Mise en place de liaisons «Online» dans le domaine de la police

Rapport de la Commission de gestion du Conseil des Etats

du 19 novembre 1998

Rapport

1 Introduction

11 Problématique

Le phénomène de la multiplication des moyens informatiques mis à la disposition des autorités fédérales pour l'accomplissement de leurs tâches légales a entraîné, notamment dans le domaine de la police, la mise en place d'un nombre toujours plus important de liaisons «online» («en ligne»; «par procédure d'appel») habilitant de nombreuses autorités à accéder directement à différentes banques de données.

Afin de permettre une approche plus explicite et visuelle de cette problématique, un schéma représentatif de quelques systèmes informatiques de police a été élaboré (*source:* 1er rapport d'activités 93/94 du Préposé fédéral à la protection des données / *mise à jour de l'OPCA – janvier 1998*). Ce schéma illustre l'ampleur des liaisons «online» existantes ou envisagées en faveur de nombreuses autorités. Il ne constitue qu'un extrait de l'ensemble des systèmes de l'administration fédérale.

Les liaisons «online» retranscrites sur ce schéma ne représentent pas toutes des accès à l'intégralité des données d'un système. De nombreuses liaisons ne permettent en fait l'accès qu'à une partie des données d'un système, en fonction de la matrice d'accès. Parmi toutes les liaisons représentées, certaines sont effectives, certaines peuvent être autorisées sur la base de lois ou d'ordonnances en vigueur, les autres sont envisagées dans le cadre de projets législatifs.

La loi fédérale sur la protection des données prévoit que les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale à cet effet. Elle stipule en outre qu'un organe fédéral n'est en droit de rendre des données personnelles accessibles au moyen d'une procédure d'appel («online») que si cela est prévu expressément; de plus, cette exigence doit être remplie au niveau d'une loi au sens formel lorsque la liaison en ligne permet l'accès à des données sensibles ou à des profils de la personnalité.

L'Office fédéral de la justice et le Préposé fédéral à la protection des données (PFPD), dans des positions exprimées lors de procédures de consultation, avis de droit ou conférences de presse, ont été amenés à différentes reprises à rappeler que ces exigences doivent être respectées pour tout traitement de données personnelles. Or, ces dernières années de nombreuses autorités fédérales ont voulu accéder à un nombre croissant de systèmes d'informations. Cette tendance a entraîné la création de bases légales permettant de justifier toute sorte d'accès, notamment dans le secteur de la police.

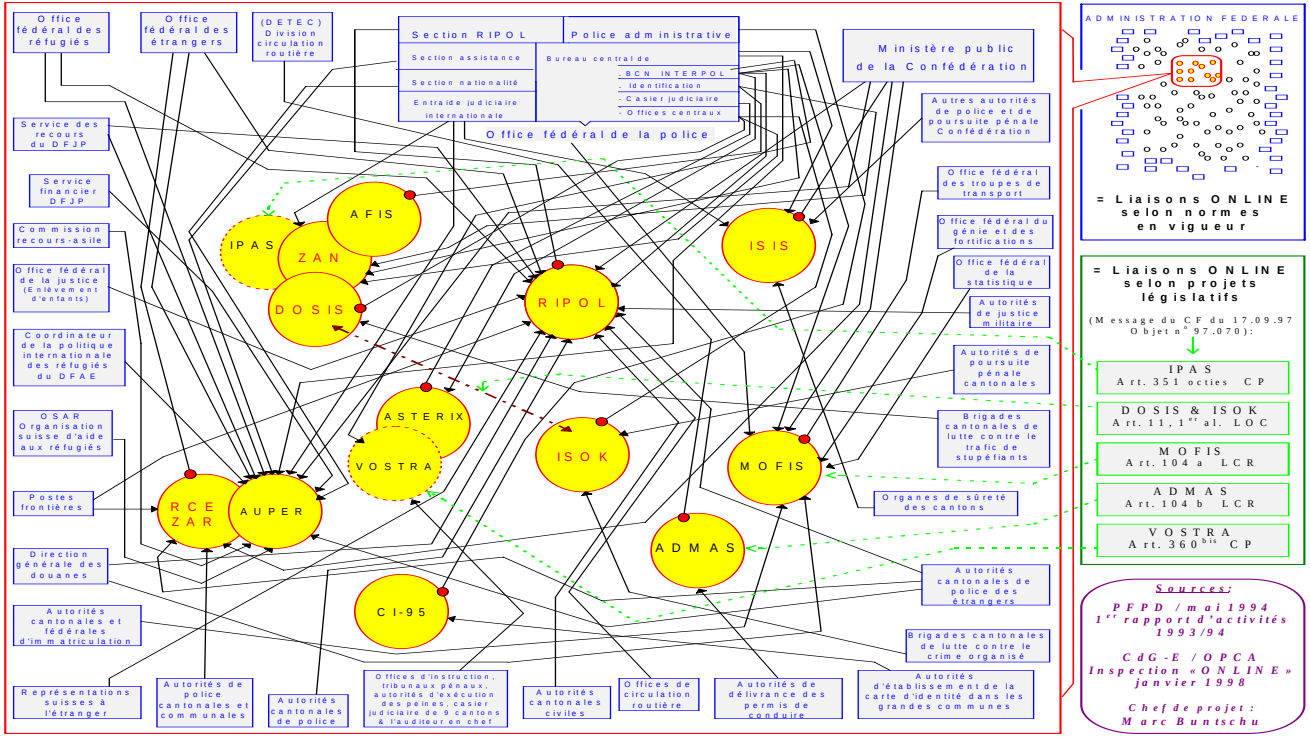
Si le principe de légalité a pour objectif premier la transparence, il ne suffit pas à lui seul à légitimer ces accès. La mise en place d'une liaison online doit être précédée d'un examen de sa nécessité, de ses coûts et de sa conformité aux principes de proportionnalité, de-

finalité et d'opportunité. En d'autres termes, les accès en ligne doivent également être conformes à ces principes et ne peuvent pas uniquement être prévus ou justifiés dans des bases légales. Cette problématique a également été mise en évidence au niveau cantonal[1] .

[1] «Ce souci s'avère particulièrement en ce qui concerne les procédures d'appel: face à la tendance qui existe actuellement de les généraliser au sein de l'administration, la commission a souhaité qu'une réflexion fondamentale soit entreprise et que le Gouvernement ne se contente pas de proposer au Grand Conseil l'adoption d'une base légale ponctuelle chaque fois qu'une nouvelle liaison informatique est mise en place» (cf. Rapport sur l'activité de l'Autorité cantonale fribourgeoise de surveillance en matière de protection des données, juillet 95 – déc. 96, p. 7).

Inspection «ONLINE» / (Mise en place des liaisons «online» dans le domaine de la police)

Inspection de la Commission de gestion du Conseil des Etats & de l'Organe parlementaire de contrôle de l'administration



12 Mandat des commissions de gestion

Dans le cadre de leur programme annuel 1998, les Commissions de gestion ont décidé de réaliser une inspection relative à la «mise en place de liaisons ‹online› dans le domaine de la police».

La section «Autorités» de la Commission de gestion du Conseil des Etats, chargée de réaliser l'inspection, a relevé différents objectifs devant être poursuivis dans le cadre de son enquête, notamment un examen au niveau conceptuel et un examen de la pratique actuelle (rapport d'expert, voir annexe I)[2].

L'enquête a d'abord pour objectif de déterminer les exigences légales et conceptuelles actuellement en vigueur dans le cadre de la mise en place des liaisons «online». Il constitue la partie théorique de l'inspection et a un caractère général quant à l'examen des exigences conceptuelles, des aspects liés à la protection des données et du respect, au niveau conceptuel déjà, des exigences de proportionnalité, de finalité et d'opportunité.

Le rapport d'expert vise à prendre en compte la pratique de l'administration fédérale dans la mise en place d'accès en ligne dès la conception d'un système ainsi que l'octroi de nouveaux accès en ligne aux autorités fédérales et cantonales.

13 Organisation et déroulement des travaux

131 Organisation

La section s'est organisée de la manière suivante:

Président:	CE Pierre Aeby
Membres:	CE Hans Danioth; CE Bruno Frick (jusqu' à fin 1997); CE Hans Hess (dès juin 1998), CE Andreas Iten; CE Franz Wicki; CE Kaspar Rhyner (jusqu' à fin mai 1998)
Secrétariat:	Mariangela Wallimann-Bornatico, secrétaire des CdG

Organe parlementaire de contrôle de l'administration (OPCA): Marc Buntschu

Expert mandaté: Lukas Fässler, avocat et expert en informatique.

132 Déroulement des travaux

Réunie le 8 avril 1997, la section «Autorités» a examiné cette problématique sur la base d'un document de travail rédigé par l'Organe parlementaire de contrôle de l'administration (OPCA). Reconnaissant la nécessité de poursuivre ses investigations, elle en a informé le Conseil fédéral par lettre du 10 avril 1997.

Après avoir pris connaissance, le 27 juin 1997, de l'esquisse de projet de l'OPCA, la section a approuvé, dans le cadre d'une étude de faisabilité, la délimitation de son enquête ainsi que son calendrier, ses aspects organisationnels et les questions qu'elle entendait traiter.

[2] Le rapport d'expert n'est pas publié dans la Feuille fédérale. Des tirés à part peuvent être obtenus auprès du Secrétariat des commissions de gestion, 3003 Berne.

Fin mars 1998, l'OPCA a déposé un document de travail. Le 6 mai 1998, l'expert mandaté a soumis oralement ses premières conclusions à la section qui, à sa séance plénière des 25 et 26 mai 1998, a informé la Commission de gestion du Conseil des Etats des premiers résultats de l'inspection. Après avoir consulté les offices concernés, l'expert mandaté a déposé son rapport définitif le 31 juillet 1998.

Le 2 septembre 1998, la section a examiné pour la première fois les résultats de l'investigation. Après un deuxième examen, elle a fait parvenir un projet de rapport au chef du DFJP et à celui du DFF en sollicitant leur avis. Elle a ensuite discuté de la position de ces départements en présence du conseiller fédéral Arnold Koller à sa séance du 5 novembre 1998. La section a également entendu le Préposé fédéral à la protection des données.

La section a rendu son rapport final à la Commission de gestion du Conseil des Etats, qui l'a adopté le 19 novembre 1998.

133 Relations avec l'administration fédérale

Tant l'OPCA que l'expert mandaté ont souligné que la collaboration avec les offices concernés du Département de justice et police avait été intéressante et constructive. Certaines des améliorations proposées par l'expert dans un premier document de travail ont déjà pu être réalisées, du moins en partie.

134 Indépendance des membres de la section

Les membres de la section «Autorités» confirment qu'ils n'ont aucun lien, ni de nature privée, ni de nature professionnelle, susceptible d'interférer avec les questions soulevées dans le présent rapport.

14 Cadre méthodologique

141 Méthodes utilisées

L' OPCA et l'expert ont commencé par procéder à un état des lieux. A cette fin, les services concernés leur ont fourni les documents suivants:

- liste des réglementations en vigueur touchant à la mise en place de liaisons informatiques «online» (lois au sens formel, ordonnances d'exécution, directives d'application, directives techniques, directives de sécurité, manuels d'application, procédures d'utilisation, standards de conduite et de déroulement de projets informatiques, mesures de controlling, etc.);
- documents relatifs au développement des systèmes informatiques analysés (dossiers d'initialisation, analyses préliminaires, concepts, réalisations, mises en œuvre, nouvelles évolutions);
- bases légales créées pour ces systèmes et leurs *accès (lois, ordonnances, directives, règlements, matrices d'accès).*

Les Offices concernés ont aussi été priés de présenter par écrit la liste des liaisons «online» de leur système informatique, avec les autorités habilitées à y accéder, ainsi

que *l'historique* du développement du système et de la mise en place des différentes liaisons «online» en question; ils ont aussi été appelés à donner leur point de vue par écrit sur les problèmes survenus lors de la mise en place des différentes liaisons «online» de leurs systèmes informatiques respectifs.

Après avoir procédé à une *analyse des documents* en question, *des entretiens* avec des représentants de certains services ont été organisés et des *avis écrits complémentaires* ont été demandés.

142 Interlocuteurs

Les interlocuteurs retenus dans le cadre de cette inspection ont avant tout été les organes et les offices impliqués dans la mise en place de liaisons «online» actuelles ou futures permettant d'accéder aux systèmes informatiques choisis par la section. Il s'agit notamment:

- de l'Office fédéral de la police,
- du Ministère public de la Confédération,
- de l'Office fédéral des étrangers et des autorités cantonales connectées en ligne aux systèmes informatiques choisis ou pour lesquelles des accès sont envisagés,
- de l'Office fédéral de l'informatique,
- des Secrétariats généraux du DFJP et du DFF,
- du centre de calcul du DFJP,
- du conseiller à la protection des données du DFJP,
- du Préposé fédéral à la protection des données.

Une étroite collaboration a également été mise en place avec le Service de contrôle administratif du Conseil fédéral (CCF), rattaché à la Chancellerie fédérale, qui a reçu mandat d'examiner *«les échanges de données en ligne entre les cantons et la Confédération»* (= projet CCF 29 / *«Online-Datenaustausch zwischen Bund und Kantonen»*[3]. Son rapport a été publié le 16 mars 1998.

143 Contenu du rapport

Ce rapport ne prétend pas traiter de manière exhaustive tous les problèmes relatifs à la mise en place des liaisons «online», la question étant fort vaste et fort complexe. Il se concentre sur les aspects conceptuels et juridiques, ainsi que sur les questions de protection des données.

Les résultats des recherches sur lesquels s'appuient les recommandations de la CdG-E devraient permettre de garantir une mise en place plus adéquate des liaisons informatiques «online» en général, notamment dans le domaine de la police.

[3] cf. Rapport du service de contrôle administratif du Conseil fédéral du 16 mars 1998 «Online-Datenaustausch zwischen Bund und Kantonen»

15 Choix des systèmes informatiques

La section s'est penchée sur plusieurs systèmes susceptibles d'être examinés [RIPOL, DOSIS, ISIS, ZAN, AFIS, RCE, AUPER]. Elle a établi plusieurs critères devant être pris en compte pour le choix définitif, en particulier: les critères du *danger*, des *atteintes* et des *abus potentiels* afférents aux liaisons «online», le critère du *nombre d'autorités habilitées à accéder* par procédure d'appel à un système informatique, ainsi que le critère de la distinction entre les *normes légales existantes* (de lege lata) et les *bases légales en cours d'élaboration* (de lege ferenda), qui permettra de voir dans quel sens la législation évolue. La section a également relevé qu'il faudra tenir compte des résultats des investigations menées par la *Délégation* des CdG sur les «événements au sein du DMF (EGB 95)».

Compte tenu de ces critères, la section a décidé de concentrer son attention sur *les systèmes informatiques* suivants:

– *RIPOL* (Système de recherches informatisées de police)
– *DOSIS* (Système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants)
– *ISIS*-[Plus] (Système provisoire de traitement des données relatives à la protection de l'Etat)
– *RCE* (Registre central des étrangers)
[= *ZAR* Zentrales Ausländerregister]

La section s'est aussi intéressée au système *ZAN* (Index central des dossiers), dans lequel des données de DOSIS peuvent être copiées, et au système *ISOK* (Système de traitement de données en matière de lutte contre le crime organisé), dont l'élaboration est directement liée au développement en cours de DOSIS.

16 Délimitation matérielle

Les discussions menées par la section ont montré le bien-fondé et la nécessité d'examiner la mise en place de liaisons «online» dans le domaine de la police. De plus, à côté des nombreuses liaisons déjà installées ces dernières années, ce secteur est en constante évolution et de nouveaux projets ou développements sont régulièrement en cours.

La commission ne remet pas en cause la nécessité de la mise en place de liaisons «online»; elle relève l'importance de l'efficacité et de la coordination policière ainsi que le degré de compatibilité des systèmes.

Par contre, la commission a clairement exprimé ses craintes vis-à-vis des dangers inhérents à ces liaisons «online» et son souhait d'une meilleure transparence. Elle a ainsi mis en évidence l'absolue nécessité d'analyser les conditions exactes de la mise en place de ces liaisons, en tenant compte de leur nombre grandissant et des risques d'atteintes et d'abus potentiels.

Si la section n'a pas voulu placer les détails techniques au centre de ses investigations, cet aspect de la question n'a toutefois pas été éludé, puisqu'il est abordé, notamment, dans le cadre de l'analyse des concepts informatiques ou de l'examen des mesures de sécurité, ou encore des mécanismes de contrôle. Pour ce dernier point, l'accent a été mis sur les aspects relatifs à la protection des données.

Cela a ainsi permis de poursuivre les investigations entamées par la CdG du Conseil national dans le cadre du *suivi de l'inspection sur l'introduction de l'informatique dans l'administration fédérale* (FF *1988* II 649). En effet, en dépit des nombreuses lacunes[4] relatives à la protection des données relevées à cette occasion, un examen approfondi de *la surveillance des projets de traitement automatisé* n'a pas été entrepris. La CdG du Conseil national avait bouclé cette inspection en mai 1997 en vue de son examen par la CdG du Conseil des Etats.

2 Examen au niveau conceptuel

21 Champ d'analyse

La question principale de cette inspection est la suivante:
Quelles sont les règles applicables en matière de conceptualisation et de mise en place des liaisons «online» dans le domaine de la police?

Autour de cette question principale, la commission a dégagé les questions incidentes suivantes:

- Existe-t-il dans l'administration fédérale, et au sein du DFJP en particulier, des *dispositions* réglant la mise en place des liaisons «online»?
- Les nombreuses *directives de l'OFI* prévoient-elles une réglementation de cette problématique?
- Quelles *exigences* doivent être remplies en matière de *protection des données*?
- Quelles sont les *bases légales applicables en matière de protection des données*?
- Le problème du respect des principes de *proportionnalité*, de *finalité*, d'*opportunité* et de *nécessité* est-il traité dans le cadre de l'élaboration des concepts informatiques?
- L'*examen des coûts* lors de la mise en place de liaisons «online» est-il prévu dans le cadre de l'élaboration des concepts informatiques?
- Existe-t-il des réglementations relatives à la *surveillance* et au *contrôle* lors de la mise en place de liaisons «online»?
- Qu'en est-il de la *procédure HERMES* en tant qu'instrument de gestion et standard pour la conduite et le déroulement des projets informatiques au sein de l'administration fédérale?
- Selon les normes en vigueur, *qui décide* des accès «online» qui peuvent être octroyés?
- Quels sont les rôles et les compétences des *groupes de projet* ou des *groupes techniques* chargés de la mise en place des liaisons «online»?

4 Evolution des systèmes interconnectés; enchevêtrement des systèmes d'information de l'administration [FF 1988 II 667, 689]. Rôle et moyens du Préposé fédéral à la protection des données en matière de surveillance [cf. lettre de la CdG du CN du 23 mai 95 au CF; procès-verbal de la séance plénière de la CdG du CN du 20 nov. 95].

22 Introduction

La commission a constaté que la gestion des banques de données et des liaisons permettant d'y accéder obéit aux lois, ordonnances et directives suivantes:

RIPOL	–	Art. 351bis Code pénal suisse
	–	Ordonnance RIPOL du 19 juin 1995
	–	Modification de l'ordonnance RIPOL du 11 septembre 1996

DOSIS	–	LF sur les Offices centraux de police criminelle de la Confédération du 7 octobre 1994
	–	Ordonnance DOSIS du 26 juin 1996

ISOK	–	LF sur les Offices centraux de police criminelle de la Confédération du 7 octobre 1994
	–	Ordonnance ISOK du 19 novembre 1997

ISIS	–	LF instituant des mesures visant au maintien de la sûreté intérieure du 21 mars 1997 (entrée en vigueur le 1er juil. 1998)
	–	Ordonnance ISIS du 31 août 1992
	–	Modification de l'ordonnance ISIS du 2 décembre 1996
	–	Directives ISIS du 31 août 1992

ZAN	–	Ordonnance concernant le Service d'identification de l'Office fédéral de la police du 1er décembre 1986
	–	Modification de l'ordonnance du 2 décembre 1996

RCE	–	Ordonnance RCE du 23 novembre 1994
	–	Modification de l'ordonnance RCE du 4 décembre 1995
	–	LF sur le séjour et l'établissement des étrangers (LSEE)

Cependant, si le principe de légalité a pour principal objectif la transparence, il ne suffit pas à lui seul à légitimer ces accès. La mise en place d'une liaison online doit en effet être précédée de toute une série d'étapes préalables (initialisation, conceptualisation, examen de sa nécessité, de ses coûts et de sa conformité aux principes de proportionnalité, de finalité et d'opportunité, étude des mesures de sécurité, évaluation globale des risques, etc.). Les accès en ligne ne peuvent pas uniquement être prévus ou justifiés dans des bases légales mais doivent donc suivre certaines procédures préalables et respecter certaines règles ou principes quant à leur conceptualisation.

L'examen de la question principale et du champ d'analyse défini autour de cette question a pour but de déterminer quelles sont les étapes préalables à toute mise en place de liaisons «online» et si des lacunes sont à constater dans ce domaine. Il s'agit en d'autres termes de savoir quelles sont les normes à appliquer lors de la

conceptualisation des liaisons «online» avant que ces liaisons et les bases légales sur lesquelles elles se fondent ne soient mises en place .

23 Examen des questions incidentes

231 Les directives de l'OFI

Les nombreuses directives de l'OFI prévoient-elles une réglementation sur cette problématique?

231.1 Liste des directives de l'OFI[5]

Au niveau fédéral, les principales bases légales réglant les questions touchant à l'informatique sont les suivantes:

- L'ordonnance du 11 décembre 1989 portant création de l'Office fédéral de l'informatique et réglant la coordination de l'informatique au sein de l'administration fédérale (RS *172.010.58)*.
- L'ordonnance du 10 juin 1991 concernant la protection des applications et des systèmes informatiques dans l'administration fédérale (RS *172.010.59*).
- Le plan directeur informatique de la Confédération, du 8 juillet 1994.

Se fondant sur ces normes, l'Office fédéral de l'informatique a édicté diverses *directives techniques* (DT), *directives concernant la sécurité informatique* (DS) et *stratégies*:

A. Liste des directives techniques

(article 3 de l'Ordonnance du CF portant création de l'OFI et réglant la coordination informatique au sein de l'administration fédérale):

DT 01	Adjudication de mandats de services informatiques à des sociétés externes, du 15 janvier 1997
Annexe 1	Critères de classification, édition 1994
Annexe 2	Tarif horaire pour prestations informatiques, édition 1998
Annexe 3	Modèle de contrat pour l'acquisition de systèmes informatiques complets et l'élaboration de logiciels spécifiques (contrat d'entreprise), édition du 15 janvier 1997
Annexe 4	Modèle de contrat pour les prestations informatiques (mandat), édition du 15 janvier 1997
Annexe 5	Conditions générales pour l'acquisition de systèmes informatiques complets et l'élaboration de logiciels spécifiques (papier jaune), édition juillet 1997
Annexe 6	Conditions générales pour les prestations informatiques (papier vert), édition juillet 1994
Annexe 7	Manuel d'utilisation, en chantier

5 cf. publication OFI «OFI-News 1997», p. 39–47 et cf. lettre OFI du 9 janvier 1998, point 4 liaisons online en général, p. 5–6

DT 02	Modalités de financement et d'acquisition dans le domaine de l'informatique, du 15 janvier 1997
Annexe 1	Liste de contrôle pour une acquisition conforme à la LMP et à l'OMP, janvier 1997
DT 03	Annonce des projets informatiques à l'OFI, du 22 août 1990
DT 04	Conception de l'informatisation des services d'enregistrement et de classement, du 11 décembre 1990
Annexe 1	Catalogue des critères d'évaluation des systèmes d'enregistrement et de classement
DT 05	Rapports annuels des services sur les effectifs du personnel, les dépenses et les coûts dans le domaine de l'informatique, du 16 septembre 1992
DT 06	MANUEL PC, supprimée le 18 octobre 1995
DT 07	Adressage du courrier électronique au sein de l'administration fédérale, du 17 janvier 1996
Annexe 1	Transition de la DT 07 de 1991 vers la DT 07 de 1996, du 17 janvier 1996
DT 08	Manuel pour chefs de projets LAN, du 16 octobre 1996
Annexes 1 à 15 (disponibles seulement en allemand)	
DT 09	Conventions de noms SNA / SNI - 92, du 16 septembre 1992
DT 10	Réutilisation du matériel informatique désaffecté, du 15 juin 1994
DT 11	Domain Name System (DNS), du 13 novembre 1996
DT 12	Coordination et standardisation de systèmes de gestion des affaires courantes, du 18 janvier 1995
Annexe 1	Modèle de données GEVER (disponible seulement en allemand)
Annexe 2	Profils de mise en œuvre (disponible seulement en allemand)
DT 13	Introduction et mise en œuvre du logiciel SAP R/3, du 12 juin 1996
Annexe 1	Architecture SAP/R3
Annexe 2	Coordination SAP
DT 14	Interface pour la remise aux Archives fédérales de données provenant d'applications GEVER, du 21 août 1996
DT 15	Systèmes de saisie du temps, fondés sur l'informatique, à l'usage de l'administration fédérale, du 17 mai 1995
Annexe 1	Feuille de saisie. saisie du temps, fondée sur l'informatique, à l'usage de l'administration fédérale, du 17 mai 1995
DT 16	Conduite de projet et développement de systèmes dans le cadre de projets informatiques, du 19 avril 1995
Annexe 1	Documents complémentaires

Annexe 2 Tâches et prestations de l'Office fédéral de l'informatique

Annexe 3 Organes de coordination et de contrôle

Annexe 4 Standards

Tiré à part supplémentaire: Directives de conduite de projet et de développement des systèmes dans le cadre de projets informatiques, du 19 avril 1995

DT 17 Adressage NSAP (Network Service Access Point), du 18 octobre 1995

Annexe 1 Formulaire de demande pour espace d'adresse NSAP Administrativ-Domain

Annexe 2 Formulaire de demande pour espace d'adresse NSAP Routing-Domain

Annexe 3 Formulaire de demande pour espace d'adresse NSAP Routing-Area

DT 18 World Wide Web (WWW) dans l'administration fédérale, du 15 janvier 1997

Annexe 1 Formulaire de demande pour son propre http-Proxy

Annexe 2 Formulaire de demande pour accéder à WWW via INTERNET depuis un serveur Proxy

Annexe 3 Formulaire de demande pour le Serveur WWW Public sur INTERNET.

DT 19 Controlling et calcul de rentabilité dans le domaine informatique au sein de l'administration fédérale, du 14 janvier 1998

B. Liste des directives concernant la sécurité informatique (DS)

(article 8 de l'Ordonnance du 10 juin 1991 concernant la protection des applications et des systèmes informatiques dans l'administration fédérale; RS *172.010.59*)

DS S01 Identification des utilisateurs et mots de passe, du 18 août 1993

Fiche technique sur l'utilisation des mots de passe dans l'administration fédérale, du décembre 1993

DS S02 Protection de base des systèmes et applications informatiques, du 19 avril 1995

Annexe 1 Instruction relative à la perception et au classement des objets à protéger

Annexe 2 Catalogue des mesures de protection fondamentales

Annexe 3 Formulaires de perception (Formulaires en couleur à commander de l'OFI)

MANUEL n° 1 pour la DS S02: Procédure pour le traitement des listes de contrôle et catalogue complet des mesures de protection fondamentales, du 1er octobre 1996

DS S03 Application de la Network Security Policy (NSP), du 25 juin 1997

C. Liste des stratégies

Selon le chiffre 3 du Plan directeur informatique de la Confédération (PDIC), les stratégies de mise en œuvre valables pour l'ensemble de l'administration fédérale seront élaborées par l'OFI en accord avec la CIC et publiées conformément à «l'Ordonnance portant création de l'OFI et réglant la coordination de l'informatique au sein de l'administration fédérale».

Stratégie GEVER

Stratégie en matière de coordination et de standardisation de systèmes de gestion des affaires courantes dans l'administration fédérale générale, du 18 janvier 1995
Appendice 1: Glossaire
Appendice 2: Bibliographie
Appendice 3: Illustrations

Stratégie télécommunications

Stratégie en matière de télécommunications de l'administration fédérale générale, du 12 juin 1996

Appendice: Signification des abréviations

Network Security Policy (NSP), du 25 juin 1998

231.2 Ces directives prévoient-elles une réglementation spécifique à la mise en place des liaisons «online»?

Pour la mise en place des liaisons «online», l'Office fédéral de l'informatique a pour mission de planifier et de gérer les *infrastructures de communication* pour toute l'administration fédérale. Au niveau matériel, les liaisons «online» dans le domaine de la police utilisent l'infrastructure de la Confédération pour communiquer des données, mais au niveau logiciel, les réseaux sont séparés, pour des raisons de sécurité.

Comme nous l'avons dit plus haut, l'Office fédéral de l'informatique élabore et édicte de nombreuses directives. Les applications telles que RIPOL, DOSIS, ISOK, ZAN, RCE et ISIS sont des unités d'organisation soumises à l'application des directives de sécurité de l'OFI. Sont ainsi applicables à ces systèmes les principes et les réglementations en matière de sécurité de l'administration fédérale, et en particulier:

- la loi fédérale et l'ordonnance sur la protection des données [RS *235.1* & RS *235.11*],
- l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale [RS *172.010.59*],
- la directive de sécurité DS S01: Identification des utilisateurs et mots de passe,
- la directive de sécurité DS S02: Protection de base des systèmes et applications informatiques,
- la directive de sécurité DS S03: Application de la Network Security Policy (NSP).

Concrètement, cela signifie notamment:

- qu'en vertu de la directive de sécurité DS S02 sur la protection de base des systèmes et applications informatiques, ces applications doivent faire l'objet d'une perception et d'une classification des objets à protéger, et dans tous les cas d'une évaluation des risques,

– que des mesures de sécurité fondées sur les directives de sécurité DS S01 et DS S02 doivent être mises en place pour ces applications,

– que des mesures d'organisation fondées sur la directive de sécurité DS S02 doivent être créées (responsable des applications, préposé à la sécurité, organe de contrôle, etc.),

– que depuis 1997, les accès à ces applications nouvellement octroyés doivent respecter les conditions de la *Network Security Policy (NSP)* et de la *directive de sécurité DS S03*: Application de la Network Security Policy.

L'importance de ces mesures de sécurité a également été mise en évidence dans le cadre d'un rapport du Département fédéral des finances intitulé *«Bericht EFD (BFI) an den Bundesrat vom 14. April 97, resp. vom 13. Juni 1997 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und –anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken»*[6] (p. ex.: évaluation des risques, nomination de responsables de la sécurité informatique, chiffrement des données, authentification, journalisation des accès, etc.).

Cependant, en dépit des nombreuses directives mentionnées plus haut et des dispositions y relatives applicables aux systèmes informatiques choisis par la section «Autorités», force est de constater que ces directives ne contiennent pas de dispositions spécifiquement consacrées à la mise en place des liaisons «online» en ce qui concerne en particulier l'examen des principes d'opportunité, de finalité et de proportionnalité. En effet, il ressort des documentations et avis fournis par l'OFI et des explications données par le conseiller à la protection des données du DFJP, que les directives susmentionnées règlent plutôt de nombreux points relatifs aux mesures de sécurité, aux procédures d'authentification et d'accès, aux mesures de chiffrement, aux mesures d'organisation, à l'évaluation des risques, aux différents niveaux de protection (1 à 3) ou encore à la protection des systèmes et applications connectées (Network Security Policy / NSP).

Toutefois, la directive DS S02 concernant la sécurité informatique comporte une annexe (no2) consacrée au «catalogue des mesures de protection fondamentales» qui prévoit dans son chapitre 8 («confidentialité et intégrité») toute une série de précisions concernant les accès aux systèmes informatiques. Mais ces précisions visent surtout les *accès individuels*. Ainsi, outre la description de mesures relatives à l'identification des utilisateurs ou aux mots de passe, cette annexe no 2 fixe certains critères tels que l'interruption de connexions restées inactives ou inutilisées, le contrôle quant aux sujets, objets, fréquence et durée des droits d'accès, l'attribution des accès cas par cas en fonction des tâches individuelles des personnes concernées ou encore l'attribution ou la modification de privilèges.

Par contre, *le déroulement* de la mise en œuvre des systèmes informatiques et des liaisons «online» permettant d'y accéder n'est pas réglé par ces directives mais par une procédure particulière de conduite des projets: la procédure HERMES.

6 vgl. Bericht EFD (BFI) an den Bundesrat vom 14. April 1997, resp. vom 13. Juni 1997 und Bundesratbeschluss vom 16. Juni 1997 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und –anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken

232 Procédure et compétences

Existe-t-il dans l'administration fédérale, au sein du DFJP en particulier, des dispositions réglant la mise en place des liaisons «online»?

Qu'en est-il de la procédure HERMES en tant qu'instrument de gestion et standard pour la conduite et le déroulement des projets informatiques au sein de l'administration fédérale?

Selon les normes en vigueur, qui décide des accès «online» qui peuvent être octroyés?

Quels sont les rôles et les compétences des groupes de projet ou des groupes techniques chargés de la mise en place des liaisons «online»?

Auditionné en détail par la section «Autorités» sur ce point particulier, le conseiller à la protection des données du DFJP a apporté de nombreuses précisions tant sur les dispositions légales appliquées par le DFJP lors de la mise en place de liaisons «online» que sur l'utilisation de la procédure HERMES en tant qu'instrument de gestion et standard pour la conduite et le déroulement des projets informatiques au sein du DFJP.

232.1 Les dispositions légales

Les dispositions légales appliquées par le DFJP sont les suivantes:

– L'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (RS *235.11*);

L'article 20, 2e al. de cette ordonnance stipule que les organes fédéraux responsables annoncent au Préposé fédéral à la protection des données, dès le début, tout projet de traitement automatisé de données personnelles. En général, cette annonce est faite par l'intermédiaire de l'Office fédéral de l'informatique.

– L'ordonnance du 10 juin 1991 concernant la protection des applications et des systèmes informatiques dans l'administration fédérale (RS *172.010.59*)

L'article 7 de cette ordonnance prévoit que les unités responsables de systèmes informatiques annoncent à l'OFI la planification des systèmes conformément aux directives de la Conférence informatique de la Confédération (CIC). En vertu de cette ordonnance, l'annonce est faite à l'OFI et en même temps une copie est transmise au Préposé fédéral à la protection des données.

– La directive technique DT 03: Annonce des projets informatiques à l'OFI, du 22 août 1990

L'article premier de cette directive technique précise que tous les nouveaux projets informatiques doivent être annoncés sous la forme d'une proposition établie selon la procédure HERMES.

232.2 La procédure HERMES en général

La procédure HERMES est une méthode de conduite et de déroulement des projets informatiques en tant qu'instrument d'organisation, de planification, d'exécution, de pilotage et de contrôle des projets informatiques[7].

Cet instrument de gestion de projets est utilisé dans l'administration fédérale depuis 1975. En 1986, une révision majeure de HERMES a été menée et son application est alors devenue obligatoire pour tous les projets informatiques.

232.3 La procédure HERMES au sein du DFJP

Selon le conseiller à la protection des données du DFJP, la procédure HERMES est utilisée en tant qu'instrument de gestion et standard pour la conduite et le déroulement des projets informatiques au DFJP. Cette méthode distingue différentes phases successives, chaque phase ne pouvant être engagée qu'après approbation de la phase précédente. Les principales phases sont:

a. l'initialisation du projet (proposition de projet). Document d'une dizaine de pages qui dit ce que l'on a l'intention de faire, quels sont les besoins, etc.

b. l'analyse préliminaire (élaboration et vérification des grandes lignes du projet; examen et préparation, s'il y a lieu, de bases légales)

c. la conception (spécification détaillée)

d. la réalisation (programmation et tests)

e. la mise en œuvre (formation des utilisateurs, exploitation du système)

La méthode HERMES cite en outre les points qui doivent être examinés dans chaque phase avant qu'une décision ne soit prise. Ces points définissent les grandes lignes d'organisation des projets informatiques.

Les rôles et les compétences des groupes de projet ou des autres organes techniques sont clairement définis dans le manuel de méthode HERMES[8]:

– instance d'approbation
– donneur d'ordre du projet
– comité de projet
– direction du projet
– etc.

Selon le Conseiller à la protection des données du DFJP, en application de la procédure HERMES, différentes instances accompagnent les projets informatiques au niveau du DFJP:

7 cf. Manuel «HERMES», conduite et déroulement de projets informatiques, OFI, édition 1995

8 cf. manuel HERMES, OFI, édition 1995, p. 6–3 à 6–13

a. l'instance d'approbation

C'est elle qui autorise le passage à la phase ultérieure.
Au DFJP, pour les grands projets, la décision appartient au secrétaire général ou à son suppléant

b. le comité de projet

Plus ou moins étoffé selon les projets, il rassemble notamment le chef de projet, le chef informatique du département (CID), un conseiller à la protection des données (celui de l'office ou celui du département, parfois les deux) et des représentants des utilisateurs (offices et cantons). Le Préposé fédéral à la protection des données participe parfois au comité de projet. Ce comité se réunit entre deux et quatre fois par an et accompagne en permanence chaque projet informatique. Pour les grands projets, un représentant des cantons fait partie du comité.

Il faut aussi dire que les projets informatiques ne sont jamais vraiment terminés. En effet, dans la plupart des projets informatiques, lorsqu'une version est installée, l'élaboration de la version suivante est directement mise en route: (RIPOL-4, RCE-3, AUPER-2, etc.) C'est pourquoi le comité suit le projet pendant toute sa durée de vie. Toute modification d'un système informatique doit être approuvée par le comité de projet, toute modification importante nécessite le déclenchement d'un nouveau cycle de phases (initialisation, analyse préliminaire, conception, réalisation, mise en œuvre).

c. la direction du projet

Il s'agit de la direction opérationnelle du projet: planification, coordination, surveillance et pilotage des activités liées au projet dans le respect des coûts et des délais prévus. Le chef de projet est responsable de la direction opérationnelle du projet.

Au DFJP, le formulaire autorisant le passage à la phase ultérieure doit être signé notamment par la direction de l'Office concerné, par le chef du centre de calculs, par le Conseiller à la protection des données du département et par le chef informatique du département. En signant le formulaire, le Conseiller à la protection des données du DFJP peut émettre certaines réserves, dont il devra être tenu compte dans la phase suivante.

Aucune acquisition de matériel informatique ne peut être effectuée sans qu'elle ait été approuvée lors d'une des phases de projet. Aucun logiciel ni matériel ne peut être acquis en dehors d'un projet fonctionnant selon la méthode HERMES.

232.4 D'où vient l'impulsion initiale pour la mise en place de liaisons «online» ou le développement d'un système d'information dans le domaine de la police?

La commission a constaté que l'impulsion initiale provient surtout des réunions de la «Commission technique suisse de police» ou d'autres organes techniques de police, notamment au sein d'lNTERPOL. *L'Office fédéral de la police et le Centre de calculs du DFJP* sont représentés au sein de ces groupes de travail et leurs collaborateurs reviennent de ces séances avec de nouvelles idées pour améliorer l'efficacité des instruments informatiques mis en œuvre. Une discussion a lieu au

sein de ces groupes et là naissent de nouvelles idées. Ces propositions sont examinées au sein de la direction de projet qui les soumet au comité de projet.

232.5 Application de la procédure HERMES par le DFJP pour les liaisons «online»

Si le comité de projet approuve l'idée d'une liaison «online», cela déclenche d'une part un examen des bases légales – et si nécessaire une modification de la loi –, d'autre part un nouveau projet selon HERMES pour la réalisation éventuelle de cette liaison «online» (les cinq phases d'HERMES devront donc être respectées).

Il ressort donc des investigations entreprises auprès du conseiller à la protection des données du DFJP que la mise en place d'une liaison «online» déclenche un nouveau cycle de phases selon HERMES, pour autant que cette liaison entraîne une modification de l'application (nouvelles fonctions). La décision de principe de réaliser et de mettre en œuvre des liaisons «online» constitue en effet une modification importante du projet qui nécessite obligatoirement le déroulement des diverses phases du projet. Indépendamment de ces phases à suivre, la décision de mise en place de la liaison «online» est donc prise par le Comité de projet, avec approbation du secrétaire général du département.

Il en va de même lorsque la décision relative au raccordement d'un canton déterminé est prise par le comité de projet. Cependant, dans ce cas là, il arrive fréquemment que l'on ait déjà les bases légales indispensables pour le raccordement des cantons et qu'un projet pilote ait été mis en place avec 4 ou 5 cantons. Le raccordement ultérieur des autres cantons ne déclenche pas à nouveau un cycle complet; de nouvelles bases légales, ou de nouveaux logiciels ne sont pas non plus nécessaire. Par contre, pour l'exploitation, le DFJP s'assure que les lignes et les périphériques nécessaires sont en place avant de raccorder d'autres cantons.

232.6 Les limites de la procédure HERMES

Comme nous l'avons déjà expliqué, *le déroulement* de la mise en œuvre des systèmes informatiques et des liaisons «online» permettant d'y accéder n'est pas réglé par des directives mais par la procédure HERMES. Si cette procédure est appliquée correctement par le DFJP , il n'en faut pas moins rappeler que cette procédure demeure avant tout une «méthode» de conduite des projets informatiques comprenant différentes phases obligatoires.

En d'autres termes, elle prévoit bien les phases qui doivent être suivies pour les décisions relatives à la mise en place de nouvelles liaisons «online» mais ne contient pas de règles ou de dispositions spécifiquement consacrées à ces dernières, notamment quant à l'examen des principes d'opportunité, de proportionnalité ou de finalité. Seuls quelques renvois ou questions sont par exemple rappelés dans la phase de l'analyse préliminaire (la sécurité et la protection des données ont-elles été analysées et appréciées en tenant compte de la situation?)[9], dans la phase de conception: (les exigences en matière de sécurité et de protection des données sont-elles remplies?)[10]

9 cf. manuel HERMES, OFI, édition 1995, p. 2–7
10 cf. manuel HERMES, OFI, édition 1995, p. 3–9

ou au niveau des types de système distingués par HERMES: (infrastructures informatiques, p. ex. l'acquisition et l'installation de réseaux de communication)[11].

La procédure HERMES appliquée par le DFJP représente donc un instrument fondamental pour la mise en place de liaisons «online» dans le domaine de la police. Encore une fois, cette procédure n'est qu'une «méthode» pour la conduite et le déroulement des projets informatiques, et elle ne prévoit pas de normes spécifiques concernant les liaisons «online».

Il ressort d'autre part des investigations entreprises auprès du conseiller à la protection des données du DFJP et du Préposé fédéral à la protection des données que des problèmes peuvent survenir au niveau de l'analyse des besoins des utilisateurs et de l'efficacité des contrôles et du suivi des développements informatiques par les autorités compétentes.

233 Aspects de protection des données et contrôle de la mise en place des liaisons «online»

Quelles sont les bases légales applicables en matière de protection des données?

Quelles exigences doivent être remplies en matière de protection des données?

Le problème du respect des principes de proportionnalité, de finalité, d'opportunité et de nécessité est-il traité dans le cadre de l'élaboration des concepts informatiques?

Existe-t-il des réglementations relatives à la surveillance et au contrôle lors de la mise en place de liaisons «online»?

233.1 Liaisons «online» et protection des données. Bases légales et exigences

Les bases légales applicables en matière de protection des données sont la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS *235.1*) et l'ordonnance du Conseil fédéral du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD; RS *235.11*).

Ces bases légales règlent non seulement les aspects liés au respect des principes de proportionnalité et de finalité par exemple (art. 4 LPD), mais également les mesures de sécurité (art. 7 LPD) et les mesures techniques et organisationnelles (art. 20 ss OLPD) à prendre lors du traitement de données personnelles.

Il convient de relever que les exigences à remplir en matière de protection des données dans le cadre de la mise en place des liaisons «online» ont été clairement dé-

11 cf. manuel HERMES, OFI, édition 1995, p. 11–4

crites dans un chapitre spécial d'un rapport du Département fédéral des finances[12], dont voici les éléments principaux:

A. Principes régissant la protection des données

Légalité

Les organes fédéraux ne sont en droit de traiter des données personnelles que si une base légale les y autorise (art. 4, 1er al., art. 17, 1er al., LPD).

Les organes fédéraux ne sont en droit de communiquer des données personnelles que si une base légale les y autorise (art. 17 et 19 LPD). Les organes fédéraux ne sont en droit de rendre des données personnelles accessibles au moyen d'une procédure d'appel que si cela est prévu expressément. Les données sensibles ou les profils de la personnalité ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel le prévoit expressément (art. 19, 3e al., LPD).

Proportionnalité

Le traitement des données personnelles doit être effectué conformément au principe de la proportionnalité (art. 4, 2e al., LPD).

Adéquation

Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances (art. 4, 3e al., LPD).

Une autorité qui souhaite avoir accès à certaines données remplit généralement des missions différentes, d'où le risque de la voir utiliser les données consultées à des fins autres que celles indiquées initialement. Or, certaines données ne peuvent être consultées qu'aux fins nécessaires pour remplir la mission concernée ou définies par une base légale. En règle générale, les données personnelles de tierces personnes ne doivent pas être communiquées, et ne doivent en aucun cas être exploitées (cf. p. ex. art. 7, 3e al., ordonnance RCE; RS *142.215*; RO *1994* 2859).

Exactitude

Quiconque traite des données personnelles doit s'assurer qu'elles sont correctes (art. 5, 1er al., LPD).

Toute modification de données doit comprendre des mécanismes de contrôle (notamment des mesures d'organisation) garantissant leur exactitude (compte tenu du but visé).

Sécurité des données

Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées (art. 7, 1er al., LPD).

12 cf. Bericht EFD (BFI) an den Bundesrat vom 14. April 97, resp. vom 13. Juni 1997 und Bundesratbeschluss vom 16. Juni 97 betr. a) Stand der Umsetzung der Verordnung über den Schutz der Informatiksysteme und -anwendungen in der Bundesverwaltung, b) Sicherheit im Umfeld Büroautomation und Auditmöglichkeiten von Zugriffen auf sensible Datenbanken (chap. 4 Büroautomation und Datenbankzugriffe / 4.2 Anforderungen des EDSB, p. 22 à 26).

B. Application / mesures

Traçabilité

Il doit être possible d'identifier l'auteur des données, et de reconstituer les opérations de traitement des données, concernant notamment leur collecte, leur modification, leur communication et leur destruction (cf. critères relatifs à la journalisation, art. 10 OLPD).

Autorisation de modifier des données

Des contrôles mémoire devront prévenir tout enregistrement, consultation, modification ou suppression de données effectué sans autorisation.

Accès aux personnes autorisées uniquement

Des contrôles d'accès devront garantir que les personnes concernées aient accès uniquement aux données dont elles ont besoin pour s'acquitter de leur mission.

Mise en relation de données

Il y a lieu de vérifier s'il est possible par des moyens informatiques de se procurer depuis différentes sources des données concernant un même objet de façon, par exemple, à établir des profils de la personnalité (absence de base légale, non-proportionnalité du traitement, sécurité insuffisante, contrôle insuffisant de l'exactitude). Si la mission concernée n'exige pas une mise en relation de données (base légale), il y a lieu de rendre techniquement impossible une mise en relation automatisée.

C. Etat de la sécurité

Il y a lieu de distinguer entre la *protection* des données (légalité, proportionnalité, adéquation, exactitude) et la *sécurité* des données (confidentialité, intégrité, disponibilité, authenticité).

Exemples de mesures techniques visant à accroître la protection des données: journalisation (contrôle de l'affection aux seules utilisations prévues); exemples de mesures techniques visant à accroître la sécurité des données: cryptage réseau, cryptage mémoire.

233.2 Examen des principes de proportionnalité, de finalité et d'opportunité (nécessité) au niveau de l'élaboration des concepts informatiques

Lors de l'audition du conseiller à la protection des données du DFJP, il a été précisé qu'une analyse des besoins des utilisateurs était effectuée au sein du DFJP dans le cadre de la procédure HERMES puisque la nécessité d'une liaison «online» résulte des besoins exprimés.

Il a cependant également été constaté qu'à l'exception de quelques renvois généraux, ni les directives de l'OFI ni la procédure HERMES ne contiennent de normes spécifiquement consacrées à la mise en place des liaisons «online», notamment en ce qui concerne l'examen des principes d'opportunité, de proportionnalité ou de finalité.

De plus, lorsque dans le cadre d'un projet informatique du DFJP, un tel examen est effectué durant les phases de la procédure HERMES, les aspects liés au développement des nouvelles liaisons «online» ne sont pas toujours déjà clairement définis, et il est même parfois impossible de voir quels accès sont prévus parce que le projet n'est pas suffisamment avancé. Cela rend d'autant plus délicat d'une part l'évaluation de la nécessité, de la proportionnalité et de la finalité des futures liaisons «online» et d'autre part l'exercice des tâches de contrôle confiées notamment au Préposé fédéral à la protection des données.

233.3 Mise en place de liaisons «online». Surveillance et contrôle

En vertu de l'article 20 OLPD, les organes fédéraux annoncent au Préposé fédéral à la protection des données, dès le début, tout projet de traitement automatisé de données personnelles, afin que les exigences de la protection des données soient immédiatement prises en considération. L'annonce au Préposé a lieu par l'intermédiaire de l'Office fédéral de l'informatique lorsqu'un projet doit également être annoncé à cet Office. Le Préposé fédéral et l'OFI collaborent dans le cadre de leurs activités relatives aux mesures techniques.

L'Office fédéral de l'informatique a pour mission de planifier et de gérer les *infrastructures de communication* pour toute l'administration fédérale. Au niveau matériel, les liaisons «online» dans le domaine de la police utilisent, lorsqu'elle existe, l'infrastructure de la Confédération pour communiquer des données, mais au niveau logique, les réseaux sont séparés, pour des raisons de sécurité. Dans le cadre de ses compétences, l'OFI prend position sur les projets informatiques développés et élabore et édicte de nombreuses directives.

En vertu de l'article 27 LPD, il appartient au Préposé fédéral à la protection des données de surveiller l'application par les organes fédéraux de la loi fédérale sur la protection des données. Dans le cadre de la mise en place de nouvelles liaisons «online», il est donc compétent pour veiller au respect des principes de proportionnalité, de finalité ou encore de nécessité. Cependant, deux problèmes se posent:

a. Premièrement, le Préposé invoque un manque de moyens, notamment en personnel. Ce problème a déjà été soulevé lors des investigations entamées par la CdG du Conseil national dans le cadre du suivi de l'inspection sur l'introduction de l'informatique dans l'administration fédérale (examen du rôle et des moyens du Préposé fédéral à la protection des données en matière de surveillance; absence de mesures concrètes et, faute de moyens, impossibilité pour le Préposé fédéral de procéder à une surveillance systématique et détaillée de tous les projets de traitement automatisé de données personnelles au sein de l'administration fédérale).

b. Deuxièmement, le Préposé fédéral a souvent du mal à se prononcer sur le développement de nouvelles liaisons «online», car dans la plupart des cas, ces liaisons ne sont pas encore clairement définies dans les concepts qui lui sont soumis au cours des différentes phases de la procédure HERMES. Les précisions nécessaires ne seront apportée que lorsque la création de bases légales est nécessaire pour tel ou tel accès.

C'est ici qu'intervient encore le problème de la législation «à titre préventif»: compte tenu des lenteurs de la procédure législative, la tentation est grande de pro-

poser le plus tôt possible des amendements de lois ou d'ordonnances visant à la création des bases légales nécessaire à de futures liaisons «online», alors même que ces liaisons n'ont pas encore été clairement définies et que leur nécessité et leur proportionnalité n'ont pas encore été démontrées.

Le Préposé fédéral à la protection des données est donc confronté à différentes difficultés dans le cadre des tâches de contrôle qu'il assume lors de la mise en place de liaisons «online»:

- Le manque de moyens, notamment en personnel, ne lui permet pas d'effectuer les contrôles adéquats qu'il a le mandat légal d'effectuer.
- L'état d'avancement d'un projet n'est pas toujours suffisant au niveau de la procédure HERMES pour se déterminer sur la nécessité ou la proportionnalité des accès.
- Cet examen peut alors être effectué lors de l'élaboration des bases légales. Certains offices ne savent cependant pas ce dont ils ont réellement besoin et ont tendance à prévoir d'emblée des accès dont ils n'ont pas vérifié la nécessité.
- D'autres offices au contraire ne voient pas l'utilité de mettre en place certains accès et ne les prévoient donc pas dans leurs projets législatifs. Une fois la loi adoptée, des besoins d'accès se manifestent et le Préposé est saisi pour autoriser ces accès, pour lesquels les bases légales font défaut.

233.4 Le contrôle des accès octroyés aux cantons

L'octroi aux cantons d'accès «online» à des systèmes informatiques de police soulève un certain nombre de problèmes, notamment au niveau du pouvoir décisionnel pour l'octroi de ces accès ou pour le contrôle du respect des exigences en matière de protection des données ou des mesures de sécurité.

Les procédures décisionnelles de demande d'accès varient selon les cantons. Le processus peut fortement varier entre une procédure extrêmement minutieuse pour la mise en place d'accès «online» telle qu'elle est pratiquée par exemple dans le canton de Lucerne par rapport à d'autres cantons où la procédure est moins transparente et où les autorités fédérales doivent veiller à ce que la hiérarchie et les compétences décisionnelles cantonales aient bien été respectées.

Un autre problème se pose du fait qu'il n'y a pas d'examen au niveau fédéral des lois cantonales de protection des données. De plus, la LPD ne donne pas de compétence aux services de l'administration fédérale de faire des investigations auprès des cantons. Le Préposé fédéral à la protection des données ne fonctionne que comme instance de conseil vis-à-vis des cantons. Les cantons ayant l'obligation d'avoir un organe de contrôle, la surveillance ne peut être exercée par le Préposé fédéral dans les cantons, ce qui peut poser problème notamment avec les accès en ligne. Il peut intervenir au moment où l'attribution d'un accès est définie, mais par la suite il n'a pas de moyen de contrôler, dans le canton, que ces accès sont respectés et qu'ils n'ont pas été étendus à d'autres organes. Ce contrôle est de la compétence des autorités cantonales. Or ce niveau de contrôle peut être très différent selon les cantons.

En outre, l'examen de la nécessité ou de la proportionnalité des accès «online» octroyés aux cantons est relatif. Le besoin général exprimé par des autorités canto-

nales est pris en compte par le DFJP dès que la hiérarchie cantonale s'est prononcée en ce sens. Ensuite des mesures de sécurité sont mises en place permettant, notamment au niveau du centre de calcul du DFJP, un certain contrôle global des accès des cantons (mots de passe, enregistrement des utilisateurs, etc.). Par contre, si un service cantonal de police d'un canton demande de raccorder cinq personnes parce qu'elles en ont besoin, le DFJP ne va pas contrôler que tel soit bien le cas.

233.5 Le cas particulier du centre de calcul du DFJP

Les investigations entreprises tant par la section «Autorités» dans le cadre de cette inspection «online» que par la délégation des CdG dans le cadre de ses contrôles relatifs aux systèmes ISIS et DOSIS ont permis de mettre en évidence une problématique inhérente à l'absence d'examen de sécurité des collaborateurs du centre de calcul du DFJP.

Contrairement aux collaborateurs de la police fédérale, les informaticiens travaillant au centre de calcul de Zollikofen ne font en effet pas l'objet d'un tel contrôle de sécurité. Or ces informaticiens ont accès à des données extrêmement sensibles dans le domaine tant de la police que de la protection de l'Etat.

Cette situation peut entraîner des problèmes au niveau des mesures de sécurité. En outre, le cas soulevé dans le cadre du rapport du service de contrôle administratif du Conseil fédéral «Online-Datenaustausch zwischen Bund und Kantonen» faisant état du développement d'un système cantonal («ABI») parallèle aux systèmes DOSIS & ISOK par d'anciens collaborateurs du centre de calcul du DFJP prouve bien la pertinence de cette problématique.

234 Examen des coûts

L'examen des coûts lors de la mise en place de liaisons «online» est-il prévu dans le cadre de l'élaboration des concepts informatiques?

De manière simplifiée, il ressort des explications fournies par le Conseiller à la protection des données du DFJP que la répartition des coûts entre la Confédération et les cantons lors de la mise en place de liaisons «online» est la suivante:

La mise en place et l'exploitation du réseau jusqu'au point d'entrée dans le canton sont du ressort de la Confédération; les cantons sont chargés de l'exploitation du réseau interne (LAN) et de l'acquisition des périphériques (PC, imprimantes, etc.).

A côté de ce principe de répartition des coûts entre Confédération et cantons, de nombreuses autres questions se posent lors de la mise en place de liaisons «online». Afin d'avoir une approche plus concrète de ces aspects, cette question a été traitée dans le cadre de l'examen des cas concrets du bloc 2. Eu égard à l'importante quantité d'accès des cantons aux systèmes informatiques de police de la Confédération, l'accent a été mis sur cette répartition des coûts entre la Confédération et les cantons, et cela pour chacun des systèmes choisis par la section «Autorités» (RIPOL, DOSIS, ISOK, ZAN, RCE et ISIS), mais aussi sur les aspects de budget, d'investissement, de coûts d'exploitation, etc.

Le détail de la problématique des coûts est traité dans le rapport d'expert.

24 Examen de la question principale

Quelles sont les règles applicables en matière de conceptualisation et de mise en place des liaisons «online» dans le domaine de la police?

Au vu des réponses apportées aux questions incidentes, on peut donner à la question principale la réponse condensée suivante:

241 Normes techniques et normes de sécurité

Sur la base de normes cadres telles que l'*ordonnance du 11 décembre 1989 portant sur la création de l'Office fédéral de l'informatique et réglant la coordination de l'informatique au sein de l'administration fédérale* et l'*ordonnance du 10 juin 1991 concernant la protection des applications et des systèmes informatiques dans l'administration fédérale*, l'Office fédéral de l'informatique a édicté de nombreuses directives techniques (DT), directives concernant la sécurité informatique (DS) et stratégies.

– Les applications telles que RIPOL, DOSIS, ISOK, ZAN, RCE et ISIS choisies dans le cadre de cette inspection sont des unités d'organisation soumises à l'applications des directives de sécurité de l'OFI. Sont ainsi applicables à ces systèmes les principes et les réglementations en matière de sécurité de l'administration fédérale (se reporter à la liste dressée au chapitre 231.2)

L'application de ces normes implique d'une part que les systèmes informatiques précités doivent faire l'objet d'une perception et d'une classification des objets à protéger et dans tous les cas d'une évaluation des risques d'autre part que des mesures de sécurité doivent être mises en place pour ces applications, que des mesures d'organisation doivent être créées (responsable des applications, préposé à la sécurité, organe de contrôle, etc.) ou encore que les accès nouvellement octroyés à ces applications doivent respecter les conditions de la *Network Security Policy (NSP)* et de la *directive de sécurité DS S03*.

242 Normes de procédure (méthode)

Le déroulement de la mise en œuvre des systèmes informatiques et des liaisons «online» permettant d'y accéder est réglé selon une procédure particulière de conduite des projets: la procédure HERMES. Cette procédure est appliquée en tant qu'instrument de gestion et standard pour la conduite des projets informatiques au sein du DFJP. Elle distingue différentes phases et règle les rôles et les compétences des différents groupes de projets ou autres organes *(instance d'approbation, donneur d'ordre du projet, comité de projet, direction du projet, etc.)*.

Il ressort des investigations entreprises auprès du Conseiller à la protection des données du DFJP que la mise en place de liaisons «online» doit déclencher à chaque fois un nouveau cycle de phases selon la procédure HERMES. Cependant, cela n'est pas le cas lorsqu'un ou plusieurs cantons sont déjà raccordés à un système, par exemple dans le cadre d'un projet pilote, et qu'est décidé ensuite le raccordement d'autres cantons.

La procédure HERMES appliquée par le DFJP représente un instrument fondamental dans le cadre de la mise en place des liaisons «online» dans le domaine de la police. Cette procédure règle la conduite et le déroulement des projets informatiques, mais ne contient pas de normes spécifiques concernant les liaisons «online», et ne dit rien, en particulier, du respect des principes d'opportunité, de proportionnalité et de finalité.

243 Normes de protection des données

La loi fédérale du 19 juin 1992 sur la protection des données et l'ordonnance du Conseil fédéral du 14 juin 1993 relative à ladite loi règlent non seulement les aspects liés au respect des principes de proportionnalité et de finalité (art. 4 LPD), mais également les mesures de sécurité (art. 7 LPD) et les mesures techniques et organisationnelles (art. 20 ss OLPD) à prendre lors du traitement de données personnelles ainsi que les mécanismes d'annonce des projets informatiques.

En vertu de l'article 27 LPD, il appartient au Préposé fédéral à la protection des données de surveiller l'application par les organes fédéraux de la LPD. Dans le cadre de la mise en place de nouvelles liaisons «online», il est donc compétent pour veiller au respect des principes de proportionnalité, de finalité ou encore de nécessité. La Commission de gestion partage l'avis du Préposé fédéral à la protection des données, qui estime qu'il manque de moyens, et notamment de personnel, pour exercer les contrôles dont il est chargé. Ce problème avait déjà été soulevé dans le cadre de l'inspection sur l'introduction de l'informatique dans l'administration fédérale, et force est de constater qu'il est toujours d'actualité.

Par ailleurs, l'efficacité des contrôles est remise en question par le fait qu'il est difficile pour le Préposé fédéral de se prononcer sur le développement de nouvelles liaisons «online» lorsque ces liaisons lui sont présentées au stade de concept et ne sont pas encore clairement définies. Ces lacunes dans le contrôle ne sont pas sans incidences sur la procédure législative: des modifications d'actes législatifs sont proposées pour des liaisons «online» qui ne sont pas encore définies avec précision, et dont la proportionnalité, la finalité, etc. n'ont pas encore fait l'objet d'un examen attentif.

244 Normes et pratiques cantonales

La mise en place des liaisons «online» doit également tenir compte des *réglementations et des procédures décisionnelles* très variables selon les différents cantons. En outre, le Préposé fédéral à la protection des données ne fonctionne que comme instance de conseil vis-à-vis des cantons. Il peut bien intervenir au moment où est définie l'attribution d'un accès, mais par la suite il n'a pas de moyen de contrôler dans le canton si ces accès sont respectés ou n'ont pas été étendus à d'autres organes. Ce contrôle là est de la compétence des autorités cantonales. Or ce niveau de contrôle peut être très différent selon les cantons.

En outre, l'examen de la nécessité ou de la proportionnalité des accès «online» octroyés aux cantons est relatif. Suite au besoin général exprimé par des autorités cantonales, des mesures de sécurité sont mises en place permettant, notamment au niveau du Centre de calcul du DFJP, un certain contrôle global des accès des can-

tons (mots de passe, enregistrement des utilisateurs, . . .). Par contre, si un service cantonal de police d'un canton demande de raccorder cinq personnes parce qu'elles en ont besoin, le DFJP ne va pas contrôler que tel soit bien le cas.

25 Conclusions

Au niveau du concept

Compte tenu des investigations qu'elle a menées en s'appuyant sur les travaux préparatoires de l'OPCA, la commission relève certains points positifs et certaines lacunes:

251

Les bases légales réglementant la mise en place des systèmes informatiques *(loi et ordonnance sur la protection des données, ordonnances et directives techniques et de sécurité de l'OFI)* et les instruments de gestion et de standard pour la conduite et le déroulement des projets informatiques au sein de l'administration fédérale *(procédure HERMES)* constituent un cadre légal et réglementaire dense et détaillé.

252

Pour la planification et la mise en place de liaisons «online», différentes dispositions découlant des normes précitées prévoient un certain nombre de réglementations, que ce soit au niveau des phases de la procédure HERMES, des mesures de sécurité et d'organisation, des directives de sécurité ou des principes de protection des données. Deux constatations doivent cependant être faites:

– D'une part, les différentes directives susmentionnées prévoient avant tout de nombreux points relatifs aux mesures de sécurité, aux mesures de chiffrement et d'authentification, aux niveaux de protection, aux mesures d'organisation, à l'évaluation des risques ou à la protection des systèmes et applications connectées (Network Security Policy / NSP), sans cependant contenir de dispositions spécifiquement consacrées à la mise en place des liaisons «online» et en particulier à l'examen préalable des principes de nécessité, de finalité ou de proportionnalité des nouveaux accès «online». L'annexe n° 2 à la directive concernant la sécurité informatique DS S02 apporte bien quelques précisions; elle ne vise cependant pas l'examen de ces principes dans le cadre de liaisons envisagées en faveur d'autorités fédérales ou cantonales mais règle plutôt les aspects liés aux accès individuels de chaque utilisateur aux systèmes (identification des utilisateurs, mots de passe, interruption des connexions inactives ou inutilisées, contrôle quant aux sujets, objets, fréquence et durée des droits d'accès, attribution des accès de cas en cas ou modification des privilèges).
– D'autre part, la procédure HERMES, en tant que méthode de conduite et de déroulement des projets informatiques, prévoit bien les phases qui doivent être suivies pour les décisions de mise en place de nouvelles liaisons «online». Hormis quelques renvois généraux elle ne contient cependant pas de règles ou de dispositions consacrées à ces dernières, notamment quant à l'examen des principes d'opportunité, de proportionnalité ou de finalité. La

procédure HERMES appliquée par le DFJP représente donc un instrument fondamental dans le cadre de la mise en place des liaisons «online» dans le domaine de la police; elle ne joue cependant qu'un rôle de «méthode» dans la conduite et le déroulement des projets informatiques.

253

L'examen des principes susmentionnés est par contre prévu dans le cadre des normes de protection des données. Ces dispositions fondent non seulement les principes d'opportunité, de proportionnalité ou de finalité mais règlent également les mécanismes d'annonce des projets de traitement automatisé de données personnelles au PFPD via l'OFI ainsi que les compétences de contrôles y relatives.

Le contrôle du respect des principes de protection des données est difficile parce que les moyens nécessaires manquent, parce que certains accès sont prévus à l'avance sans que leur utilité soit démontrée, et parce que certaines demandes sont déposées pour des accès n'ayant pas de base légale.

254

La mise en place de liaisons «online» à des systèmes informatiques de la Confédération en faveur des cantons soulève divers problèmes, notamment en ce qui concerne les nombreuses réglementations cantonales différentes (en matière de protection des données p. ex.), les procédures décisionnelles qui varient selon les cantons, l'examen de la nécessité ou de la proportionnalité ou encore le contrôle des accès octroyés.

255

Le tableau suivant reprend les principes ou les phases de base liés à la mise en place des liaisons «online» en mentionnant les étapes avec leurs aspects satisfaisants [✓] et les lacunes [✘]:

a.	Cadre réglementaire relatif à la conceptualisation des liaisons «online» sous forme de directives techniques (DT), de directives concernant la sécurité informatique (DS) ou de stratégies	✓
b.	Standard et méthode de conduite et de déroulement des projets informatiques en tant qu'instrument d'organisation, de planification, d'exécution et de pilotage	✓
c.	Mécanismes d'annonce des projets informatiques	✓
d.	évaluation des risques	A examiner selon résultats du rapport d'expert
e.	Planification des mesures de sécurité	
f.	Examen «préalable» à la mise en place des liaisons «online»	
g.	Nécessité	✘
h.	Proportionnalité	
i.	Finalité	

j.	Octroi d'accès «online» avec les cantons (procédures décisionnelles, réglementations, contrôle)	✘
	Contrôle des liaisons «online» (examen à posteriori, contrôle de l'étendue des accès, etc.)	✘
k.	Bases légales sur lesquelles se fondent les systèmes informatiques	✓
l.	Dispositions de lois au sens formel prévoyant expressément des accès «online» à des données sensibles	✓

Enquête auprès de l'administration

Les résultats présentés dans le rapport d'expert (voir annexe I) corroborent et complètent les conclusions de la commission.

L'expert insiste sur la nécessité de sensibiliser le législateur aux questions de normes de délégation, et de lui recommander un choix exact de notions. La commission partage le point de vue de l'expert qui estime que les autorisations en matière de raccordements «online» doivent obéir à une réglementation générale d'un niveau supérieur. La pratique actuelle consistant à déléguer les compétences jusqu'au bas de la hiérarchie administrative ne tient pas compte de l'importance de l'information dans le domaine de la police, ni du caractère sensible des données traitées. Le rôle de l'autorité indépendante chargée de délivrer des autorisations de raccordement sera mieux assumé par une unité administrative hiérarchiquement supérieure que par une unité qui a elle-même recours à un service d'information, et qui peut donc avoir un intérêt à ce que ce système soit plus largement utilisé. Les conditions légales très strictes, préalables à toute exploitation des systèmes d'information de police (nécessité, proportionnalité et opportunité), doivent être garanties dans le cadre d'une procédure clairement définie.

L'expert propose notamment les mesures suivantes:

- le DFJP édicte des prescriptions claires sur la procédure à suivre pour autoriser la mise en place de liaisons «online». La transparence ainsi créée permet de garantir que la procédure se déroule toujours de la même façon;
- création de bases légales même pour les projets pilotes;
- création de normes minimales pour la collaboration entre la Confédération et les cantons dans le cadre des requêtes et de l'installation de liaisons «online» avec les systèmes fédéraux d'informations;
- impliquer des responsables politiques (Confédération et cantons) dans la procédure de décision sur la réalisation et l'admissibilité des liaisons «online»;
- trouver un lieu plus approprié pour le centre de calcul du DFJP;
- introduire un contrôle de sécurité pour les collaborateurs du centre de calcul du DFJP;
- fusionner rapidement les réseaux parallèles KOMBV-KTV et DFJP-WAN.

26 Motion et recommandations de la commission

Au vu des considérations qui précèdent, la commission présente une motion à son conseil et soumet au Conseil fédéral une série de recommandations. Elle invite également ce dernier à examiner les recommandations de l'expert, et, si elles paraissent opportunes, à les mettre en œuvre le plus rapidement possible.

Motion de la Commission de gestion du Conseil des Etats

Liaisons «online». Renforcer la protection pour les donneés personnelles

Le Conseil fédéral est invité à soumettre aux Chambres fédérales une révision de la loi du 19 juin 1992 sur la protection des données. Cette révision a pour objectif:

a. d'imposer des bases légales pour toute liaison «online» même lorsqu'il s'agit d'un projet pilote

b. de prévoir, pour les requêtes et l'installation de liaisons «online» avec les systèmes informatiques de la Confédération, des normes minimales permettant d'améliorer la collaboration entre la Confédération et les cantons. La Confédération règle l'accès, l'utilisation, la protection et le contrôle de ses banques de données.

Recommandations de la Commission

261 Opportunité, proportionnalité et finalité

La multiplication des moyens informatiques entraîne la mise en place d'un nombre toujours plus important de liaisons «online» habilitant de nombreuses autorités fédérales et cantonales à accéder directement à différentes banques de données. Avant de réglementer ces liaisons dans des lois au sens formel, le Conseil fédéral les examine sous l'angle de l'opportunité, de la proportionnalité et de la finalité.

262 Contrôle par l'instance compétente

Le Conseil fédéral veille à ce que les liaisons «online» soient contrôlée de manière plus appropriée par le Préposé fédéral à la protection des données. Le contrôle doit garantir que ne sont établies que des liaisons dont la nécessité a été démontrée, dont l'objectif est connu, dont les coûts ont été prévus et pour lesquels les risques (d'utilisation abusive ou d'atteinte à la personnalité) ont fait l'objet d'une évaluation.

263 Liaisons «online»: transparence dans les messages du Conseil fédéral

Le Conseil fédéral veille à ce que ses messages contiennent toutes les précisions sur les accès envisagés tant au niveau de leur nécessité et de leur finalité qu'au niveau de la proportionnalité et de l'étendue de ces accès, ainsi que sur les autorités auxquelles ils seraient octroyés.

264 Collaboration et coordination entre la Confédération et les cantons

Le Conseil fédéral veille à une meilleure collaboration entre la Confédération et les cantons. afin d'une part de promouvoir la mise en place de procédures décisionnelles cantonales uniformisées ou comparables, sinon similaires, dans le respect du fédéralisme et des réglementations cantonales en vigueur.

265 Procédure d'autorisation pour des liaisons «online». Principes de base

Le Conseil fédéral fixe des principes de base à respecter dans les procédures d'autorisation de liaisons «online» dans le domaine de la police. Il règle en particulier les attributions, les compétences et les responsabilités.

266 Contrôle des normes de délégations

Le Conseil fédéral contrôle la délégation générale des compétences jusqu'au bas de la hiérarchie et dans tous les domaines concernés. Il veille à ce que les autorisations d'accès en ligne soient octroyées par une instance concédante adéquate et indépendante qui soit consciente tant de l'importance et de la portée de sa décision que du caractère sensible des données traitées.

267 Contrôle de sécurité

Le Conseil fédéral donne aux organes fédéraux exploitant des systèmes informatiques la possibilité de contrôler, par des inspections de sécurité, que les utilisateurs cantonaux et communaux respectent les règles fixées pour la mise en place des connexions et les principes de sécurité.

268 Normes pour les demandes d'autorisation

Le Conseil fédéral fixe les normes auxquelles doivent répondre les demandes visant à établir une liaison «online» dans le domaine de la police.

269 Contrôle d'utilisation

Le Conseil fédéral veille à ce que les liaisons «online» dans le domaine de la police fassent l'objet de contrôles réguliers visant à déterminer la fréquence d'utilisation.

2610 Collaborateurs du Centre de calcul du DFJP. Contrôles de sécurité

Le Conseil fédéral instaure des contrôles de sécurité pour les collaborateurs du Centre de calcul du DFJP. En effet, ces personnes ne sont aujourd'hui soumises à aucun contrôle de sécurité, bien qu'elles aient accès à des données particulièrement sensibles (informations personnelles, données concernant la police, la sécurité de l'Etat, etc.).

2611 Emplacement du Centre de calcul du DFJP

Le Conseil fédéral veille à ce que le Centre de calcul du DFJP soit installé dans un lieu plus approprié.

2612 Fusion de KOMBV-KTV et DFJP-WAN

Le Conseil fédéral se prononce le plus rapidement possible sur l'opportunité d'opérer une fusion de KOMBV-KTV et de DFJP-WAN.

27 Suite de la procédure

La commission invite le Conseil fédéral à faire connaître son avis sur le présent rapport et sur les recommandations qu'il contient d'ici à la fin du mois de février 1999.

Au nom de la Commission de gestion du Conseil des Etats

Le président, Peter Bieri, conseiller aux Etats

Au nom de la section «Autorités»

Le président, Pierre Aeby, conseiller aux Etats

La secrétaire des Commissions de gestion, Mariangela Wallimann-Bornatico

Annexe 1: Rapport d'expert et résultats de la procédure de consultation (pas publié dans la FF)

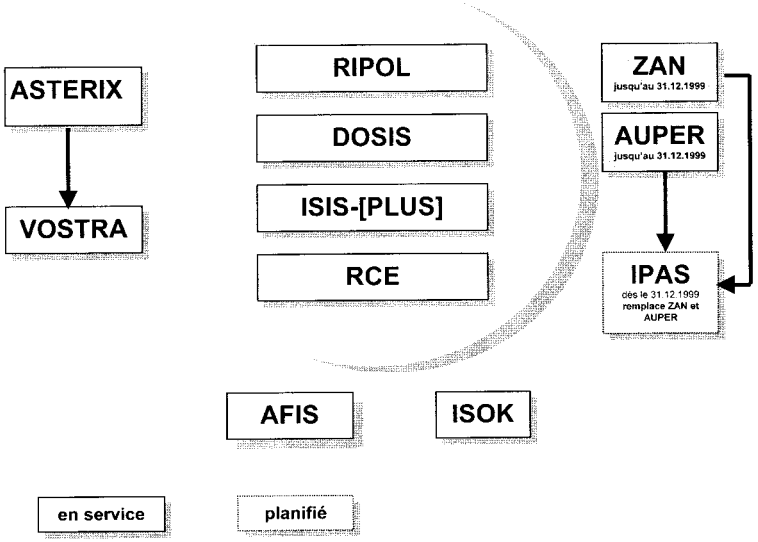
Annexe 2: Abréviations

Annexe 3: Sommaire des systèmes

Abréviations

ABI	«Automation Büro Innendienst»
AFIS	Système automatique d'identification des empreintes digitales (Automatic Fingerprints Identification System)
AUPER	Système d'enregistrement automatisé des personnes
CCF	Service de contrôle administratif du Conseil fédéral
CF	Conseil fédéral
CdG-E	Commission de gestion du Conseil des Etats
CdG-N	Commission de gestion du Conseil national
CIC	Conférence informatique de la Confédération
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
DFJP-WAN	Département fédéral de justice et police «Wide-Area-Network»
DOSIS	Système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants
HERMES	(Procédure HERMES) Conduite et déroulement de projets informatiques / Standard de l'Office fédéral de l'informatique
ISIS	Système provisoire de traitement des données relatives à la protection de l'Etat
ISIS-Plus	Projet de système de traitement des données relatives à la protection de l'Etat avec accès «online» des autorités cantonales
ISOK	Système provisoire de traitement de données en matière de lutte contre le crime organisé
KOMBV-KTV	«Kommunikation der Bundesverwaltung – Kantonalverbund»
LMSI	Projet de loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LPD	Loi fédérale sur la protection des données du 19 juin 1992 [RS *235.1*]
LSEE	Loi fédérale sur le séjour et l'établissement des étrangers
MPC	Ministère public de la Confédération
online	(Liaisons «online») Liaisons en ligne; accès par procédure d'appel; accès directs à des systèmes informatiques
OFI	Office fédéral de l'informatique
OFP	Office fédéral de la police
OLPD	Ordonnance relative à la loi sur la protection des données du 14 juin 1993
OPCA	Organe parlementaire de contrôle de l'administration
PFPD	Préposé fédéral à la protection des données
RCE	Registre central des étrangers (= ZAR: Zentrales Ausländerregister)
RIPOL	Système de recherches informatisées de police
ZAN	Index central des dossiers (Zentraler Aktennachweis)

Sommaire des systèmes



Système	Nom	Compétences et responsabilité
RIPOL Art. 1 et 4 ordonnance RIPOL	**Système de recherches informatisées de police**	*Office fédéral de la police*
DOSIS Art. 19 ordonnance DOSIS	Système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants	*Office fédéral de la police*
ISIS-[PLUS] Art. 1er et 23. 1er al. ordonnance ISIS	**Système provisoire de traitement des données relatives à la protection de l'Etat**	*Ministère public de la Confédération* Chef de la Police fédérale
RCE Art. 1 ordonnance RCE	**Registre central des étrangers**	*Office fédéral des étrangers*
ZAN	I**ndex central des données**	*Office fédéral de la police* – Section d'identification – Offices centraux *Bureau central suisse de police Interpol*

Système	Nom	Compétences et responsabilité
AUPER Art. 3 ordonnance AUPER	**Système d'enregistrement des personnes**	*Office fédéral des réfugiés* *Office fédéral de la police* – Division de l'entraide judiciaire internationale et des affaires de police – Bureau central de police – Section assistance des Suisses de l'étranger – Section de la nationalité *Office fédéral des étrangers* *Service des recours et Service financier du DFJP* *Commission de recours en matière d'asile*
IPAS Nouv. art. 351^{octies}, 1er al. CP	**Système informatisé de gestion et d'indexation de dossiers et de personnes**	*Office fédéral de la police*
AFIS Art. 6 ordonnance conc. le Service d'identification de l'OFP	Système automatique d'identification des empreintes digitales	*Office fédéral de la police* Section d'identification
ISOK Art. 21, 1er al. ordonnance ISOK	**Système de traitement des données en matière de lutte contre le crime organisé**	*Office fédéral de la police*
VOSTRA Art. 1, al. 1bis, 1ter, 1^{quater} ordonnance sur le casier judiciaire		

40304