué de presse, l'examen demandé au DDPS se faisait attendre et l'ordonnance entrerait en vigueur dès réception d'un avis favorable de Berne.[75]

La DélCdG a invité l'OFJ à une audition concernant les examens réalisés sur la surveillance cantonale en matière de protection de l'Etat, qui s'est tenue le 29 septembre 2009. Le vice-directeur de l'OFJ a commenté l'avis du 13 mars 2009 et donné par ailleurs des informations relatives à la prise de position de l'OFJ sur le projet d'ordonnance du canton de Bâle-Ville, que l'office avait préparée pour le 15 septembre 2009 à la suite des questions du SAP.

L'OFJ a réitéré dans son avis que l'art. 23, al. 2, OMSI disposait que les organes cantonaux de surveillance devait recueillir l'assentiment du SAP pour accéder aux données relevant de la LMSI. Il a estimé que le Conseil fédéral pouvait appuyer ce principe sur la délégation de compétence prévue à l'art. 17, al. 1, LMSI, ajoutant toutefois que l'art. 16, al. 3, LMSI précisait expressément que les prérogatives de surveillance prévues par le droit cantonal devaient être réservées.

Aux yeux de l'OFJ, l'art. 23, al. 2, OMSI doit permettre aux autorités cantonales de surveillance d'accomplir leurs tâches correctement. A l'inverse, la disposition per-

72 Le 10.3.2009, le Conseil d'Etat a décidé de soumettre un crédit supplémentaire au Grand Conseil pour annuler la réduction budgétaire. Le Grand Conseil a approuvé le crédit supplémentaire le 14.10.2009.

73 La DélCdG avait été informée des travaux préparatoires de l'ordonnance à l'occasion de sa visite du 30.1.2009 aux organes de protection de l'Etat du canton de Bâle-Ville.

74 Communiqué de presse du Département de la justice et de la sûreté du canton de Bâle-Ville «Double stratégie pour un meilleur contrôle de la sûreté», 1.4.2009.

75 Communiqué de presse du Département de la justice et de la sûreté du canton de Bâle-Ville «Le gouvernement adopte l'ordonnance sur la sûreté», 8.9.2009.

met le cas échéant au SAP de refuser l'accès aux données lorsque des raisons tenant à la sûreté intérieure le commandent. L'idée n'étant pas d'entraver les organes cantonaux dans leur mission, l'accès peut être refusé uniquement pour des motifs touchant à la sûreté intérieure ou extérieure.

Pour ce qui est de l'exécution de la surveillance, les autorités cantonales – à commencer par les organes parlementaires de surveillance – peuvent accéder aux données disponibles dans la mesure où elles ont reçu le feu vert du service fédéral compétent. Le SAP ne peut refuser son assentiment par principe, mais seulement pour les données qui ne doivent pas être transmises pour des raisons liées à la sûreté.

En vertu du droit en vigueur, toujours selon l'OFJ, il est donc possible d'envisager un traitement différencié qui permet à la fois aux autorités cantonales de surveillance de vérifier si les services cantonaux travaillent correctement et si les procédures sont bien définies au niveau cantonal, cela même sans connaissance de certains cas particulièrement sensibles. Un accès sans restriction à l'ensemble des données n'est pas indispensable pour répondre à ces questions, selon l'OFJ.

L'OFJ a jugé d'un œil critique la Commission de surveillance, qui est à l'origine de l'ordonnance sur la sûreté du canton de Bâle-Ville, estimant qu'il était manifeste que ladite commission voulait intégrer les autorités cantonales de la sûreté afin d'avoir accès à leurs données sans devoir soumettre son action à l'approbation du SAP.

De l'avis de l'OFJ, ce genre de construction déboucherait sur des conflits insolubles avec la LMSI. Si la Commission de surveillance est une instance de contrôle, comme on peut le conclure à la lecture du descriptif de ses tâches, l'accès pour elle aux données relevant de la LMSI doit rester sujet à approbation, comme le prévoit l'art. 23, al. 2, OMSI. Si la commission est en revanche rattachée à l'autorité cantonale de protection de l'Etat chargée de collecter des informations, ce statut est en contradiction avec le descriptif de sa fonction, qui se limite à des compétences de contrôle. Les membres de la Commission de surveillance ne pourraient pas non plus travailler sans être liés par des instructions, comme le prévoit l'ordonnance, car les prescriptions du SAP seraient aussi contraignantes pour eux.

Le DDPS a transmis l'avis négatif de l'OFJ au canton de Bâle-Ville au début d'octobre 2009.[76] Lors de sa discussion du 26 octobre 2009 avec le chef du DDPS, la DélCdG a toutefois appris que des discussions se poursuivaient entre les deux parties et que le chef du DDPS voulait rencontrer le directeur du Département de la justice et de la sûreté du canton de Bâle-Ville.

A l'occasion de cette rencontre, qui a eu lieu le 6 novembre 2009, il a été convenu d'élaborer des modalités contraignantes pour la surveillance de la sûreté cantonale dans le cadre de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP). Des représentants des cantons et du DDPS, avec le soutien de l'OFJ, ont élaboré de nouvelles dispositions pour régir la surveillance des services cantonaux par voie d'ordonnance.

Selon la réglementation proposée, la surveillance cantonale doit connaître les mandats concrets confiés par la Confédération à l'organe cantonal de la sûreté et être à même de vérifier son travail sur la base de ces critères. Pour réaliser ces contrôles spécifiques, l'organe cantonal de surveillance peut exiger avoir accès aux données

76 Communiqué de presse du Département de la justice et de la sûreté du canton de Bâle-Ville «Ordonnance cantonale sur la sûreté: le canton a reçu la réponse de la Confédération», 2.10.2009.

de la protection de l'Etat qui sont traitées au niveau cantonal sur mandat de la Confédération.

Lorsqu'une demande d'accès concrète est refusée, le canton peut 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, de la loi sur le Tribunal fédéral (LTF)[77]. La CCDJP a pris connaissance des résultats de ces travaux et les a approuvés le 8 avril 2010.

5.2 Les limites de l'art. 3 LMSI

A sa séance du 30 janvier, la DélCdG s'est fait présenter une analyse de l'avis remis le 16 octobre 2008 par l'OFJ sur mandat du DDPS concernant l'enregistrement d'un député au Grand Conseil du canton de Bâle-Ville. Dans la discussion avec le vice-directeur de l'OFJ, la question a aussi été soulevée de savoir dans quelle mesure, le cas échéant, il pouvait être admis que des informations concernant l'exercice des droits politiques soient saisies dans ISIS. Cette question en soulève d'autres, qui touchent à l'interprétation des limites que l'art. 3 LMSI impose aux organes de protection de l'Etat pour le traitement des données. Pour répondre à ces questions, la DélCdG a exigé du DDPS un avis supplémentaire; daté du 2 juin 2009, il a été présenté à la DélCdG le 29 septembre 2009.[78]

Selon l'avis, l'art. 3 LMSI interdit aux organes de protection de l'Etat de traiter des informations relatives à l'engagement politique ou à l'exercice des droits découlant de la liberté d'opinion, d'association et de réunion. L'al. 1 de l'article attache toutefois ce traitement à des conditions restrictives. Le traitement, et donc la conservation de telles informations, est licite uniquement lorsqu'une présomption sérieuse permet de soupçonner que les droits politiques sont détournés pour préparer ou exécuter des actes violents.

Ce principe posé par l'art. 3 LMSI est toutefois relativisé lorsqu'une personne fait partie d'une organisation ou d'un groupe que le Conseil fédéral a intégré à la liste d'observation en application de l'art. 11 LMSI. Lorsqu'il est question des activités de ces organisations et de leurs protagonistes, toutes les informations peuvent être traitées. Aux termes de l'art. 11, al. 2, LMSI, le Conseil fédéral intègre les organisations à la liste d'observation uniquement lorsqu'elles sont concrètement soupçonnées de menacer la sûreté intérieure ou extérieure du pays.

La condition au traitement d'informations sur les activités politiques d'une personne ne réside pas dans un soupçon fondé contre la personne en question; la question fondamentale est en fait de savoir si la personne peut être considérée comme un protagoniste d'une organisation figurant sur la liste d'observation. Pour cela, il faut qu'une relation puisse être établie entre l'organisation et la personne en question, que celle-ci soit membre de ladite organisation ou qu'elle la soutienne par un autre biais, à travers des dons financiers ou une aide logistique.

L'art. 3, al 2, LMSI règle les conditions auxquelles des informations sur l'exercice des droits politiques peuvent être saisies comme données relatives à la personne. Cela arrive dans ISIS par exemple lorsqu'une demande d'autorisation de manifester

77 Loi du 17.6.2005 sur le Tribunal fédéral (LTF; RS **173.110**).
78 Avis de l'OFJ du 2.6.2009 concernant l'interprétation de l'art. 3, al. 2, LMSI.

est reliée à une personne enregistrée via une relation dans la banque de données. Après cela, il est possible d'accéder à cette information en faisant une recherche basée sur le nom de la personne.

L'art. 3, al. 2, LMSI dispose que les informations recueillies sur la base de l'art. 3, al. 1, LMSI ne peuvent pas être enregistrées avec référence nominale lorsque les soupçons relatifs à un comportement punissable ne sont pas corroborés par les activités observées. Si l'on respecte la disposition à la lettre, il n'est pas autorisé d'enregistrer nominalement une information relative à un engagement politique lorsque les soupçons relatifs à un comportement punissable ne sont pas immédiatement corroborés par les activités observées. En principe, il faut la confirmation d'un soupçon d'informations supplémentaires auxquelles il est nécessaire de pouvoir accéder nominalement afin qu'elles puissent être intégralement retenues pour la vérification du soupçon.

Par contre, lorsque, sur la base d'une esquisse de soupçon non confirmée, toutes les informations relatives à une personne concernant l'exercice de ses droits politiques peuvent être immédiatement saisies dans ISIS, il n'y a plus de distinction par rapport au traitement d'autres informations qui ne bénéficient pas du régime de protection prévu à l'art. 3 LMSI. Or cette pratique serait en contradiction avec l'esprit général de la LMSI, qui prête une grande valeur à l'exercice des droits politiques et entend soumettre le traitement de données dans ce contexte à un régime spécial.

De l'avis de l'OFJ, il faut par conséquent que les informations collectées sur la base de l'art. 3, al. 1, LMSI soient traitées avec une retenue particulière dans le cas d'une saisie nominale. Cette retenue n'a toutefois pas été constatée dans le cadre des investigations que l'OFJ a menées en relation avec l'enregistrement d'un député au Grand Conseil de Bâle-Ville.

L'OFJ estime que, dans sa version en vigueur, l'art. 3, al. 2, LMSI pose un problème au niveau de l'exécution. Cependant, si l'art. 3, al. 2, LMSI devait être abrogé, il faudrait s'assurer que le traitement de données collectées sur la base de l'art. 3, al. 1, LMSI soit soumis à des conditions plus strictes que le traitement des autres informations. Ainsi, une vérification institutionnalisée des données à brefs intervalles pourrait permettre une décision rapide concernant la corroboration des éléments fondant le soupçon. Il serait en outre imaginable, aux yeux de l'OFJ, de durcir les exigences relatives à l'enregistrement de la première communication conformément à l'art. 3, al. 1, LMSI afin que les indices très minces ne soient carrément jamais saisis nominalement.

6 Appréciations de la DélCdG

6.1 Critères de la haute surveillance

La DélCdG surveille l'activité de la protection de l'Etat et la contrôle sous l'angle la légalité, de l'opportunité et de l'efficacité (art. 52, al. 2, LParl)[79]. Par ses contrôles, elle doit s'assurer que toutes les données enregistrées dans ISIS sont traitées conformément à la loi. Concrètement, ces informations doivent être exactes et importantes pour les activités de protection de l'Etat prescrites par la loi (art. 15, al. 1, LMSI).

79 Loi du 13 décembre 2002 sur l'Assemblée fédérale (LParl; RS **171.10**).

Le contrôle de chaque enregistrement dans ISIS dépasserait toutefois largement le cadre de la mission de haute surveillance parlementaire, qui, dans le meilleur des cas, doit se fonder sur des sondages. Il s'ensuit que la DélCdG doit aussi mettre en œuvre d'autres moyens pour savoir si la qualité des données mérite sa confiance. Un point essentiel à cet égard est le fonctionnement du contrôle interne de protection des données, qui doit garantir leur qualité et leur pertinence conformément à la loi (art. 5, al. 5, LMSI). La DélCdG peut en outre examiner l'organisation et les procédures de traitement des données sous l'angle de leur adéquation aux objectifs visés, notamment pour vérifier si elles permettent d'obtenir la qualité des données requise par la loi.

En dernière analyse, ce sont le département compétent et le Conseil fédéral qui répondent de la légalité du fonctionnement des organes de protection de l'Etat. La DélCdG observe donc aussi avec quelle régularité et quelle intensité les instruments de contrôle sont utilisés à ce niveau.

6.2 Les contrôles de qualité ne satisfont pas aux exigences légales

L'examen par la DélCdG du système interne d'assurance qualité correspond à la forme première de la haute surveillance dans le sens d'un «contrôle des contrôleurs». A cette fin, la DélCdG a procédé à ses propres investigations auprès du SAP. Son appréciation du contrôle interne de la protection des données au sein du SAP se fonde toutefois principalement sur les éléments mis au jour par l'enquête réalisée en interne au DDPS par la Surveillance SR en 2009.

L'enquête de la DélCdG a révélé que, dans l'ancien système ISIS, le SAP accusait déjà des retards substantiels dans ses tâches légales d'assurance qualité. A la migration vers ISIS-NT, 76 000 appréciations générales étaient en souffrance. Les problèmes liés à l'introduction d'ISIS-NT ont fait que, pendant presque quatre ans, le SAP a suspendu les appréciations générales périodiques et n'était pas non plus à même de soumettre toutes les nouvelles communications à un contrôle initial. Ainsi, quelque 16 000 contrôles initiaux et 40 000 contrôles périodiques prescrits légalement n'ont pas été faits depuis le début de 2005.

Dans ces circonstances, on ne plus parler de cas en suspens dans le contrôle qualité du SAP. Alors que les contrôles initiaux ont encore été partiellement exécutés, la DélCdG constate sur la base de l'évolution de ces dernières années que, pour les appréciations générales périodiques en suspens, l'activité de contrôle effective ne correspond aucunement aux prescriptions de l'art. 16 de l'ordonnance ISIS.

La DélCdG n'a pas vérifié systématiquement la qualité des contrôles effectués. Sur les échantillons qu'elle a examinés de plus près, elle a trouvé certains cas remontant à l'époque de l'ancien système ISIS pour lesquels les appréciations générales périodiques n'avaient pas été effectuées selon des critères assez stricts. D'après la surveillance interne du DDPS, le contrôle matériel de la pertinence pour la protection de l'Etat n'était souvent fait que de manière aléatoire au moment du contrôle initial. La délégation n'en conclut pas pour autant que les collaborateurs de la Section Assurance qualité aient délibérément appliqué des standards laxistes à leurs contrôles.

La direction du SAP a ordonné des coupes dans la systématique des contrôles de qualité. Aux termes de l'art. 16, al. 3, de l'ordonnance ISIS, les informations qui

figurent dans la banque de données depuis plus de trois ans, avec l'appréciation «peu fiables», doivent être effacées à l'occasion d'une appréciation générale. La poursuite du traitement de ces données doit être motivée et requiert l'autorisation de la direction du service.

Selon une directive interne du 18 octobre 1999 – dont la validité a été une nouvelle fois confirmée en 2009 – la Section Assurance qualité peut, face à des informations peu fiables relevant du domaine de la prolifération, compter sur l'approbation automatique du chef du SAP pour la conservation des données lorsque les informations présentent «un lien avec la Suisse» et respectent le «mandat légal». Comme en principe aucune information qui ne satisfait pas à ces critères ne devrait légalement être enregistrée dans ISIS, cette réglementation s'applique de facto à toutes les informations sur la prolifération. Pareil automatisme supprime, pour la Section Assurance qualité, la tâche qui consiste à contrôler dans chaque cas l'importance d'une information peu fiable. Or cette suppression est en contradiction avec l'exigence de contrôle de la pertinence visée à l'art. 15, al. 5, LMSI.

Par ailleurs, le Conseil fédéral a aussi dilué les critères applicables au contrôle de la qualité par voie d'ordonnance. Dans la révision du 30 novembre 2001 de l'ordonnance ISIS, il a abrogé la disposition qui exigeait le réexamen de toutes les communications peu fiables déjà enregistrées relatives à une personne à l'occasion de la saisie d'une nouvelle communication la concernant (art. 9, al. 3, ordonnance ISIS du 1.12.1999). Dans sa proposition au Conseil fédéral, le DFJP avait soutenu que la disposition n'était pas nécessaire, vu que la vérification concernant la fiabilité d'une communication intervenait de toute façon quelques années plus tard dans le cadre de l'appréciation générale périodique. La proposition précisait que la preuve avait été apportée que la Section Assurance qualité effaçait même des données sûres lorsqu'elles n'étaient plus nécessaires pour la protection de l'Etat.[80]

Dans le commentaire relatif à la révision de l'ordonnance ISIS du 30 novembre 2001, on peut toutefois lire que la réévaluation systématique de toutes les communications relatives à une personne à la saisie d'une nouvelle communication la concernant s'est révélée impraticable dans les faits.[81] Or cette exigence avait déjà été adoptée en août 1992 avec l'ordonnance ISIS provisoire et représentait donc la pratique en vigueur, sur laquelle le Conseil fédéral s'était appuyé dans son message relatif la LMSI. Il aurait appartenu au DFJP d'éclaircir pourquoi le SAP estimait soudainement qu'une disposition n'était plus exécutable sept ans après son entrée en vigueur. Au lieu faire en sorte que l'ordonnance soit respectée ou de prêter son concours, le DFJP a soutenu l'abrogation de la disposition dérangeante.

Le département compétent et le Conseil fédéral ont ajouté foi aux indications du SAP, selon lesquelles les contrôles abandonnés seraient compensés dans le cadre des appréciations générales périodiques. Rétrospectivement, compte tenu du fait que ces contrôles n'étaient alors plus effectués que de manière sporadique et qu'ils ont ensuite été totalement abandonnés, les motifs avancés par le DFJP pour l'abrogation de la disposition ne peuvent qu'être qualifiés de fallacieux.

80 Proposition du DFJP au Conseil fédéral concernant la révision totale de l'ordonnance du 30.11.2001 sur le système de traitement des données relatives à la protection de l'Etat (ordonnance ISIS), p. 3 du texte allemand (non traduit).

81 Commentaire de la proposition du DFJP au Conseil fédéral concernant la révision totale de l'ordonnance du 30.11.2001 sur le système de traitement des données relatives à la protection de l'Etat (ordonnance ISIS), p. 4 du texte allemand (non traduit).

La DélCdG ne peut pas se borner à constater que l'assurance qualité n'a pas satisfait aux normes légales au cours des dix dernières années. Les contrôles systématiques sont un élément clé de la loi, par lequel Conseil fédéral et Parlement voulaient éviter que des données non conformes au droit et inutiles soient traitées dans le système de la protection de l'Etat.

La LMSI autorise d'une part également que soient réunies «des informations sur des personnes dont il s'avère ultérieurement qu'elles n'ont pas participé à une activité illicite»[82]. Cependant, comme le précisait aussi le Conseil fédéral dans son message relatif à la LMSI, la loi empêcherait que ne soient rassemblées des informations à la seule fin de les accumuler «tant que des règles restreignant les traitements (traitement interdit si le soupçon n'est pas confirmé; contrôle périodique des données; échéances légales, etc. […]) garantissent que seules seront traitées les données pouvant effectivement fournir des renseignements sur les dangers menaçant la sûreté intérieure et extérieure»[83]. Dans les délibérations relatives à la LMSI, la majorité des Chambres fédérale a non seulement suivi l'argumentation du Conseil fédéral, mais a intégré l'obligation de procéder à des contrôles périodiques des données à l'art. 15, al. 5, LMSI.

La promesse du Conseil fédéral et la volonté clairement exprimée du Parlement étaient d'accorder aux services de protection de l'Etat le droit de collecter des données à la condition qu'ils s'engagent en contrepartie à procéder à un contrôle qualité systématique. Tel était le modèle négocié dans la procédure démocratique pour une «protection de l'Etat réformée», comme l'avait déclaré le chef du DFJP le 5 juin 1996 devant le Conseil national. Il avait dit en substance que naguère, une grande quantité de matériel en fin de compte pas du tout pertinent pour la sûreté de l'Etat était collectée, que c'était la faute de l'ancien système de protection de l'Etat, et qu'aujourd'hui, grâce à la nouvelle loi et aux contrôles institués, nous avions de bonnes raisons de penser que seules seraient encore collectées les données revêtant de l'importance pour la protection de l'Etat.[84]

Aux yeux de la DélCdG, veiller à la sûreté est une mission essentielle de l'Etat. Cela confère à la protection de l'Etat non seulement le droit, mais l'obligation de collecter à titre préventif des informations sur les activités de certaines organisations et personnes. L'aspect déterminant est que la collecte de données doit aller de pair avec une appréciation continue de la pertinence de ces données et de l'opportunité de la poursuite de la collecte. Si ces conditions ne sont pas remplies, il faut pourvoir à l'effacement de ces données. C'est là le but qui sous-tend le contrôle qualité prescrit par la loi. Ni le SAP ni le DFJP n'ont satisfait à cette condition fondamentale inscrite dans la loi.

La DélCdG apprécie donc les problèmes d'exécution de l'art. 3, al. 2, LMSI mis au jour par l'OFJ à la lumière de l'incapacité du SAP de respecter les critères de qualité légaux. Les problèmes existants ne peuvent être résolus qu'à la condition que l'assurance qualité fonctionne de manière systématique et en parfaite conformité avec le droit. C'est un passage obligé pour avoir la garantie que des soupçons mi-

82 Message du 7.3.1994 concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire «S. o. S. – pour une Suisse sans police fouineuse» (FF **1994** II 1199).
83 Message du 7.3.1994 concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire «S. o. S. – pour une Suisse sans police fouineuse» (FF **1994** II 1199).
84 BO **1996** N 735 (CF Koller Arnold).

neurs ne soient pas saisis en lien avec une personne et qu'un examen sérieux soit fait pour confirmer ou dissiper un soupçon d'abus des droits politiques au service d'activités menaçant la sûreté de l'Etat. Une abrogation de l'art. 3, al. 2, LMSI ne saurait résoudre le problème tant que ce fonctionnement n'est pas garanti.

6.3 Doutes quant à la pertinence et à l'exactitude des données

On ne dispose pas d'informations fiables concernant la qualité effective des données dans ISIS-NT, vu que, dans la majorité des cas, le SAP n'a pas fait les contrôles de qualité prévus par la loi. La DélCdG doit donc fonder son appréciation sur les résultats de ses propres analyses par sondage concernant le fonctionnement du traitement des données au SAP.

La DélCdG a soumis les effacements qui lui ont été communiqués à une analyse approfondie. Rétrospectivement, on peut dire que la saisie initiale de la majeure partie des cas examinés n'était pas du tout justifiée ou que les enregistrements en question ont été conservés trop longtemps dans ISIS. Les cas couvrent un large éventail de menaces potentielles et le moment de leur saisie se répartit de manière relativement homogène sur les dix premières années d'ISIS.

Les effacements ont été faits à l'occasion des appréciations générales exécutées par le SAP vers la fin de 2008, lorsqu'il a repris cette activité. Depuis lors, le SAP n'a cependant pas réussi à diminuer significativement les retards accumulés sur le front des appréciations générales périodiques. Concernant la réduction de la grande majorité des cas en suspens, on est fondé à penser que, sur la base de ceux examinés par la DélCdG, un très grand nombre de cas doivent encore être effacés, soit que leurs informations n'ont jamais présenté une pertinence suffisante, soit qu'ils ont été conservés trop longtemps dans ISIS.

Il ressort de la statistique générale sur le stock de données qu'ISIS-NT ne compte même pas deux communications par individu enregistré avec le statut de personne revêtant en propre une importance pour la protection de l'Etat.[85] Les connaissances sur un grand nombre de personnes doivent par conséquent se limiter à une seule communication. Si cela ne veut pas forcément dire que les informations sont superficielles, le fait indique très probablement que des informations subséquentes manquent pour pouvoir effectivement motiver un éventuel soupçon. On peut aussi mettre en doute l'utilité d'une base d'information si ténue dans les échanges avec l'étranger. Dans bien des cas, la communication transmise à la demande d'un service étranger se limitera au constat que telle personne est ou n'est pas enregistrée. Parfois, cette simple mention peut cependant entraîner des conséquences fâcheuses pour la personne concernée.

La DélCdG émet aussi des réserves concernant la légalité des enregistrements d'une grande part des 83 000 personnes qui se sont accumulées dans ISIS-NT sous l'étiquette de «tiers». Il s'agit en particulier des quelque 52 000 personnes enregistrées à la suite d'un contrôle des photos d'identité. Dans le cadre de ce programme de recherches, les personnes d'une douzaine d'Etats font l'objet d'un enregistrement

[85] Selon un rapport du SRC du 26.3.2010, quelque 152 000 communications étaient stockées dans ISIS-NT.

lors de leur entrée et de leur sortie de Suisse. La liste des Etats couverts est au besoin actualisée par le Conseil fédéral.

Selon l'ordonnance, les tiers doivent toutefois avoir un lien avec un objet qui revêt de l'importance du point de vue de la protection de l'Etat (art. 3, let. i, ordonnance ISIS)[86]. Un tel lien ne peut pas être établi uniquement sur la nationalité et l'entrée en Suisse. Le lien doit pouvoir être attesté par une appréciation matérielle; autrement dit, il faut pouvoir exposer pourquoi la poursuite du traitement de ces données et un enregistrement nominal sont nécessaires. La DélCdG constate que le SAP a traité les données de dizaines de milliers de personnes, accumulant les informations sans dessein et sans disposer de la base légale pour ce faire.

Les règles mécaniques appliquées à la saisie et au traitement des données ont aussi contribué à la présence systématique de données non conformes aux prescriptions légales. Le passage du statut de tiers à celui de personne présentant en propre de l'importance du point de vue de la protection de l'Etat a donné lieu à des milliers d'entrées non pertinentes sous l'angle de la sûreté de l'Etat. Les instructions de saisie applicables aux «activistes violents» ont conduit la Section Analyse préliminaire à enregistrer des faits et des appréciations manifestement incorrects dans ISIS-NT.

La DélCdG ne partage pas non les vues du SAP lorsqu'il prétend que le système d'information de la protection de l'Etat n'est pas une liste de suspects et qu'il contient aussi des informations à décharge des personnes enregistrées. La délégation ne peut pas davantage suivre le SAP lorsqu'il déclare qu'il faudrait arrêter de considérer le fait d'être fiché comme une tare[87]. La DélCdG estime au contraire que les informations «positives» (c'est-à-dire *à décharge*) devraient obligatoirement donner lieu à l'effacement d'un enregistrement dans ISIS.

Aux yeux de la DélCdG, il n'est pas acceptable que les personnes pour lesquelles le SAP n'a par exemple pas eu d'objection concernant leur naturalisation restent dans ISIS. Inacceptable aussi le fait que les personnes qui ont été victimes d'un crime touchant à la sûreté de l'Etat – une prise d'otage par exemple – finissent par figurer avec référence nominale dans ISIS en raison de l'affaire en question. Dans ses contrôles par sondage, la DélCdG a trouvé des cas de ce type, qui, de plus, n'ont été effacés que plusieurs années après l'événement.

La DélCdG doute de la légalité de l'explication du SAP, qui estime que toutes ces informations qui lui parviennent doivent être saisies dans le système ISIS01 (Protection de l'Etat) pour pouvoir faire preuve de toutes ses activités ultérieurement. Si la DélCdG estime qu'il est important d'avoir une traçabilité de l'activité des autorités fédérales, il n'en reste pas moins que l'art. 15, al. 1, LMSI exige clairement et sans ambiguïté que les informations fausses et non pertinentes ne doivent pas être traitées, mais détruites. La loi part ainsi de l'idée que les organes de protection de l'Etat disposent d'informations qu'ils ne doivent pas traiter du tout ou qu'ils ne doivent plus traiter après un certain temps.

L'utilisation du système d'information de la protection de l'Etat comme vecteur documentaire est aussi en contradiction patente avec le but et l'esprit de la LMSI et dévoie la volonté du législateur au point d'arriver à produire un résultat contraire: le

86 Le 1.1.2010 le Conseil fédéral a abrogé l'ordonnance ISIS du 30.11.2001. Les dispositions de l'art. 3 de l'ordonnance ISIS ont été repris à l'art. 2 OSI-SRC.
87 Déclaration du directeur a.i. du SAP à l'audition du 19.5.2009.

simple fait que le SAP reçoive et traite une communication confère à cette information a priori la nécessaire pertinence du point de vue de la protection de l'Etat. Avec des données collectées selon ce principe, force est de constater, aux yeux de la DélCdG, que les informations figurant dans ISIS-NT ne sont pas toutes correctes et importantes et qu'elles ne satisfont donc pas aux critères de la LMSI.

En sa qualité d'organe de haute surveillance, la délégation a de bonnes raisons de penser que les données figurant ISIS-NT ne satisfont pas aux exigences légales de qualité. Ce constat a des conséquences graves car, en dernière analyse, cela signifie que ces données ne permettent pas de protéger l'Etat conformément à la loi.

L'état actuel des données dans ISIS remet aussi fondamentalement en cause l'utilité et l'efficacité de la protection de l'Etat. La collecte, le traitement et la conservation de données erronées et inutiles entravent un travail efficace au service de la sûreté intérieure. Cette situation peut déboucher sur des actions inappropriées et des pannes, lesquelles mettent en fin de compte la sûreté de l'Etat en danger.

6.4 Les mauvaises priorités du projet ISIS-NT

Au début de 2005, le SAP a mis en service le programme de banque de données pour ISIS-NT dans le délai prévu. Différentes fonction du programme, notamment dans le domaine de la maintenance des données, n'étaient à ce moment pas encore disponibles. De plus, la migration des données à partir de l'ancienne ISIS avait été mal préparée et le SAP a sous-estimé ou ignoré les conséquences en termes de gestion des données dans le nouveau système.

Après avoir déjà négligé la qualité des données dans l'ancienne ISIS, le SAP a méjugé leur importance pour une migration des données efficace vers ISIS-NT. Aucun effort n'a été déployé pour isoler et sortir du fichier avant la migration les informations qui n'étaient plus utiles. Comme le montrent les échantillons analysés par la DélCdG, un tel contrôle aurait été nécessaire car, aux yeux de la délégation, la majeure partie des cas n'auraient pas été assez importants sous l'angle de la protection de l'Etat pour justifier leur migration dans le nouveau système.

Mais les nombreux effacements non réalisés en raison des retards déjà accumulés dans l'ancien système au niveau des appréciations générales périodiques auraient dû appeler à eux seuls une vérification approfondie. Selon ses propres dires, le SAP estimait toutefois qu'un tiers des cas contrôlés pouvaient être effacés lors des appréciations générales périodiques.[88] Une part substantielle des quelque 76 000 personnes enregistrées qui auraient dû avoir fait l'objet d'une appréciation périodique avant la migration aurait donc dû être effacée.

Le SAP a repris dans le nouveau système ISIS-NT les données superflues, dont la conservation est donc illicite. Au lieu de rattraper les contrôles qualité et les effacements en suspens, il a procédé, pour l'ensemble des données migrées, à une mise au net gourmande en ressources, qui a fini par prendre quatre ans. Un examen de la qualité avant la migration aurait sans aucun doute permis au SAP d'avoir des fichiers de meilleure qualité à moindre coût.

88 V. réponse du Conseil fédéral du 5.9.2001 à la question ordinaire de Dardel, Jean-Nils «Personnes enregistrées dans les systèmes de données JANUS et ISIS» (01.1068).

De son côté, le DFJP n'a rien entrepris pour garantir en temps utile les ressources humaines nécessaires à une exploitation d'ISIS-NT conforme aux prescriptions légales. Le 16 juin 2004, dans sa proposition au Conseil fédéral, il avait pourtant estimé que du personnel supplémentaire serait nécessaire pour la saisie et la gestion des données. Mais il déclarait en même temps qu'il n'était pas en mesure de chiffrer les effectifs supplémentaires nécessaires pour garantir le respect des prescriptions légales dans le traitement des données, tout en précisant qu'il était disposé à libérer les postes nécessaires par des économies au SAP ou ailleurs au DFJP.

Ce faisant, le DFJP a évité une discussion au Conseil fédéral sur les frais de personnel potentiels du projet ISIS-NT et a pris seul la responsabilité de doter le service de traitement des données des ressources humaines qui permettraient son exécution conforme à la loi. Pour y parvenir, le DFJP aurait préalablement dû planifier le renforcement de la Section Assurance qualité. Compte tenu des 76 000 appréciations générales périodiques en souffrance dans l'ancien système ISIS, le manque d'effectif dans la Section Assurance qualité était non seulement avéré, mais aussi chiffrable.

Le SAP a longtemps sous-estimé le travail supplémentaire exigé par la mise au net des données après la migration. Une année et demie après le transfert des données, la fin des travaux de mise au net avait été annoncée à la DélCdG pour la fin de 2006. La mise au net n'a été achevée que deux années supplémentaires plus tard, après l'embauche en 2007 de personnel temporaire, qui ne disposait toutefois pas de qualifications préalables.

Le nouveau modèle de données d'ISIS-NT exigeait une démarche beaucoup plus précise et plus systématique pour la saisie des nouvelles informations, avec pour conséquence, outre l'accroissement du temps nécessaire à la saisie des données, des exigences accrues en ce qui concerne les compétences des collaborateurs de la Section Analyse préliminaire. De plus, le concept d'exploitation d'ISIS-NT commandait que les communications entrantes soient disponibles intégralement et sans délai dans le système pour les activités de renseignement de la Confédération et des cantons.

Le passage à ISIS-NT a placé la Section Analyse préliminaire devant de gros problèmes que le SAP n'avait pas anticipés. Ainsi, le SAP a mobilisé le personnel chargé de l'assurance qualité pour former et appuyer les collaborateurs de la Section Analyse préliminaire, ce qui a eu pour conséquence de suspendre les appréciations générales périodiques pendant presque quatre ans. La Section Assurance qualité se limitait aux contrôles initiaux, sans toutefois pouvoir les assurer sans défaut pour toutes les nouvelles communications.

Le problème des ressources foncièrement insuffisantes du SAP dans le domaine de l'assurance qualité s'est encore aggravé du fait de la croissance ininterrompue des stocks de données dans ISIS-NT. Au début de 2004, dans l'ancien système, on comptait environ 60 000 personnes revêtant de l'importance du point de vue de la protection de l'Etat et un nombre non déterminé de tiers. Six ans plus tard, le nombre des personnes présentant une importance directe pour la sûreté avait presque doublé pour atteindre près de 120 000 unités, et ISIS-NT contenait plus de 80 000 enregistrements de tiers. Au total, plus de 200 000 personnes sont donc aujourd'hui enregistrées dans ISIS-NT.

Le changement de statut de tiers lié à des automatismes non conformes à la loi dans les domaines de la mise au net et de la saisie des données a contribué au doublement du nombre des personnes revêtant en propre une importance pour la protection de

l'Etat. Mais la croissance du nombre d'institutions présentant de l'importance pour la sûreté n'est pas en reste: partant de 4780 entreprises et organisations revêtant une importance avérée pour la protection de l'Etat étaient enregistrées dans l'ancien système en 2004, il a doublé aujourd'hui.[89]

Si le nombre des tiers n'a pas diminué dans le même temps, cela tient aux deux personnes supplémentaires engagées par le SAP à partir de 2008 pour enregistrer dans ISIS-NT des dizaines de milliers de personnes en qualité de tiers sur la base des contrôles des photos d'identité. La décision de dégager des capacités de saisie supplémentaires pour le contrôle des photos d'identité apparaît peu judicieuse à la DélCdG, vu le manque patent de ressources de la Section Assurance qualité. En outre, le SAP n'arrivait toujours pas à traiter en temps utile les passages à la frontière, et l'entrée en vigueur de l'accord de Schengen a réduit d'autant les possibilités de relevé systématique des mouvements de voyageurs.

En investissant ses ressources en priorité dans la saisie des données, le SAP n'a pas seulement soustrait des capacités à la Section Assurance qualité, mais encore empêché l'effacement de milliers d'enregistrements ISIS – un facteur supplémentaire ayant contribué à faire gonfler le volume des données dans ISIS-NT.

Par ailleurs, du fait des structures relationnelles des données, l'effacement d'une personne enregistrée se révèle beaucoup plus lourd dans ISIS-NT que dans l'ancien système. Lorsqu'une personne est effacée à la suite d'une appréciation générale, les communications qui contiennent d'autres personnes enregistrées demeurent dans le système. Pour que la personne qui a fait l'objet d'un effacement ne puisse plus être trouvée par une recherche nominale, il faut donc aussi effacer son nom dans la brève synthèse de la communication, rédigée par la Section Analyse préliminaire. Or cette opération exige un travail manuel considérable, vu qu'un processus d'automatisation n'est possible que dans une certaine limite.

A cela vient s'ajouter le fait que, à partir de 2009, la Section Assurance qualité devait commencer à effacer systématiquement des informations dans ISIS. C'est à partir de ce moment que les premières données, saisies dans ISIS depuis 1994, ont atteint leur durée maximale de conservation de 15 ans. Dès lors, ce n'est plus seulement le doublement des enregistrements dans ISIS qui pèse sur les capacités de la Section Assurance qualité, mais encore l'augmentation – à la fois qualitative et quantitative – du travail requis par les effacements.

Sous le régime de l'ancienne ISIS, le SAP ne parvenait pas même à garantir l'assurance qualité alors qu'il devait gérer un volume de données deux fois moins important qu'aujourd'hui. Les ressources de la Section Assurance qualité n'ont pas augmenté sensiblement depuis. Avec les capacités et l'organisation actuelles du traitement des données, il n'est de fait pas possible de respecter les prescriptions de qualité de la LMSI, même si le personnel de la Section Assurance qualité pouvait se concentrer pleinement sur les contrôles initiaux et les appréciations générales périodiques. Rétrospectivement, la DélCdG ne peut que constater que le DFJP a mené le projet ISIS-NT d'une manière qui ne permettait pas un traitement des données conforme à la loi.

Il serait certes aujourd'hui possible de réduire la masse de cas en souffrance en augmentant les capacités de la Section Assurance qualité. Mais le problème de fond

89 Les chiffres de l'année 2004 sont tirés des statistiques sur l'état des principaux fichiers de personnes que fedpol a remis à la CAJ-N par courrier du 6.4.2004.

est que la charge de travail de la section est directement proportionnelle à la quantité des communications saisies. Tant que la quantité d'informations enregistrées dans le système de protection de l'Etat dépassera les capacités de contrôle matériel et, en dernière analyse, d'utilisation, la qualité des données ne sera pas garantie.

Lorsque que le chef du SAP déclare que le service n'exige pas de recevoir des données, mais qu'elles lui sont envoyées[90], cela met en lumière la nécessité de réduire la masse des données par un tri raisonné avant leur enregistrement dans ISIS-NT. Il faut que la qualité supplante la quantité dans le mécanisme de saisie des données.

Cet objectif ne peut être atteint qu'au prix d'un pilotage ciblé de l'afflux d'information. Les rapports des cantons, notamment, devraient être préparés d'emblée dans l'optique d'un classement électronique ultérieur. Au lieu d'un rapport volumineux couvrant tous les aspects d'une manifestation, il serait plus opportun de regrouper les renseignements obtenus dans des volets thématiques. Il faudrait aussi éviter à l'avenir d'établir de longues listes nominales totalement hétérogènes quant à l'importance des différentes personnes du point de vue de la protection de l'Etat. Cela faciliterait une maintenance nuancée et donc durable des différentes informations figurant dans ISIS.

La DélCdG est d'avis qu'il faut limiter les informations enregistrées dans le système de protection de l'Etat à raison de ce qui peut être examiné sous l'angle de sa pertinence pour la sûreté de l'Etat et contrôlé régulièrement conformément aux prescriptions légales. Ce critère se fonde sur l'objectif de légalité, mais aussi sur le fait que les données qui ne sont pas gérées sont en fin de compte inutiles.

La délégation estime qu'il est extrêmement important que les enseignements du projet ISIS-NT ne soient pas oubliés quand viendra l'heure d'un nouveau système. A ce moment-là, il faudra garantir que le système informatique comme son utilisation seront planifiés de sorte que toutes les conditions d'un traitement des données conforme au droit soient réunies.

6.5 Séparation des activités de protection de l'Etat et de conservation des données

Les deux rapports de la CEP-DFJP permettent de se faire une image de la façon dont les fichiers relatifs à la protection de l'Etat étaient gérés avant l'ère informatique. A l'époque, c'était le service de l'exploitation préliminaire qui était chargé de la saisie des informations collectées sur les fiches de la cartothèque. Ses collaborateurs avaient pour mission de résumer l'essentiel du contenu des rapports et communications fournis par les informateurs et d'en faire mention sur la fiche correspondante[91].

A l'introduction d'ISIS, la saisie des données est restée une tâche confiée au service d'exploitation. En sus, un service de contrôle interne[92] devait garantir la protection des données après la saisie des informations. Le législateur avait défini les critères pour ce faire à l'art. 15 LMSI. Lorsque la mission de protection de l'Etat est passée

90 Audition de la DélCdG du 18.11.2008.
91 Rapport de la CEP-DFJP du 22.11.1989 (FF **1990** I 776).
92 V. art. 6, al. 4, de l'ordonnance ISIS provisoire du 31.8.1992 et art. 9, al. 4 de l'ordonnance ISIS du 1.12.1999.

de la police fédérale au SAP, la structure de l'organisation a été maintenue, sous les dénominations Section Analyse préliminaire et service d'Assurance qualité.[93] La saisie était alors totalement séparée de l'assurance qualité, qui intervenait en aval avec un personnel différent. De même, la saisie et la maintenance des données d'ISIS-NT étaient distinctes de l'utilisation des données pour les activités de protection de l'Etat proprement dites.

Ainsi, certains collaborateurs du SAP qui étaient chargés du traitement des données dans ISIS ne travaillaient pas au niveau de la protection de l'Etat avec ces données et ne pouvaient donc pas juger en connaissance de cause de leur utilité et de leur pertinence pour la protection de l'Etat. Le personnel de la Section Analyse préliminaire, notamment, n'avait pas les connaissances nécessaires pour estimer de manière autonome l'importance d'une information pour la sûreté de la Suisse. Le libellé «analyse préliminaire» était déjà trompeur. La mission de ses collaborateurs se limitait à la représentation correcte des informations entrantes dans le modèle de données complexe d'ISIS-NT.

L'examen matériel qui aurait permis de déterminer si les informations enregistrées étaient pertinentes pour la sûreté de l'Etat n'était pas exigé de la Section Analyse préliminaire. Pire: la direction du SAP s'attachait à simplifier la mission de saisie par des règles mécaniques, notamment pour faire passer les tiers au statut de personne revêtant de l'importance pour la protection de l'Etat. Comme le montre l'enquête de la DélCdG, ces mécanismes se sont en fin de compte révélés être une tentative impropre de déterminer l'importance d'une information tout en faisant l'économie de leur examen par les collaborateurs de la Section Analyse préliminaire.

La DélCdG avait déjà constaté dans son rapport annuel 2007 que, au sein du SAP, «ce contrôle de la qualité constitue une tâche administrative effectuée en parallèle au travail d'analyse à proprement parler des services de renseignement»[94]. Contrairement à cette pratique, au SRS, ce sont les analystes – donc les personnes qui utiliseront les informations à des fins de renseignement – qui évaluent la fiabilité d'une information sur la base de la vue d'ensemble de toutes les données disponibles à ce moment-là et qui en tiennent compte dans leurs analyses. Comme il est ressorti de la visite de la DélCdG au SRS le 26 août 2009, les experts compétents décident aussi, sur la base de l'analyse, si une information doit présenter un lien nominal avec une personne dans une banque de données. Le fait que les analystes doivent en règle générale saisir les données eux-mêmes les pousse d'emblée à un arbitrage entre l'utilité de l'information et le travail requis par chaque saisie dans le système. Cette pratique a largement contribué à éviter que des informations probablement non pertinentes ne trouvent place dans les fichiers.

Au SAP, par contre, l'appréciation des informations finissait toujours par être de la responsabilité de la Section Assurance qualité, qui – après la saisie des données par la Section Analyse préliminaire – devait décider si elles respectaient les objectifs fixés par la LMSI. Pour les appréciations générales périodiques, il appartenait aussi à la Section Assurance qualité de décider si les informations étaient encore utiles aux autres utilisateurs d'ISIS, notamment ceux chargés de l'analyse. L'exécution des charges centrales qui devaient distinguer la protection de l'Etat «réformée» après

93 V. art. 10, al. 2 et 4 de l'ordonnance ISIS du 30.11.2001.
94 Rapport annuel 2007 des CdG et de la DélCdG des Chambres fédérales, du 25.1.2008 (FF **2008** 4579 4674)

l'affaire des fiches a donc été déléguée à moins d'une demi-douzaine de collaborateurs de la Section Assurance qualité.

Au bout du compte, les autres services du SAP ont ainsi été libérés de la responsabilité de devoir s'assurer qu'ils travaillent avec des données qui respectent les prescriptions légales. Ces services ne percevaient manifestement pas la qualité déficiente des données ISIS comme un problème. A la connaissance de la DélCdG, personne ne semble s'être plaint des déficiences grossières de la Section Analyse préliminaire dans la «transformation» des tiers ou de la présence dans ISIS d'informations totalement surannées et inutiles.

Du point de vue organisationnel, la Section Assurance qualité était indépendante des services qui utilisaient les informations d'ISIS-NT pour les activités de renseignement proprement dites. L'assurance qualité était toutefois subordonnée au même chef de division que la Section Analyse préliminaire, qui était chargée de la saisie des données dans ISIS-NT. La mobilisation de collaborateurs de la Section Assurance qualité pour faire le travail de la Section Analyse préliminaire a contribué de manière déterminante au fait que le personnel de la première n'a pas pu remplir sa mission légale.

La séparation organisationnelle entre l'assurance qualité et les services qui utilisaient les données ISIS n'était cependant pas couplée avec la compétence d'interdire l'accès aux données non contrôlées. Ainsi, les autres services du SAP pouvaient continuer d'utiliser et de traiter ce genre de données malgré leur qualité incertaine.

La DélCdG constate que le contrôle qualité du SAP était conçu et aménagé pour fonctionner par beau temps. Or les nuages s'étaient manifestement accumulés après l'introduction d'ISIS-NT. Aux yeux de la DélCdG, la responsabilité d'éviter que les données non conformes à la loi soient utilisables incombait au chef du SAP, de même que celle de pourvoir à ce qu'il soit remédié aux problèmes fondamentaux touchant à la qualité des données, dont il est établi qu'il avait connaissance.

Pour toute mesure, le SAP s'est limité à falsifier la date de la dernière appréciation générale périodique pour tous les enregistrements personnels transférés dans ISIS-NT à la migration. De fait, elle a été fixée globalement à une date arbitraire, quand bien même le contrôle ainsi signalé n'avait jamais eu lieu. Conjuguée à la modification de la règle de calcul de la date de la prochaine appréciation générale, cette pratique révèle un manque de volonté de remédier aux carences à la source.

La direction du SAP a par ailleurs aussi omis de s'intéresser systématiquement à la qualité des données et à la performance de la Section Assurance qualité. Comme il ressort du rapport d'inspection de la Surveillance SR, la Section Assurance qualité a cessé en 2008 d'établir des statistiques concernant les résultats des contrôles de la saisie parce que ces informations n'intéressaient manifestement personne.[95] Le SAP n'était pas non plus en mesure de suivre systématiquement le nombre des nouveaux enregistrements, des contrôles initiaux, des appréciations générales périodiques et des effacements dans ISIS-NT.[96] La DélCdG estime que la direction du SAP a

95 Rapport d'inspection de la Surveillance SR du DDPS du 22.2.2010 sur l'examen de la légalité du traitement des données dans le système ISIS-NT Protection de l'Etat du SAP, p. 18 du texte allemand (non traduit).

96 Lorsque la DélCdG, par lettre du 25.3.2010, a demandé la communication de ces données par trimestre, le directeur du SRC lui a répondu, en date du 12.4.2010, que la chose n'était pas possible en ce moment. Ce n'est qu'en été 2010 qu'ISIS-NT pourrait être programmée de sorte à permettre la livraison de ces chiffres.

manqué gravement à son obligation de surveillance interne. Le directeur de fedpol et le chef de département compétent n'ont pas non plus assumé leur mission de surveillance dans une mesure suffisante.

La DélCdG est convaincue qu'en matière de protection de l'Etat il ne faut pas séparer les activités relatives à la conservation et à la maintenance des données des autres activités préventives. Au contraire, la gestion des données doit faire partie intégrante de l'activité de protection de l'Etat proprement dite, sous peine de voir l'exploitation du système d'information de protection de l'Etat dévoyée comme une fin en soi.

6.6 Surveillance aux différents niveaux

6.6.1 Surveillance et conduite par le département

La loi prévoit un contrôle administratif particulier pour l'activité sensible de protection de l'Etat (art. 26, al. 1, LMSI), sans pour autant régler la forme de son organisation. A ce jour, les départements responsables ont confié la mission à un organe de contrôle ad hoc, qui sert au chef de département à assumer son obligation de surveillance, mais aussi de conduite en fin de compte. La DélCdG est consultée concernant le plan de contrôle annuel du chef du département (art. 26, al. 1, LMSI) et s'entretient chaque année avec l'organe de surveillance départemental.

Dans son enquête sur ISIS, la DélCdG a constaté que la coopération entre la haute surveillance et la surveillance exercée par le DDPS a fonctionné de manière exemplaire. Dans ses investigations, la délégation a pu s'appuyer, pour des points essentiels, sur les inspections de l'organe interne de surveillance, dont les résultats ont notamment aidé la DélCdG à confirmer différentes incohérences qu'elle avait mises au jour dans ses propres démarches.

Les résultats des enquêtes départementales ont aussi servi au PFPDT. A la demande de DélCdG, le DDPS a remis au préposé le rapport sur la légalité du traitement des données dans ISIS-NT. Pour chaque demande d'accès, le PFPDT est tenu d'examiner si les données concernant le demandeur qui, le cas échéant, figurent dans ISIS-NT sont traitées conformément à la loi.

La DélCdG salue le fait que, après le transfert du SAP, le DDPS ait entrepris sans délai le contrôle administratif prévu par la LMSI. Toutefois, elle attend maintenant que le DDPS mène à terme avant la fin de l'année la mise en place de son organe de surveillance et qu'il pourvoie effectivement les deux postes supplémentaires accordés par le Conseil fédéral.

Au cours de son enquête, la DélCdG a constaté que le SAP n'établissait que de manière irrégulière des statistiques sur les données de la protection de l'Etat, qui plus est souvent sur demande de la délégation. Comme l'ont montré de manière récurrente les rapports du SAP à l'intention de la DélCdG, la direction du SAP n'a pas déployé d'efforts pour avoir des chiffres fiables concernant le contrôle qualité. Ce manque de transparence n'a pas facilité la surveillance exercée sur le SAP. Le DDPS devrait donc veiller à ce que les services de protection de l'Etat produisent systématiquement les indicateurs nécessaires à la conduite au niveau départemental.

Une surveillance départementale ne peut produire ses effets sur la durée que si le chef du département utilise systématiquement cet instrument et lui confère le poids nécessaire. Ordonner des contrôles n'a en fin de compte un sens que dans la mesure

où le département est disposé à remédier aux insuffisances et dysfonctionnements constatés.

Le chef du DDPS doit s'acquitter d'une tâche exigeante: faire cesser le traitement des données non conformes à la loi et pourvoir à ce que seules soient enregistrées à l'avenir les données qui sont vraiment utiles pour les activités de renseignement dans le cadre effectif des prescriptions légales. Les problèmes diagnostiqués par la DélCdG plongent leurs racines dans l'organisation et les procédures sur lesquelles s'appuie l'exploitation d'ISIS-NT; ils ne peuvent pas être réglés par des seules mesures urgentes. Après la fusion du SRS et du SAP, les jalons sont déjà plantés pour le prochain projet de réforme du renseignement.

Comme l'a montré l'inspection de la DélCdG, le SAP a passé sous silence le caractère chronique des cas en suspens dans les appréciations générales périodiques à l'occasion de la première inspection sur le traitement des données dans ISIS-NT réalisée par l'inspectorat du DFJP en 2006. Jusqu'à la fin de 2008, le SAP a systématiquement évité de révéler à la DélCdG que les appréciations générales avaient été abandonnées depuis le début de 2005 en violation des prescriptions légales. Pendant cette période, dans ses déclarations tant orales qu'écrites, le SAP a au mieux minimisé cet état de fait, tenant même parfois un discours fallacieux.

Il appartient maintenant au chef du DDPS d'apporter rapidement les correctifs nécessaires. Il doit en outre rappeler clairement qu'une information ouverte vis-à-vis des organes de surveillance est indispensable.

6.6.2 La liste d'observation comme instrument de conduite du Conseil fédéral

Aux termes de l'art. 11 LMSI, le Conseil fédéral approuve chaque année la liste d'observation. Selon l'ordonnance, il faut que des indices établissent le bien-fondé des soupçons selon lesquels des organisations ou groupements mettent en péril la sûreté de la Suisse pour que le Conseil fédéral les mette sur la liste. Si ces conditions sont remplies, les services de protection de l'Etat sont autorisés à collecter toutes les informations sur les activités de ces organisations et de leurs protagonistes. Cela recouvre notamment aussi les informations concernant leur engagement politique, qui hors de ce cadre sont protégées par les limites de l'art. 3 LMSI. La loi prévoit que le département compétent doit porter chaque année la liste d'observation à la connaissance de la DélCdG.

La DélCdG a suivi de près l'évolution de la liste d'observation depuis l'entrée en vigueur de la LMSI. Le 17 novembre 2005, elle a invité le chef du DFJP à veiller à ce que soient établies chaque année sur la base des trois critères prévus par l'art. 17, al. 4, OMSI[97] les raisons pour lesquelles une organisation reste inscrite sur la liste. Depuis, le SAP a fait, pour chaque entrée de la liste d'observation, une mention des dispositions qui s'opposent à l'effacement. Ces indications n'étaient toutefois pas suffisantes pour comprendre les considérations matérielles qui ont présidé à cette décision.

97 Le Conseil fédéral a abrogé l'OMSI le 1.1.2010. Les dispositions de l'art. 17 OMSI sont depuis reprises à l'art. 27 de l'ordonnance du 4.12.2009 sur le Service de renseignement de la Confédération (OSRC; RS **121.1**).

Le Conseil fédéral a par exemple décidé, en septembre 2006, de maintenir l'organisation terroriste «Japanese Red Army» sur la liste d'observation. La chose n'a pas manqué d'étonner la DélCdG, qui avait constaté lors de sa visite inopinée du 28 août 2006 (v. chap. 2.3) que les dernières informations en date sur cette organisation dans ISIS remontaient à l'année 2001. Il était en outre de notoriété publique que le groupe, qui avait commis des attentats et des prises d'otages dans le monde entier dans les années 70 et 80, avait été déclaré dissous par l'une de ses dirigeantes, alors emprisonnée.

Dans ce contexte, la DélCdG a annoncé au chef du SAP à l'occasion d'une discussion en date du 10 octobre 2006, qu'elle exigerait une motivation détaillée justifiant la présence de cette organisation sur la liste, si elle devait encore y figurer l'année suivante. En 2007, à l'occasion d'une appréciation générale, le Conseil fédéral a retiré de la liste d'observation 18 groupes, parmi lesquels la «Japanese Red Army», dont la DélCdG avait remis en cause la présence sur la liste.

A sa séance du 10 octobre 2006, la DélCdG s'est fait expliquer le fonctionnement des listes internationales sur la base desquelles les Nations Unies et l'Union européenne (UE) désignent les organisations et groupements terroristes. La liste de l'UE, contrairement à la liste d'observation suisse, n'est pas confidentielle. Comme la DélCdG l'apprit à cette occasion, la participation à l'une des entités figurant sur la liste de l'UE est en soi interdite et punissable. Le chef du SAP a précisé que, pour pouvoir coopérer de manière cohérente avec les services partenaires étrangers, le SAP est convenu avec ses collègues européens qu'il s'attacherait à intégrer tous les groupements de la liste européennes dans son mandat, et donc aussi à la liste d'observation.

Les explications du chef du SAP ont en outre permis à la DélCdG de mieux comprendre comment le critère de la menace pour la sûreté intérieure ou extérieure prévu à l'art. 11, al. 2, let. b, LMSI était interprété concrètement: selon les déclarations du chef du SAP, une organisation qui avait tué des touristes suisses dans un attentat à l'étranger remplissait les conditions pour être intégrée à la liste d'observation.

La liste d'observation est le principal moyen à la disposition du Conseil fédéral pour influer sur l'activité de la protection de l'Etat. La DélCdG a constaté que le Conseil fédéral a régulièrement approuvé des modifications apportées à la liste ces dernières années. Au fil des cinq dernières années, 18 groupes sont venus s'ajouter à la liste, tandis que 29 en ont été retirés. Pour l'essentiel, les suppressions ont été faites à l'occasion de l'appréciation générale quadriennale prévue par l'ordonnance (art. 17, al. 3, OMSI).

La DélCdG ne dispose d'aucun élément indiquant que les délibérations du Conseil fédéral relatives à la liste d'observation aient débouché sur l'intégration ou le retrait d'organisations. Avant d'être soumise au Conseil fédéral, la liste d'observation est en règle générale transmise à la Délégation du Conseil fédéral pour la sécurité, qui en prend acte. Cette prise de connaissance, qui peut prendre différentes formes, peut précéder une consultation dans le cadre de l'Organe de direction pour la sécurité.

Se fondant sur des instructions internes du département[98], l'inspectorat du DFJP et, depuis une date plus récente, la Surveillance SR du DDPS accompagnent chaque

98 Directives du chef du DDPS du 18.12.2008 relatives aux rapports concernant les activités de maintien de la sûreté intérieure selon la LMSI (non traduit).

année la procédure d'actualisation de la liste d'observation, avec pour conséquence notamment que le SAP a dû mieux documenter ses bases d'information. Toutefois, la décision de faire figurer ou non une organisation sur la liste d'observation reste en dernière analyse du ressort du SAP, respectivement du département responsable.

De l'avis de la DélCdG, le Conseil fédéral ne met pas assez à profit «cet examen honnête et cette approbation de cette liste positive» pour «garantir la conduite politique de la police préventive»[99], comme le chef du DFJP l'avait prôné lors du débat du 5 juin 1996 relatif à la LMSI. La conduite de la protection de l'Etat, qui est une tâche délicate du point de vue politique, ne peut pas être laissée aux seuls soins du département compétent ou d'un office.

Le législateur a laissé au Conseil fédéral la décision de savoir quand l'intérêt public commande de déroger aux «garanties inscrites dans la [LMSI] d'un exercice des droits politiques largement exempt de surveillance»[100]. Le Conseil fédéral devrait donc prendre ce genre de décision en s'appuyant sur une appréciation matérielle fondée. Le fait qu'une organisation figure sur une liste de l'UE ou des Nations Unies, par exemple, ne saurait exonérer le Conseil fédéral d'une telle appréciation.

6.6.3 Surveillance dans les cantons

La requête de la CdG-BS a donné des impulsions notables à la haute surveillance parlementaire, l'une d'elles prenant la forme d'une réflexion approfondie sur les limites de l'art. 3 LMSI au sein de DélCdG. La délégation salue donc expressément les efforts déployés par la CdG-BS pour faire usage de ses droits de surveillance.

La DélCdG salue également le fait que le gouvernement de Bâle-Ville se soit engagé résolument pour partager la responsabilité politique des activités de la sûreté cantonale. Les visites de la DélCdG dans les cantons ont montré qu'un intérêt régulier des autorités politiques pour les activités des organes de protection de l'Etat ne pouvait avoir que des conséquences positives sur le travail de ces derniers.

Mais la DélCdG constate aussi que, par le passé, le SAP s'est peu employé à soutenir les cantons pour qu'ils assument leurs droits de surveillance. Lorsque, dans un cas concret, la CdG-BS a voulu faire des contrôles, le SAP a même fait usage du droit que lui conférait l'ordonnance pour empêcher abusivement la surveillance cantonale.

Le chef du DDPS et le directeur du Département de la justice et de la sûreté du canton de Bâle-Ville ont entre-temps pris les dispositions pour que soit trouvée, sous l'égide de la CCDJP, une solution viable permettant une surveillance par les organes exécutifs cantonaux. La DélCdG soutient cette solution, qui relativise l'exigence de l'assentiment du SAP qui a prévalu jusqu'ici. Les gouvernements cantonaux peuvent désormais exiger que, lorsque l'accès aux données est refusé, le cas soit soumis au chef du DDPS et, éventuellement, porté devant le TF.

Selon l'avis de l'OFJ, le régime juridique actuel n'exclut pas une surveillance par les législatifs cantonaux, même si le cas de figure n'est pas prévu explicitement par la LMSI. Au-delà du cas de la CdG-BS, la DélCdG a connaissance d'autres organes parlementaires cantonaux qui se penchent sur la question de la surveillance de la

99 BO **1996** N 719 (CF Koller Arnold) (en allemand).
100 Avis de l'OFJ du 2.6.2009, p. 13.

protection de l'Etat. La CdG du Grand Conseil du canton de Bâle-Campagne, par exemple, s'est aussi adressée à la délégation à ce propos.

La solution mise au point sous l'égide de la CCDJP donne la possibilité aux organes assumant la haute surveillance cantonale de vérifier, en application du droit cantonal, si l'organe de contrôle du gouvernement cantonal assume sa mission correctement. Lorsque l'exécutif cantonal n'a toutefois pas institué d'organe de contrôle, le législatif cantonal devrait s'adresser directement aux autorités fédérales compétentes, qui, en vertu de l'art. 17, al. 1, LMSI, gardent la compétence pour autoriser ou refuser l'accès aux données de la protection de l'Etat.

Une telle procédure apparaît toutefois problématique à la DélCdG en ce sens que la haute surveillance du Parlement cantonal serait exercée en court-circuitant le gouvernement du canton. La DélCdG est d'avis que les Parlements cantonaux qui veulent exercer eux-mêmes la haute surveillance sur les organes de la sûreté de leur canton devraient créer les conditions nécessaires à cet effet, en commençant par instituer un contrôle adéquat par le gouvernement cantonal.

6.6.4 Droit d'accès des personnes directement concernées

L'enquête de la DélCdG a montré que l'exercice du droit d'accès par des particuliers a apporté une contribution non négligeable au contrôle de la légalité du traitement des données dans ISIS. C'est grâce à des demandes concrètes que le PFPDT a pu exercer avec une plus grande efficacité sa fonction de surveillance prévue à l'art. 27 LPD. Ce sont en particulier les requérants qui, en parallèle, ont saisi le TAF ou, autrefois, la CFPD, qui ont contribué à pousser le SAP à améliorer la légalité du traitement des données dans ISIS.

Les décisions de la CFPD ont notamment fait en sorte que soit soulevée la question de la conformité du droit d'accès indirect avec la CEDH. De plus, le TAF a constaté que l'art. 18 LMSI est en fait applicable uniquement à la banque de données Protection de l'Etat (ISIS01), et a recommandé que la banque de données Administration (ISIS02) soit soumise à la loi sur la protection des données. La DélCdG appuie cette recommandation, dont la mise en œuvre avait été annoncée par le SAP.

De l'avis de la DélCdG, le droit d'accès indirect prévu à l'art. 18 LMSI ne satisfait pas aux dispositions de la CEDH. Ce point de vue est partagé par le Conseil fédéral dans sa réponse à la motion Leutenegger-Oberholzer[101], où il propose de développer le droit d'accès selon la LMSI dans la direction de l'art. 8 LSIP (v. chap. 4.3). La DélCdG suit le Conseil fédéral sur ce point.

La volonté de réviser l'art. 18 LMSI dans le sens de la LSIP paraît défendable à la DélCdG, vu que le Conseil fédéral a soumis, sur proposition du DDPS, les informations obtenues de l'étranger au droit de surveillance ordinaire de la loi sur la protection des données. Ce pas a été franchi avec l'adoption de l'art. 23 de l'ordonnance sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC)[102], entrée en vigueur le 1er janvier 2010.

101 Motion 08.3852 «Fichiers de la Confédération. Droit d'accès» du 17.12.2008.
102 Ordonnance du 4.12.2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC; RS **121.2**).

7 Recommandations de la DélCdG

L'enquête de la DélCdG s'est concentrée sur le traitement des données dans ISIS-NT jusqu'au moment de la fusion du SAP et du SRS au début de 2010. Les constatations de la délégation demeurent néanmoins valables pour le SRC, car celui-ci a repris pour l'essentiel les structures de l'organisation et le personnel du SAP pour le traitement des données selon la LMSI. Dans le même temps, les dispositions pertinentes de l'ordonnance ISIS ont été reprises dans la nouvelle OSI-SRC.

Cette nouvelle ordonnance règle aussi le traitement des informations collectées selon les tâches de l'ancien SRS (art. 1, let. a, LFRC). L'art. 21, al. 2, OSI-SRC prévoit d'étendre la compétence de la Section Analyse préliminaire à la saisie d'informations recherchées par des moyens de renseignement à l'étranger dans les banques de données. Ce qui fait que le modèle de traitement des données du SAP est maintenant appliqué à l'ensemble du SRC.

Pour remédier aux problèmes que l'inspection a mis en lumière, la DélCdG formule les recommandations suivantes à l'intention du Conseil fédéral et du DDPS:

Recommandation 1: La DélCdG recommande au DDPS de verrouiller provisoirement l'accès à toutes les données saisies dans ISIS depuis cinq ans ou plus et qui n'ont pas fait l'objet d'une appréciation générale depuis. Le Conseil fédéral est invité à désigner un préposé à la protection des données externe, qui décidera, sur proposition du SRC et en temps utile, de la réouverture de l'accès aux données verrouillées ou de leur effacement. Avant une décision du préposé, les informations verrouillées sur les personnes enregistrées devront être accessibles uniquement à l'assurance qualité interne du SRC. Les vérifications en souffrance devront être faites avant le milieu de 2012, en tous les cas au plus tard à la migration vers le système appelé à succéder à ISIS-NT. Le préposé présente un rapport semestriel au Conseil fédéral.

Recommandation 2: La DélCdG recommande au DDPS de faire effacer tous les tiers saisis dans ISIS-NT sur la seule foi du programme de recherches fondé sur le contrôle des photos d'identité.

Recommandation 3: La DélCdG recommande au DDPS de redéfinir l'allocation des ressources en personnel au sein du SRC dans le cadre d'un projet formel. Les ressources doivent être engagées de sorte que seules soient saisies dans ISIS-NT les informations dont la pertinence du point de vue de la protection de l'Etat a effectivement été examinée à la saisie et qui peuvent faire l'objet d'une appréciation régulière conformément aux prescriptions légales.

Recommandation 4: La DélCdG exige du DDPS un rapport qui expose la manière dont les compétences d'analyse du personnel peuvent être mises au service de l'appréciation afin d'éviter la saisie dans ISIS-NT d'informations inexactes et non pertinentes et de garantir l'effacement en temps utile des données qui ne sont plus nécessaires.

Recommandation 5: La DélCdG exige du DDPS un rapport qui expose la manière dont l'attribution des mandats aux organes de sûreté des cantons peut être améliorée et comment les cantons peuvent contribuer à la saisie d'informations utiles dans ISIS-NT.

Recommandation 6: La DélCdG recommande au DDPS 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» (art. 25, al. 1, let. a, OSI-SRC), à l'exclusion des données administratives.

Recommandation 7: La DélCdG recommande au Conseil fédéral de proposer aux Chambres fédérales une définition légale claire des «tiers» dans les travaux de révision de la LMSI actuellement en cours. La définition retenue doit empêcher l'accumulation sans dessein de données personnelles ne revêtant aucune importance pour la protection de l'Etat.

Recommandation 8: La DélCdG recommande 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.

Recommandation 9: La DélCdG recommande au DDPS de revoir les directives régissant la saisie des données dans ISIS et de supprimer toutes les règles qui permettent l'enregistrement d'une personne dans ISIS sans appréciation matérielle de l'ensemble des informations qui la concernent.

Recommandation 10: La DélCdG recommande au Conseil fédéral de soumettre tous les fichiers d'ISIS aux dispositions des art. 8 et 9 LPD, à l'exception de la banque de données «ISIS01 Protection de l'Etat» (art. 25, al. 1, let. a, OSI-SRC).

Recommandation 11: La DélCdG recommande au Conseil fédéral de proposer aux Chambres fédérales de remplacer l'actuel droit d'accès indirect par un droit d'accès selon les modalités visées à l'art. 8 LSIP dans les travaux de révision relatifs à l'art. 18 LMSI actuellement en cours.

Recommandation 12: La DélCdG recommande au Conseil fédéral d'abandonner le programme préventif de recherches fondé sur le contrôle des photos passeport. Si le Conseil fédéral décide de poursuivre le programme, il doit présenter un rapport justifiant ce choix. Le cas échéant, le rapport devra mettre en lumière l'utilité et l'efficacité du contrôle des photos passeport, et prendre position en particulier sur le rapport entre le volume de travail requis par le programme et sa contribution à l'accomplissement de la mission de protection de l'Etat, prévue à l'art. 2 LMSI. Il devra en outre se prononcer sur la compatibilité du programme avec les accords de Schengen et de Dublin.

Recommandation 13: La DélCdG recommande au DDPS de définir des indicateurs sur la base desquels le département pourra procéder à un examen de plausibilité pour déterminer si l'assurance qualité fonctionne conformément aux prescriptions légales.

Recommandation 14: La DélCdG recommande 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 15: La DélCdG recommande au DDPS de renforcer le personnel de la Surveillance SR jusqu'à la fin de 2010, conformément aux assurances données par le Conseil fédéral à la DélCdG en décembre 2008.

Recommandation 16: La DélCdG recommande au DDPS, dans la perspective de la future banque de données ISIS, d'analyser systématiquement les exigences légales et de ne mettre en exploitation un nouveau système que s'il satisfait intégralement aux

prescriptions légales. Par ailleurs, seules les données qui remplissent tous les critères de l'art. 15 LMSI doivent être transférées.

Recommandation 17: La DélCdG exige du DDPS un rapport sur les possibilités techniques actuelles et à venir pour accéder à des données électroniques via une recherche orientée personne. Le rapport devra donner les bases permettant de déterminer les possibilités techniques qui peuvent être utilisées en respectant les art. 3 et 5 LMSI. Le rapport devra être établi hors de l'administration et se fonder sur l'état actuel des connaissances académiques.

8 Suite de la procédure

La Délégation des commissions de gestion invite le Conseil fédéral à prendre position sur le présent rapport et les recommandations qu'il contient d'ici à *fin octobre 2010*.

21 juin 2010

Au nom de la Délégation des commissions de gestion

Le président:
Claude Janiak, député au Conseil des Etats

La secrétaire:
Beatrice Meli Andres

Les commissions de gestion du Conseil des Etats et du Conseil national ont pris acte du présent rapport et approuvé sa publication.

30 juin 2010

Au nom des commissions de gestion

Le président de la Commission de gestion
du Conseil des Etats:
Claude Janiak, député au Conseil des Etats

La présidente de la Commission de gestion du
Conseil national:
Maria Roth-Bernasconi, conseillère nationale

Liste des personnes entendues au cours de l'inspection

Bühler, Jürg	Chef suppléant SAP, directeur a.i. SAP
Buntschu, Marc	Chef Unité 2, secrétariat du PFPDT
Bourquin, Gilles	Sous-chef Etat Major Renseignements, Police cantonale de Genève
Chevalier, Mario	Sous-chef Etat Major Opérations, Police cantonale de Genève
Gass, Hanspeter	Chef Département de la justice et de la sûreté, canton de Bâle-Ville
Gloor Scheidegger, Caroline	Conseillère juridique, secrétariat du PFPDT
Greiner, Daniel	Chef suppl. Gestion de l'information, SAP
Gudet, Charles	Chef inspection Surveillance SR, DDPS
Hug, Thomas	Procureur général, Ministère public du canton de Bâle-Ville
Kipfer, Christoph	Chef Division judiciaire, Police cantonale bernoise
Kronig, Philipp	Chef Gestion de l'information, SAP
Liechti, Michel	Chef Surveillance SR, DDPS
Mader, Luzius	Vice-directeur OFJ
Maurer, Ueli	Chef du DDPS
Möschli, Jörg	Chef Unité spéciale 9, Ministère public du canton de Bâle-Ville
Rebord, Raphaël	Chef Etat Major, Police cantonale de Genève
Riesen, Hans-Rudolf	Chef Section Assurance qualité, SAP
Rüegsegger, Kurt	CSI-DFJP
Rüegsegger, Paul	Chef Division Protection de l'Etat, Police cantonale bernoise
Schönbett, Frédéric	Conseiller juridique, secrétariat du PFPDT
Thibault, Gilles	Chef Brigade de la sûreté intérieure, Police cantonale de Genève
Thür, Hanspeter	Préposé fédéral à la protection des données et à la transparence
Von Daeniken, Urs	Chef SAP
Voser, Beat	Commissaire en chef, Ministère public du canton de Bâle-Ville