Annexe 1

Mise en place de liaisons "online" dans le domaine de la police

Rapport d'expert sur la pratique de l'administration fédérale

à l'intention de la section "Autorités"
de la Commission de gestion du Conseil des Etats

avec appendice 1:
Évaluation et résumé de la procédure de consultation interne à l'administration

Document	C:\Eigene Dateien\ONLINE\Expertenbericht.doc
Version:	4.0 document final
Date:	30/07/1998
Remplace le document du:	30/06/1998
Auteur:	©Lukas Fässler, licencié en droit, avocat, Hirschmattstrasse 36, 6002 Lucerne
Dernière modification le:	30.7.1998
Autorisés:	Section Autorités des la CdG-CE; OPCA; Offices fédéraux concernés, ainsi que le SG du DFJP et le SG du DF; Lukas Fässler, Lucerne
Distribué le:	1.8.1998

Original: allemand

Inhaltsverzeichnis

1 MANDAT DE L'EXPERT

11 Champ de l'examen

L'Organe parlementaire de contrôle de l'administration (OPCA) a été mandaté par la Commission de gestion du Conseil des Etats (CdG-CN) pour évaluer la **mise en place de liaisons « online »** (en ligne) **dans le domaine de la police**. Selon mandat[1], le présent rapport d'expertise concerne la problématique du 2e bloc. Les domaines et les questions au premier plan du présent examen sont les suivants :

- Situation initiale
  a) Présentation de la situation actuelle des accès en ligne déjà en service vers les systèmes d'information en matière de police retenus par la CdG CE à ce stade de l'analyse.

- Perspectives de développement
  a) Perspectives d'avenir en matière de développement et bases de planification des mises en place d'accès en ligne aux systèmes d'information en matière de police.

- Procédure
  a) Examen des conditions, procédures et compétences exactes en vigueur lors de la planification et de la mise en place d'accès en ligne aux systèmes d'information en matière de police.
  b) Selon quelles procédures et comment la mise en place des accès en ligne est-elle réalisée lorsque ces accès ont déjà été planifiés au cours du développement du système d'information concerné ?
  c) Selon quelles procédures et comment la mise en place des accès en ligne est-elle réalisée lorsque ces accès ont été planifiés après coup ?

- Bases légales
  a) Quelles sont les bases légales qui ont été élaborées afin de justifier légalement les accès aux systèmes d'information en matière de police ?
  b) Comment la question de l'élaboration des bases légales nécessaires est-elle examinée ?

- Projets pilotes
  a) Comment et en vertu de quelles conditions procède-t-on dans le cadre des « projets pilotes » qui deviennent de plus en plus nombreux ?
  b) Quelles sont les bases légales particulières qui sont élaborées pour ces projets pilotes ?

- Procédure de consultation / droit d'être entendu
  a) Quels sont les organes qui sont entendus dans le cadre de la procédure de mise en place d'accès en ligne à des systèmes d'information ?

- Contrôle
  a) Quelles sont les mesures de contrôle qui sont prises ?

---

1 *Contrat d'expertise du 21 octobre 1997 avec cahier des charges, chiffres 22 et ss.*

- Coûts
  a) Lorsque les cantons ont accès à un système d'information, quelle est la clé de répartition des coûts entre la Confédération et les cantons ?
  b) Qui assume concrètement les coûts d'une liaison directe entre la Confédération et les cantons ?

- Protection des données et sécurité des données
  a) Quelles mesures de sécurité ont-elles été prévues ou sont-elles prises en pratique ?
  b) Quelles sont les garanties exigées par les cantons en matière de respect de la légalité et de protection des données ?

- Archivage
  a) Quelles sont les procédures appliquées en matière d'archivage des données de ces systèmes informatiques ?

12 Problématiques

Les champs d'examen évoqués ci-dessus nécessitent de répondre aux questions de détail résumées dans le tableau synoptique ci-dessous. Ce tableau constitue la base et le profil directeur des entretiens personnels avec les personnes de contact indiquées.

Champ d'examen	Problématique
Situation initiale	- Vérification des listes chronologiques (tableau des accès en ligne) et précisions en relation avec d'éventuelles questions qui en découlent (termes, abréviations etc.). - Des différences par rapport à la situation initiale au moment de l'audition peuvent-elles être constatées ?
Perspectives de développement	- Quels sont les nouveaux accès en ligne qui sont planifiés pour les deux prochaines années (1998 et 1999) ? - Quels sont les unités administratives (nouveaux utilisateurs) concernés ? - Quels sont les unités administratives (propriétaires des données) responsables ? - Qui est responsable du projet correspondant ? - A quel stade de planification les diverses étapes de développement se trouvent-elles ? - Quels sont les documents relatifs à ce sujet (étude préliminaire, concept, concept de détail, plan d'exécution, organisation de projet, manuel de projet) ?
Procédures **a)** lorsque les accès en ligne ont **déjà** été planifiés au cours du développement du système	- Quelle est la procédure en matière d'accès en ligne par des tiers ? - Qui est compétent pour quoi ? - A quel endroit les procédures, les tâches, les compétences et les responsabilités sont-elles réglées ? - Y a-t-il une autorité compétente en matière d'autorisation ? - Comment la gestion de projet est-elle assurée ? - Comment le contrôle du projet est-il assuré ? - Comment la sécurité et la protection des données sont-elles assurées ?

b) lorsque le besoin de ces accès apparaît **après coup**	- Des exemples concrets d'accès en ligne installés après coup (également pour une durée limitée) sont-ils concernés par le présent examen ? - Quelle est la procédure en matière d'accès pour des tiers ? - Qui est compétent pour quoi ? - A quel endroit les procédures, les tâches, les compétences et les responsabilités sont-elles réglées ? - Y a-t-il une autorité compétente en matière d'autorisation ? - Comment la gestion de projet est-elle assurée ? - Comment le contrôle du projet est-il assuré ? - Comment la sécurité et la protection des données sont-elles assurées ? - Comment la procédure de suppression des accès en ligne limités dans le temps est-elle réglée ? - Quelle est la documentation disponible au sujet des accès en ligne installés après coup (cas concrets) ?
Bases légales	- Quelles sont les bases légales régissant les accès en ligne ? - lorsque les accès en ligne sont planifiés à l'avance - lorsque les accès en ligne deviennent nécessaires après coup - Qui entreprend de contrôler les principes en vigueur en matière de délégation de la responsabilité des accès en ligne à l'unité administrative compétente ? - Dans le cadre de quelle procédure ce contrôle est-il effectué ? - De quelle manière les résultats de ce contrôle sont-ils traités ?
Projets pilotes	- Quels sont les accès en ligne concernés par le présent examen qui ont été installés dans le cadre de projets pilotes ? - Quels sont les écarts constatés par rapport à la procédure et aux bases de la gestion de projet ordinaire ? - Le cas échéant, comment ces écarts sont-ils traités ? - Les projets pilotes sont-ils soumis à des instances ou à des mesures de contrôle supplémentaires ? - Quelles sont les bases légales qui permettent la mise en place d'accès en ligne dans le cadre de chaque projet pilote concerné ?
Procédure de consultation Droit d'être entendu	- Quels sont les organes de l'office, du département et de toute l'administration qui sont entendus lors de la mise en place d'un accès en ligne ? - Y a-t-il des bases légales, des directives ou des instructions à ce sujet ? - De telles prises de positions sont-elles consignées ? - Qui est responsable du respect et de la mise en œuvre des points à respecter indiqués par les services entendus et consultés ? - Comment procède-t-on en cas de divergences

	d'opinion ?
Contrôle	- Quelles sont les mesures de contrôle qui sont prises au niveau de la *gestion du projet* en matière de respect des exigences légales et des points à respecter imposés ou convenus ? - Quelles sont les mesures de contrôle qui sont prises au niveau de l'*exploitation courante* (utilisation concrète et maintenance) en matière de respect des exigences légales et des points à respecter imposés ou convenus ?
Coûts	- Comment les coûts d'investissement et d'exploitation des accès en ligne sont-ils budgétisés et imputés, tant à l'intérieur qu'à l'extérieur de l'administration ? - A l'intérieur de l'administration fédérale, les coûts des accès en ligne sont-ils répartis sur les utilisateurs ? - Le centre de service ou le responsable des données facture-t-il les coûts des prestations au sein de l'administration ? - Comment les coûts de mise en place (coûts d'investissement) et d'exploitation des accès en ligne de services hors de l'administration fédérale sont-ils budgétisés et facturés ? - En vertu de quelles bases légales les questions concernant les coûts sont-elles réglées (facturation et imputation) ?
Protection des données **Sécurité des données**	- Lors de la mise en place d'accès en ligne dans le cadre de projets ordinaires, qui est-ce qui élabore les concepts de protection et de sécurité des données et comment ? - Est-ce que de tels concepts existent déjà pour les accès actuels ? - Lors de la mise en place d'accès en ligne dans le cadre de projets pilotes, qui est-ce qui élabore les concepts de protection et de sécurité des données et comment ? - Ces concepts sont-ils soumis à des tiers à titre de consultation, en vue d'examen voire pour autorisation ? - Est-il possible de trouver des exemples concrets de telles procédures de consultation, d'examen et d'autorisation relatifs à des systèmes examinés ? - Comment ces questions sont-elles traitées lors d'accès en ligne par des tiers (cantons) ? - Y a-t-il des exemples concrets à ce sujet ? - Quelles sont les garanties exigées par les cantons en matière de respect de la légalité et de la protection des données ? - Des contrats d'exploitation des banques de données concernées (réglant les responsabilités, la protection des accès, les droits d'accès ainsi que les questions de responsabilité civile et pénale) ont-ils été conclus avec les cantons ? Si oui, de tels contrats peuvent-ils être produits ?
Archivage	- Comment l'archivage des données des systèmes d'infor-

	mation concernés est-il effectué concrètement ? - A ce sujet, quelles sont les dispositions à respecter ? - En matière d'archivage, qui est responsable de l'initialisation, de la réalisation et du transfert des données ?

Toutes les questions ci-dessus n'ont pas été traitées à l'occasion des auditions personnelles des responsables des systèmes examinés. Dans certains cas au vu de la situation initiale (pas de projet pilote en cours, pas d'accès en dehors de l'administration fédérale) elles n'étaient pas pertinentes, dans d'autres il a été possible d'y répondre au moyen d'une documentation fournie par les organes concernés.

Le présent tableau de questions a été distribué à chaque responsable de manière à lui permettre de se préparer en vue de l'entretien personnel avec l'expert.

13 Procédure

L'élaboration du présent rapport d'expertise a été coordonnée en collaboration avec l'OPCA en fonction de la planification de l'ensemble du projet. Tout d'abord, les organes compétents pour les systèmes informatiques choisis ont été priés de fournir une documentation sur le développement des systèmes analysés (dossier d'initialisation, analyse préliminaire, concept, réalisation, mise en œuvre, exploitation, entretien ainsi que nouveaux développements) ainsi que les bases légales qui ont été mises en place pour justifier ces systèmes et leurs accès du point de vue légal. Parallèlement, les organes concernés ont établi un tableau des accès en ligne actuels à l'attention de l'OPCA et de l'expert. Ce tableau comporte les données suivantes : partenaires de liaison, données concernant les liaisons, nombre d'utilisateurs, motifs juridiques, réseaux de communication utilisés, protocole de communication, droits d'accès techniques ainsi que mesures de sécurité. Ce tableau présenté de manière chronologique constitue une première vue d'ensemble des accès en ligne aux systèmes d'information en matière de police. Après l'analyse de ces documents, des auditions avec des représentants de divers organes ont été réalisées selon l'aperçu ci-dessous.

Date	Organe	Domaine examiné	Personne entendue
2.2.1998	**Office fédéral de la police**	RIPOL et DOSIS	• Adrian Lobsiger Adjoint de la direction • Arnold Bolliger Chef de la division des Services spéciaux
3.2.1998	**Office fédéral des étrangers**	RCE	• Christoph Müller Adjoint de la direction • Bernhard Hayoz Chef suppléant de la section registre central des étrangers/Statistique Chef de projet utilisateurs OFE • Claudio Hayoz Conseiller à la protection des données OFE • Rudolf Müller Projet informatique OFE

11.2.1998	**Police fédérale**	ISIS ISIS-PLUS	• Christoph Herrli Chef d'évaluation préliminaire de l'information et exploitation

Une fois la documentation et les dossiers remis par les représentants des organes fédéraux cités, l'expert les a analysés par domaine d'examen. Il a ensuite évalué les résultats de cette enquête pour les intégrer au présent rapport d'expert.

Les premiers résultats du présent rapport d'expertise ont été présentés à la section « Autorités » de la Commission de gestion du Conseil des Etats le 6 mai 1998. Suite à cette séance, l'expert a analysé la série des documents demandés ultérieurement et a intégré les résultats de cette analyse dans le présent rapport. Les 1er et 2 juin 1998, l'expert a informé l'Office fédéral de la police, la Police fédérale, l'Office fédéral des étrangers ainsi que le Centre de calcul du DFJP au sujet des résultats principaux de l'expertise. Suite à ces explications, la procédure de consultation interne a été lancée. Le délai pour les prises de position a été arrêté au 23 juillet 1998. Les résultats de cette procédure de consultation interne sont présentés dans un document séparé intitulé « Supplément 1, Evaluation et résumé de la procédure de consultation interne (version 1.0) » du 30 juillet 1998.

Le projet final de ce rapport d'expertise a été remis à l'Organe parlementaire de contrôle de l'administration le 27 avril 1998.

2 BASES LEGALES ET PRINCIPES REGISSANT LES ACCES EN LIGNE

Le présent chapitre a pour but de présenter un bref aperçu des bases légales (lois, ordonnances, stratégies, instructions, directives, normes et standards) et des principes régissant la préparation, la mise en œuvre et l'exploitation de systèmes informatiques ouverts à des tiers ou destinés à le devenir (accès en ligne existants ou planifiés).

*Par « **accès en ligne** » il faut comprendre chaque traitement informatique généralement en temps réel réalisé par un utilisateur sur un système informatique, ou au moyen d'une application spécialisée d'un système informatique, par le truchement d'une infrastructure de communication.* La présente étude concerne exclusivement les systèmes informatiques RIPOL, DOSIS, ISIS (-PLUS) et RCE qui sont mis à disposition de tiers au sein ou à l'extérieur de l'administration fédérale.

21 Bases légales dans le domaine de la police

Tous les systèmes d'information examinés [RIPOL, DOSIS, ISIS (-PLUS) et RCE] sont sous la responsabilité d'unités organisationnelles de la Confédération, et ces dernières sont soumises aux directives de sécurité de l'Office fédéral de l'informatique (OFI). Pour cette raison, les principes et les objectifs en matière de sécurité informatique s'appliquent également à ces systèmes. Par conséquent, bien que non exhaustifs, les actes législatifs ci-dessous sont déterminants en tant que dispositions de droit supérieur :

a) Loi fédérale sur la protection des données du 19 juin 1992 (LPD) RS 235.1.
b) Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD) RS 235.11.
c) Ordonnance portant création de l'Office fédéral de l'informatique et réglant la coordination de l'informatique au sein de l'administration fédérale du 11 décembre 1989 (OINFAF) RS 172.010.58.
d) Ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale du 10 juin 1991, RS 172.010.59.
e) Ordonnance sur la classification et le traitement d'informations de l'administration civile du 10 décembre 1990, RS 172.015.

Ces bases légales permettent de déduire les **principes de planification, de mise en œuvre et d'exploitation d'accès en ligne dans le domaine de la police** suivants :

1. Les organes fédéraux et, par conséquent, les autorités cantonales (au sens de l'article 24, 1er et 4e alinéas LPD) ne sont en droit de traiter des données personnelles que s'il existe une base légale (article 17, 2e alinéa LPD). Les données sensibles ne peuvent être traitées que si une loi au sens formel le prévoit expressément (article 17, 2e alinéa LPD)

2. Des données personnelles ne peuvent être rendues 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 (article 19, 3e alinéa LPD).

Principe 1 :
Il faut des bases légales pour le traitement (en ligne) de données personnelles.

Principe 2 :
Il faut une loi au sens formel pour le traitement (en ligne) des données sensibles ou des profils de la personnalité.

3. Dans la mesure où des autorités cantonales accomplissent des tâches fédérales en matière de lutte contre le terrorisme, l'extrémisme violent, le crime organisé, le service de renseignements prohibés ou pour garantir la sécurité militaire, elles sont soumises au droit fédéral sur la protection des données (article 24, 1er et 4e alinéas LPD).

Principe 3 :
Les principes de la Confédération en matière de protection des données s'étendent également aux autorités cantonales qui accomplissent des tâches fédérales.

4. Avant qu'un organe de la Confédération puisse installer un accès en ligne, il est nécessaire de vérifier tout d'abord si cet accès est nécessaire et s'il est compatible avec les principes de la proportionnalité et de l'opportunité (conformité avec le but). Ce principe découle de l'article 4, 2e et 3e alinéa LPD.

Principe 4 :
La mise en place d'un accès en ligne n'est possible que s'il est nécessaire et qu'il respecte les principes de la proportionnalité et de l'opportunité.

Principe 5 :
Ces principes (4) doivent être vérifiés avant la mise en place de tout accès en ligne.

5. En collaboration avec les organes compétents, le responsable de l'application doit évaluer les risques tant pour les accès en ligne prévus lors du développement du système que pour les accès en ligne devenant nécessaires après coup. En particulier, il faut garantir une protection suffisante des communications. Dans ce domaine, il convient de prendre les mesures de protection adéquates (article 1er, 2e alinéa, lettre d, articles 3 et 4 de l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, RS 172.010.59).

Principe 6 :
Il est nécessaire d'entreprendre une évaluation des risques avant la mise en place de tout accès en ligne.

6. Les organes de la Confédération doivent prendre les mesures techniques et organisationnelles en matière de protection et de sécurité des données (articles 8, 9 et 20, 1er alinéa OLPD, RS 235.11). Ils doivent assurer que les systèmes et applications informatiques sont protégés contre les influences extérieures et contre tout accès non autorisé lors de leur planification, de leur réalisation et de leur exploitation (article 1er, 1er, 2e et 4e alinéas de l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, RS 172.010.59).

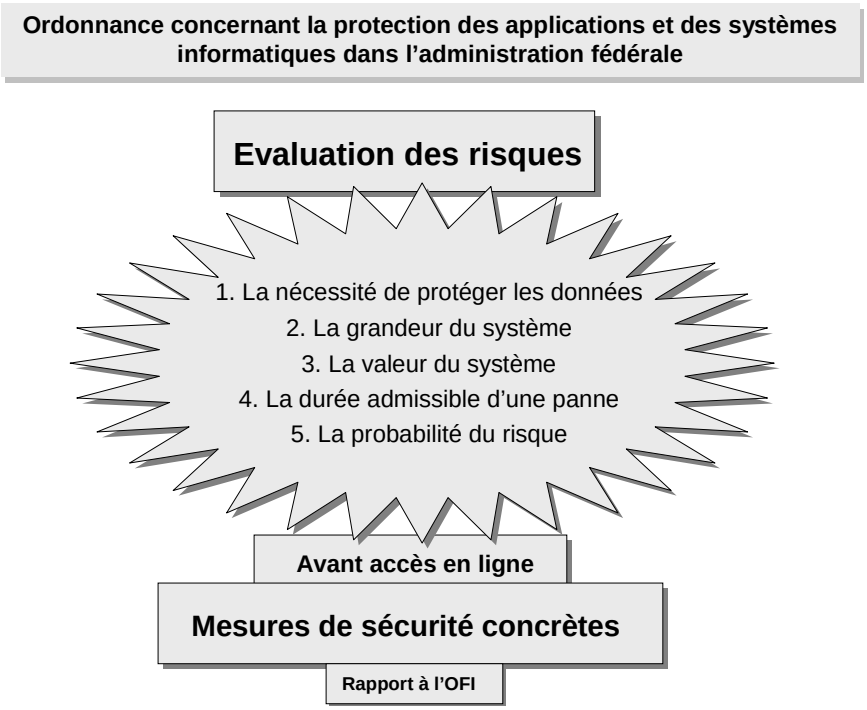


Illustration : Schéma de base relatif aux articles 3 et 4 de l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale.

Principe 7 :
Il est nécessaire de prendre des mesures techniques et organisationnelles appropriées en matière de protection des données contre les influences extérieures et contre tout accès non autorisé avant la mise en place de tout accès en ligne.

7. Les mesures de sécurité doivent être contrôlées régulièrement pour savoir si elles sont toujours d'actualité (article 6, 3e alinéa de l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, RS 172.010.59) et la planification de systèmes doit être déclarée en temps utile au Préposé fédéral à la protection des données (article 11, 2e alinéa LPD) et à l'OFI (article 7, 1er alinéa de l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, RS 172.010.59). Tous les nouveaux projets informatiques ainsi que toutes les modifications importantes d'applications existantes doivent être annoncés à l'OFI au moyen d'une proposition de projet selon HERMES (article 2 de la directive technique numéro 3).

   Par « importantes » il faut comprendre les modifications qui impliquent
   - une modification des bases légales en vigueur,
   - une charge en personnel qui dépasse l'équivalent de deux années de travail d'un collaborateur,
   - une charge impliquant un décaissement de plus de 200'000 francs.

Principe 8 :
Il est nécessaire de déclarer toute planification, modification et nouvelle conception de systèmes informatiques au Préposé fédéral à la protection des données et à l'OFI.

Principe 9 :

Il est nécessaire de contrôler régulièrement les mesures de sécurité pour savoir si elles sont toujours d'actualité et les adapter aux directives techniques de l'OFI en vigueur.

8. L'Office fédéral de l'informatique établit (article 3, 1er alinéa, lettre c OINFAF RS 172.010.58) les instructions et directives nécessaires (article 3, 2e alinéa, lettre l OINFAF RS 172.010.58) d'entente avec les autres organes compétents (article 5, 2e alinéa de l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, RS 172.010.59). Les directives techniques et les décisions de portée générale de la Conférence informatique de la Confédération (CIC) s'étendent à l'ensemble des unités administratives de la Confédération (article 58 de la loi fédérale sur la procédure administrative), à l'exception de l'Entreprise des PTT et des Chemins de fer fédéraux.

   Dans le cadre de ces dispositions, il convient en particulier de respecter les directives suivantes :

   Directives techniques
   - DT 03 Annonce des projets informatiques à l'OFI, du 22 août1990.
   - DT 08 Manuel pour les chefs de projets LAN, du 16 octobre 1996.
   - DT 09 Conventions de noms SNA / SNI – 92, du 16 septembre1992.
   - DT 11 Domain Name System (DNS), du 13 novembre 1996.
   - DT 16 Conduite de projet et développement de systèmes dans le cadre de projets informatiques, du 19 avril 1995 ainsi que Manuel HERMES, édition 1995.
   - DT 17 Adressage NSAP (Network Service Access Point), du 18 octobre 1995.
   - DT 18 World Wide Web (WWW) dans l'administration fédérale du 15 janvier 1997.

   Directives en matière de sécurité informatique
   - DS S01 Identification des utilisateurs et mots de passe, du 18 août 1993 ainsi que Fiche technique sur l'utilisation des mots de passe dans l'administration fédérale, de décembre 1993.
   - DS S02 Protection de base des systèmes et applications informatiques, du 19 avril 1995.
   - Manuel numéro 1 pour la DS S02 : Procédure pour le traitement des listes de contrôle et catalogue complet des mesures de protections fondamentales du 1er octobre 1996.
   - DS S03 Application de la *Network Security Policy* (NSP), du 25 juin 1997.

9. L'office fédéral compétent doit régler les détails du traitement des données, donc également des accès en ligne, dans un **règlement de traitement**, respectivement au moyen de **directives en matière de mesures organisationnelles et techniques**.
   - Pour le RIPOL : article 4, 1er alinéa ordonnance RIPOL,
   - Pour DOSIS : article 9, 4e alinéa ordonnance DOSIS,
   - Pour le RCE : article 7, 4e alinéa ordonnance RCE,
   - Pour ISIS : article 5, 3e alinéa et article 20, 2e alinéa ordonnance ISIS.

Principe 10 :

Il est nécessaire d'édicter des règlements de traitement et de régler les mesures organisationnelles et techniques par la voie de directives.

22 Résumé

En résumé, les principes suivants s'appliquent aux accès en ligne dans le domaine de la police :

Principes régissant les accès en ligne
1. Il faut des bases légales pour le traitement en ligne de données personnelles.
2. Il faut une loi au sens formel pour le traitement en ligne de données sensibles ou de profils de la personnalité.
3. Les principes de la Confédération en matière de protection des données s'étendent également aux autorités cantonales et communales qui accomplissent des tâches fédérales.
4. La mise en place d'accès en ligne n'est possible que si ces derniers sont nécessaires et qu'ils respectent les principes de la proportionnalité et de l'opportunité.
5. Il est nécessaire d'examiner la nécessité, la proportionnalité et l'opportunité des accès en ligne avant leur mise en place.
6. Il est nécessaire d'entreprendre une évaluation des risques avant la mise en place de tout accès en ligne.
7. Les organes responsables prennent des mesures techniques et/ou organisationnelles appropriées en matière de protection des données contre les influences extérieures et contre tout accès non autorisé avant la mise en place de tout accès en ligne.
8. Il est nécessaire de déclarer toute planification, modification et nouvelle conception de systèmes informatiques au Préposé fédéral à la protection des données et à l'OFI.
9. Il est nécessaire de contrôler régulièrement les mesures de sécurité pour savoir si elles sont toujours d'actualité et les adapter aux directives techniques de l'OFI en vigueur.
10. Il est nécessaire d'édicter des règlements de traitement ainsi que des directives.

Tableau : Résumé des principes régissant les accès en ligne.

3 RESULTATS DE L'EXAMEN

31 RIPOL

311 Bases et principes légaux

Les bases légales suivantes sont déterminantes dans le domaine du système de recherche informatisé de personnes et d'objets (RIPOL) :

1. Code pénal suisse (RS 311.0 ; article 351bis CP en particulier),
2. Ordonnance sur le système de recherches informatisées de police du 19 juin 1995 (ordonnance RIPOL, RS 172.213.61),
3. Instructions de l'Office fédéral de la police concernant la mise en service de RIPOL 2 du 25 juin 1990,
4. *Benutzer- und Wartungsreglement « automatisiertes Fahndungssystem des Bundesamtes für Polizeiwesen »* de mai 1987, en allemand uniquement (cité par la suite : règlement d'utilisation et de maintenance de l'OFP de mai 1987)

Ces bases légales permettent de déduire les principes relatifs à l'autorisation par les autorités fédérales compétentes d'accès en ligne dans le domaine de la police suivants :

L'Office fédéral de la police (OFP) assume la responsabilité du système RIPOL. Il coordonne ses activités avec les autorités fédérales et cantonales qui participent au RIPOL. L'OFP délivre aux utilisateurs concernés les autorisations nécessaires à l'emploi du système et veille à ce que la présente ordonnance et les instructions y relatives soient respectées (article 4, 1er alinéa ordonnance RIPOL). Les divers droits de traiter des données enregistrées dans le RIPOL (article 6, 1er alinéa ordonnance RIPOL) sont réglés dans une annexe séparée jusqu'au niveau de chaque champ (A = visualisation, B = contrôle si enregistré ou pas, C = visualisation uniquement des étrangers enregistrés, M = mutation). Pour assurer la sécurité des données, les transmissions de données aux représentations suisses à l'étranger assumant des tâches consulaires ainsi qu'aux services étrangers d'Interpol interviennent en la forme chiffrée (article 17, 1er alinéa ordonnance RIPOL). Les autorités concernées adoptent, dans leur domaine, les mesures organisationnelles et techniques qui s'imposent conformément aux dispositions légales sur la protection des données. L'accès au RIPOL est protégé au moyen de profils individuels d'utilisateurs et de mots de passe. Les autorités directement raccordées au RIPOL (par des accès en ligne) réglementent les autorisations d'accès aux terminaux et protègent efficacement les locaux de travail contre tout accès indu (article 17, 2^{e}, 3^{e} et 4^{e} alinéas ordonnance RIPOL). Le Centre de calcul du DFJP (CC DFJP) veille à ce que les données et les programmes du RIPOL puissent être reconstitués en cas de panne, de vol ou de perte (article 17, 5^{e} alinéa ordonnance RIPOL).

Selon le règlement d'utilisation et de maintenance de l'OFP de mai 1987, le groupe de projet RIPOL (constitution voir chiffre 6.1 du règlement) est responsable de l'examen des souhaits d'extension, c'est-à-dire des développements supplémentaires du projet. L'OFP (les compétences internes ne sont pas précisées) décide des demandes de raccordement des utilisateurs fédéraux du projet. Le service informatique du DFJP est responsable de la réalisation des demandes de raccordement budgétisées (chiffre 713 du règlement). En ce qui concerne les rapports avec les cantons raccordés, les développements du projet et les modifications importantes du logiciel ainsi que les adaptations par l'OFP, ils sont communiqués au Groupe de travail « informatique » de la commission technique des polices suisses. Les demandes de raccordement et d'augmentation du nombre de terminaux d'accès doivent être remises par écrit par le commandement de la police concerné

directement à l'OFP (chiffre 712 du règlement : Office fédéral de la police, *suite à la réorganisation, la désignation de cette unité organisationnelle n'est plus en vigueur*). La décision correspondante est prise par l'OFP qui détermine le moment de la réalisation du raccordement (chiffre 81 du règlement).

312 Situation actuelle en matière de liaisons en ligne

Nombre d'utilisateurs

Selon la liste chronologique du 26 novembre 1997 des liaisons en ligne avec le RIPOL, dont l'actualité a été confirmée lors de l'audition du 2 février 1998,

13'234 utilisateurs

ont été reliés au RIPOL depuis 1984 jusqu'à aujourd'hui.

Catégories d'utilisateurs

La légitimité de tous les utilisateurs raccordés au moyen de liaisons en ligne découle de l'article 351bis CP. Les modalités d'exploitation de ce système d'information par ces diverses catégories d'utilisateurs ont été concrétisées par le Conseil fédéral dans l'ordonnance RIPOL (article 3 ordonnance RIPOL).

Réseau et mesures de sécurité

Tous les partenaires raccordés communiquent par le truchement d'infrastructures de la Confédération (LIS/DFJP, WAN-DFJP, KOMBV3 ou KOMBV4). La communication est effectuée par TCP/IP, par X.25 ou SNA (protocoles de communication normalisés). Les mesures de sécurité sont en partie basées sur des logiciels (chiffrages *end-to-end* ou par lien sur le réseau de base du DFJP) et en partie sur une isolation au moyen un mur coupe-feu. Ces mesures sont destinées à empêcher que des données non protégées puissent transiter en clair par les réseaux de communication.

313 Procédure de raccordement

En ce qui concerne les tâches, les compétences et les responsabilités en matière d'accès directs d'utilisateurs internes ou externes à l'administration, il faut tout d'abord se référer à la norme de délégation de compétences de l'article 351bis, 4^{e} alinéa, lettre b CP. Ensuite, le législateur a édicté des normes concrètes relatives aux liaisons en ligne en définissant de manière exhaustive les autorités (fédérales et cantonales) qui ont le droit d'utiliser le RIPOL (article 351bis, 2^{e} et 3^{e} alinéas CP). Il spécifie les droits d'utilisation au moyen de deux notions :

- ***diffuser*** des signalements par le RIPOL (article 351bis, 2^{e} alinéa CP)
- ***obtenir*** des données par le RIPOL (article 351bis, 3^{e} alinéa CP).

Au 4^{e} alinéa de l'article 351bis CP, le législateur charge le Conseil fédéral de désigner *les autorités qui peuvent introduire directement des données dans le RIPOL, celles qui peuvent le consulter et celles auxquelles des données peuvent être communiquées de cas en cas*. Le Conseil fédéral s'est conformé à cette disposition dans la mesure où il a défini les autorités concernées (article 3 ordonnance RIPOL) ainsi que les responsabilités du système d'information (article 4 ordonnance RIPOL). Dans l'article 3 de l'ordonnance RIPOL, le Conseil fédéral énumère les autorités qui peuvent

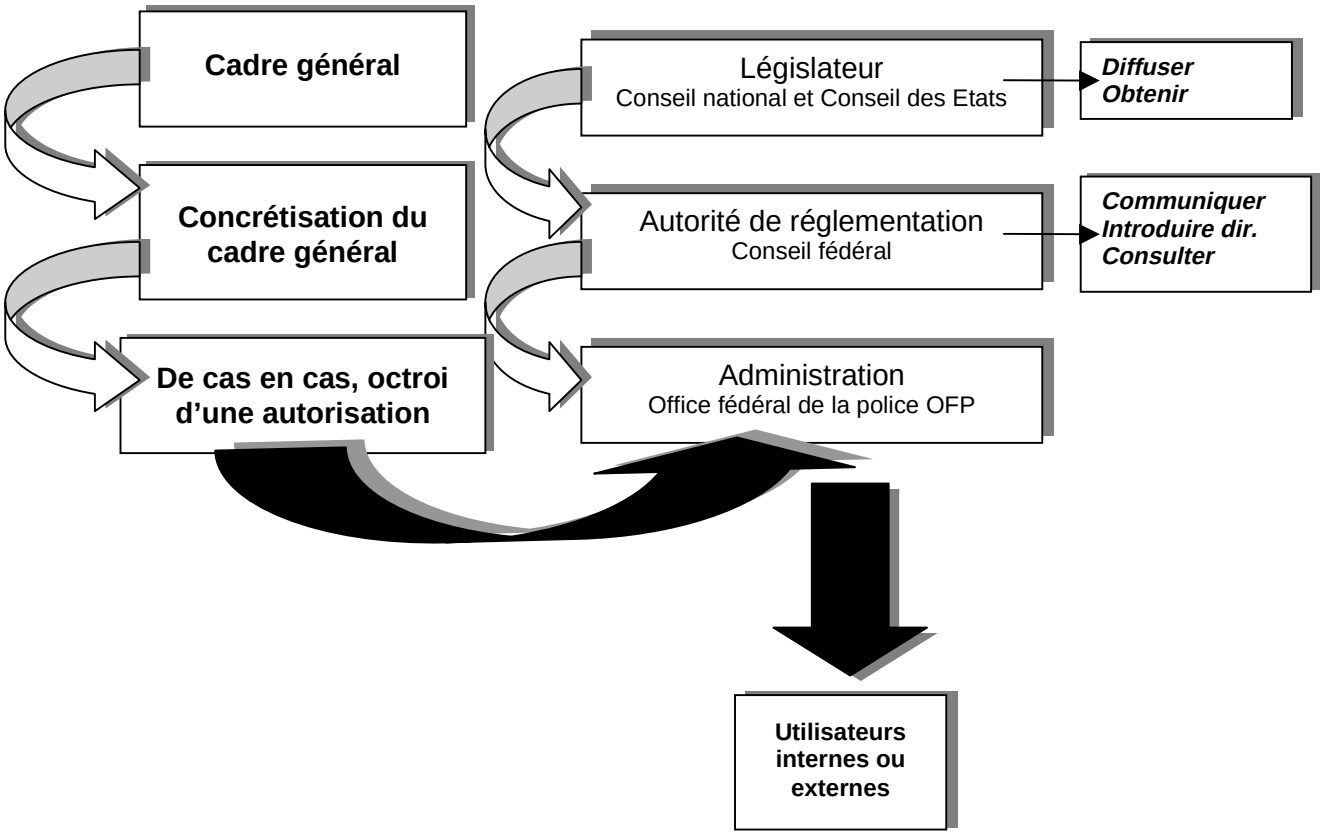
- ***communiquer*** des signalements à l'OFP (article 3, 1er alinéa ordonnance RIPOL)
- ***introduire directement*** des signalements dans le système (article 3, 2^{e} alinéa ordonnance RIPOL)
- ***consulter*** des données directement (en ligne) (article 3, 3^{e} alinéa ordonnance RIPOL).

Tout d'abord il est possible de constater que, sous le titre de « Système de recherche informatisé de police », le législateur lui-même a défini un certain nombre d'autorités en tant qu'utilisateurs du système (article 351bis, 2^{e} et 3^{e} alinéas CP). Il définit leurs compétences d'utilisation au moyen des notions de « diffusion de signalements » et d'« obtention de données ». En outre, il charge également le Conseil fédéral de désigner les autorités qui peuvent introduire directement des données dans le RIPOL, celles qui peuvent les consulter et celles auxquelles des données peuvent être communiquées de cas en cas. Ainsi, le rapport des notions de « diffusion » et d'« obtention » avec la norme de délégation de compétences (« le Conseil fédéral désigne... », article 351bis, 4^{e} alinéa CP) ainsi que la notion de « consultation » (*direkt abfragen* dans la version allemande[1]) utilisée dans ce cadre-là n'apparaît plus de manière tout à fait claire. Les catégories d'utilisateurs du RIPOL définis aux 2^{e} et 3^{e} alinéas de l'article 351bis CP sont-elles exhaustives ou le Conseil fédéral dispose-t-il de compétences plus étendues lui permettant encore de désigner d'autres autorités pouvant accéder au RIPOL ? De plus, étant donné les possibilités techniques actuelles en matière de communication, les notions auxquelles le législateur a recouru ne sont pas en mesure de clarifier la situation. Enfin, la clause générale de l'article 351bis, 3^{e} alinéa, lettre h CP « autres autorités judiciaires et administratives » laisse une très grande marge de manœuvre en matière de liaison en ligne.

Pour sa part, le Conseil fédéral a transmis la responsabilité du RIPOL à l'OFP (article 4 ordonnance RIPOL). L'OFP a le devoir, la compétence et la responsabilité de délivrer aux utilisateurs (c'est-à-dire aux autorités concernées au sens de l'article 3 ordonnance RIPOL) les autorisations nécessaires à l'emploi du système, de veiller à ce que l'ordonnance soit respectée et d'édicter les instructions qui en découlent (article 4 ordonnance RIPOL). A l'article 6 de l'ordonnance RIPOL, le Conseil fédéral donne des précisions au sujet de l'accès aux données. L'utilisateur n'a accès qu'aux banques de données dont il a besoin pour accomplir ses tâches légales (article 3, 3^{e} alinéa ordonnance RIPOL). Le droit de traiter des données enregistrées dans le RIPOL est réglé dans une annexe.

1 *Note du traducteur*

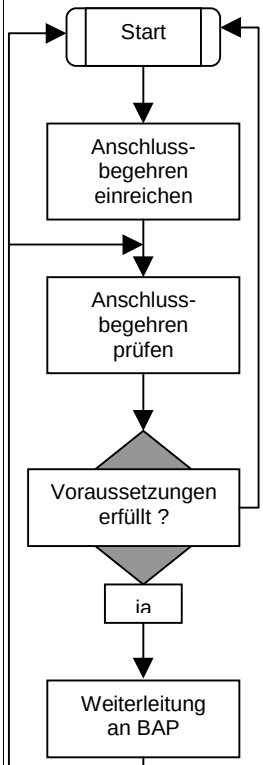
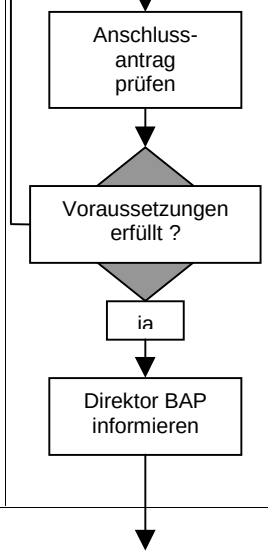
Cascade de délégation en matière d'autorisation d'accès en ligne



A l'occasion de la séance d'automne 1994 de la Conférence des commandants des polices cantonales de Suisse, la procédure de demande d'accès des polices communales a été définie en accord avec l'OFP (annexe 2 des documents que l'OFP a remis ultérieurement à l'expert). Les étapes résumées dans un courrier sont présentées ci-dessous sous forme d'un tableau synoptique. Les étapes qui y sont présentées s'appliquent à toutes les demandes d'accès, à l'exception des demandes d'accès des représentations suisses à l'étranger et des services d'Interpol. Cette présentation correspond aux exigences qu'un système de gestion de la qualité selon la norme internationale ISO 9000 doit respecter et, d'une manière générale, conviendrait à toutes les procédures importantes de l'administration fédérale. Elle part du principe qu'une affaire au sens large du terme est considérée comme étant un intrant (input) qui est traité, étape par étape, par les collaborateurs compétents (responsabilité) selon des listes d'opérations (check-lists) et en fonction d'instructions de travail (procédure ; description et moyens annexes). Le résultat (extrant ou output) doit correspondre aux standards de qualité (mesure de la performance) définis par l'autorité compétente ou par le législateur.

Il est possible de présenter la procédure d'autorisation d'accès en ligne dans le domaine du RIPOL de manière synoptique :

Bundesamt für Polizeiwesen	Bewilligungsverfahren für Online-Anbindung RIPOL	Prozess 0xx

Input	Ablauf	Beschreibung und Hilfsmittel	Verant-wortung	Output
Interne Anfrage, interne Bedarfsab-klärung, interner Rationalisie-rungsantrag etc.		Jede Polizeibehörde (nicht der Kantonspolizei unterstellte Gemeinde- bzw. Stadtpolizeien), die Anschluss an RIPOL wünscht, stellt ein schriftliches Gesuch mit kurzer Begründung an die zuständige Kantonspolizei (Beilage 4a der Nachlieferung von Unterlagen durch das BAP zuhanden des Experten). Diese prüft, ob die rechtlichen kantonalen Voraussetzungen für einen Online-Anschluss gegeben sind. Sie fällt eine Entscheidung und leitet das Gesuch an das Bundesamt für Polizeiwesen (BAP) weiter **Formular 4.5**	Gemeinde-polizei Kantonspolizei Kantonspolizei Kantonspolizei	Anschluss-begehren Gesuchsprüfung Antrag Kantonspolizei
Antrag Kantonspolizei		Das BAP prüft, ob die rechtlichen Voraussetzungen gegeben sind. Diese Prüfung erfolgt durch den Chef der Abteilung Besondere Dienste (BESODI) zusammen mit dem Datenschutz-beauftragten des Amtes in rechtlicher, qualitativer und quantitativer Hinsicht sowie seitens des RZ EJPD betreffend technischer Sicherheit. Bei einem negativen Entscheid antwortet das BAP (konkrete *?* der Chef BESODI) direkt dem Gesuchsteller (mit Kopie zur Kenntnis an die zuständige Kantonspolizei). **Formular 4.1** Der Direktor BAP wird über den Bewilligungsentscheid in Kenntnis gesetzt **Formular 4.2**	BAP Chef BESODI DSB des BAP Chef BESODI Chef BESODI	Bewilligungs-entscheid für Online-Anschluss Negativent-scheid an den Gesuchsteller Kopie an KAPO Mitteilung an Direktor BAP

	Zustellung Bewilligungs-entscheid	Bei einem positiven Entscheid schickt das BAP das Begehren an die zuständige Kantonspolizei und bedient das RZ EJPD mit einer Entscheidskopie **Formular 4.3 und Formular 4.4**	Chef BESODI	Bewilligungs-entscheid Entscheidkopie an RZ EJPD
Anschluss-gesuch an RZ EJPD Technische und örtliche Kommunika-tionsinfrastruk-turen der neuen Benutzer	Technisches Anschlussgesuch stellen	Das kantonale Polizeikommando stellt ein Anschlussgesuch beim RZ EJPD **Formular 3**	Polizei-kommando	
	Technische Betriebsbereitschaft erstellen	Das RZ EJPD sorgt im direkten Kontakt mit den zuständigen kantonalen Stellen (Polizei, Informatik) für die technische Betriebsbereitschaft (Netzwerk, Knoten, Anschlüsse etc.). **Standards, Normen & Richtlinien RZ EJPD**	RZ EJPD Bereich Telematik, Planung & Engineering	Technischer Anschluss gemäss Standards
	Technische Betriebsbereitschaft melden	Das RZ EJPD meldet dem BAP die technische Betriebsbereitschaft des Anschlusses.	RZ EJPD	Meldung Betriebs-bereitschaft an BAP
Zugriffs-parameter	Benutzeranforde-rungen festlegen	Das BAP regelt die Anschlussmodalitäten. Die notwendigen Benutzerprofile und Zugriffsanforderungen werden direkt mit der zuständigen kantonalen oder kommunalen Stelle vereinbart.	Chef BESODI	Benutzerprofile Zugriffsanforde-rungen
	Benutzerverant-wortlichen bestimmen lassen	Grössere Verwaltungseinheiten (z.B: Kantonspolizeikorps) geben ihre Profile selber ein. In diesem Falle verlangt das BAP, dass von der nachsuchenden Verwaltungseinheit gegenüber dem verantwortlichen Kommandanten ein zuständiger Benutzerverantwortlicher bezeichnet wird.	Benutzer-verantwortlicher	
	Benutzerparametri-sierung eingeben	Die neue «REGI-Kennung» muss mit dem RZ EJPD konkret abgestimmt werden. Anschliessend sind die Benutzerparametrisierungen im System einzugeben. **CL00001**	Chef BESODI oder Benutzerverant wortlicher	Benutzerpara-metrisierung
	Zur produktiven Nutzung freigeben	RIPOL wird dem neuen Benutzer zur produktiven Nutzung zur Verfügung gestellt	Chef BESODI oder Benutzerver-antwortlicher	
	Ende			
Version 1.0	**Was** Prozessestellung	**Wann erstellt** **Von wem** 6.3.1998 FI	**Geprüft** 20.4.1998 Bo	**Freigabe** 30.4.1998 Wi

Tableau : Description possible de la procédure sur la base des opérations connues effectuées en vue d'une mise en place d'un accès en ligne au RIPOL.

CL 00001 Mise en place des paramètres des utilisateurs

« L'OFP peut ensuite ''saisir'' le nouvel administrateur xx. Il s'agit ici d'attribuer à l'actuel administrateur de la police cantonale yy un nouveau numéro d'utilisateur en tant qu'administrateur zz. Pour ce faire, il faut changer la *REGI-Kennung* dans le masque 1111 et enregistrer avec F2, muter le profil 802 dans le masque 2211 et enfin attribuer les masques 1111, 1112, 1113, 1121, 2211 et 2212 dans le ''*Sportoto*'' 9000. »

etc.

314 Exploitation et maintenance

Le RIPOL est opérationnel depuis 1984. Au cours des quatorze dernières années, diverses unités administratives, internes et externes à l'administration fédérale, y ont été successivement raccordées (voir liste chronologique de l'annexe 1). Les exigences envers le RIPOL ont régulièrement augmenté à la demande des utilisateurs. Un règlement d'utilisation et de maintenance du projet RIPOL, édicté par l'OFP en mai 1987, définit les modalités de développement et la maintenance du système. La section chargée du système de recherches informatisées de l'OFP est responsable des développements et de l'exploitation du RIPOL. Un groupe de projet est chargé d'examiner les propositions en matière de développement ou d'extension du projet. La direction du projet incombe au chef de l'Office fédéral de la police. La prise en compte des exigences cantonales et communales par l'OFP est assurée par le groupe de travail « informatique » de la commission technique des polices suisses ainsi que par le groupe de travail des utilisateurs concernés. Les principes de ce règlement ont fait leurs preuves.

Des tentatives d'autonomisation tant au niveau de la Confédération que dans les cantons font apparaître des applications parallèles. En particulier les cantons ont une tendance à mettre en place des systèmes unifiés et intégrés au niveau intercantonal sans se sentir concernés par les standards de la Confédération en matière de protection des données. Le manque de stratégie, le formalisme juridique, les attentes des organes de recherche et les exigences en matière de protection des données rendent toute coordination difficile (voire point 324 ci-dessous). L'exploitation du système ABI développé par le secteur privé et proposé aux cantons par d'anciens collaborateurs du CC DFJP (!) interprète de toute évidence la législation sur la protection des données de manière plutôt approximative et pourrait bientôt concurrencer les solutions de la Confédération, en particulier dans les domaines des systèmes RIPOL et DOSIS. Le système ABI dont la mise en oeuvre dans les domaines de la lutte contre le crime organisé et contre le trafic illicite de stupéfiants est déjà planifié, jouit d'une popularité grandissante au sein des corps de police cantonaux. Il sera bientôt exploité par dix-neuf cantons [voir « Echange de données en ligne entre Confédération et cantons », Rapport du Service de contrôle administratif du Conseil fédéral du 22 décembre 1997, version complétée du 9 février 1998 (cité **Rapport CCF** par la suite), pages 26 et 26 ; lettre de l'OFP du 5 décembre 1997 adressée à l'OPCA, page 7].

315 Participation aux coûts

En vertu de l'article 22 de l'ordonnance RIPOL, l'infrastructure de communication (mise à disposition du réseau) est financée par la Confédération. Elle prend en charge le raccordement et le fonctionnement des circuits de transmission des données jusqu'à un dispositif central de commutation (distributeur principal, nœud central) sis au chef-lieu du canton. La Confédération prend également en charge l'ensemble des coûts du projet, des extensions et développements (développement du logiciel) ainsi que les coûts générés par le centre de calcul (exploitation du système). La Confédération ne facture pas ses prestations en matière d'informatique et de télécommunication. Dans les circonstances actuelles, une

telle facturation aurait certainement des effets négatifs sur l'acceptabilité et la mise en œuvre des systèmes d'information unifiés dans le domaine de la police (Rapport CCF, pages 32 et 33).

Les cantons assument les frais d'installation et d'exploitation du réseau de redistribution sur leur territoire ainsi que les frais d'acquisition et d'exploitation pour les postes de travail raccordés.

316 Cantons et autres accès externes à l'administration fédérale

Du point de vue de son utilisation aux niveaux cantonal et communal, le RIPOL est une grande application largement utilisée. La liste chronologique révèle que 12'628 utilisateurs (soit 95.4 pour cent) sont des utilisateurs aux niveaux cantonal et communal, donc externes à l'administration fédérale. Parmi les 606 utilisateurs internes à l'administration fédérale (soit 4,6 pour cent seulement), on trouve également 24 représentations suisses à l'étranger et 30 services d'Interpol.

Utilisateurs du RIPOL			
EXTERNES à l'administration fédérale	**95.4%**	**=**	**12'628 utilisateurs**
INTERNES à l'administration fédérale	**4.6%**	**=**	**606 utilisateurs**

Selon les explications données par le chef de la division des Services spéciaux lors de l'audition du 2 février 1998, les représentations suisses à l'étranger (consulats) sont également raccordées au RIPOL. La légitimation de ces liaisons ressort de l'article 3, 3^{e} alinéa, lettre b de l'ordonnance RIPOL selon lequel les représentations suisses à l'étranger assumant des tâches consulaires peuvent consulter directement (en ligne) des données concernant les signalements de personnes ainsi que les infractions non élucidées, y compris la recherche d'objets. Ces liaisons ont été rendues possibles avec la révision de l'ordonnance de l'automne 1995. La transmission de données aux représentations suisses à l'étranger assumant des tâches consulaires ainsi qu'aux services étrangers d'Interpol intervient en la forme chiffrée (article 17, 1er alinéa ordonnance RIPOL). La procédure de raccordement a été conduite à un niveau informel, c'est-à-dire que le Secrétariat général du DFJP aurait pris les dispositions correspondantes avec le Secrétariat du DFAE. Ce n'est qu'après cet aboutissement que la mise en œuvre de ces dispositions a été confiée aux directions administratives compétentes. En ce qui concerne l'OFP, c'est à nouveau le chef de la division des Services spéciaux qui est compétent pour les autorisations en matière de raccordement.

317 Perspectives de développement

La loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC, RS 172.213.71) est entrée en vigueur le 15 mars 1995. Elle constitue la base légale permettant à la Confédération de soutenir les cantons et les forces de police étrangères dans la lutte contre le crime international organisé. Cette loi reconnaît à la Confédération un rôle central en matière de détection et de lutte contre le crime organisé. La loi sur les Offices centraux de police criminelle règle également les échanges d'informations internationaux et intercantonaux. En se basant sur les articles 11, 1er alinéa, 12, 2^{e} alinéa, 13, 1er alinéa et 15 de la loi sur les Offices centraux de police criminelle, ces derniers ont, en vue d'accomplir les tâches qui leur sont confiées, le droit de gérer et d'exploiter un système de traitement des données pour lutter contre le crime organisé (ISOK). En tant que système de recherche informatisé de personnes et d'objets, le RIPOL n'est pas concerné par ces développements. Pour cette raison, le RIPOL n'est touché ni par l'élaboration des nouvelles ordonnances sur les Offices centraux de police criminelle et sur le système de traitement de données en

matière de lutte contre le crime organisée (ordonnance ISOK), ni par la révision de l'ordonnance sur le système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants (ordonnance DOSIS).

Sur la base des explications orales fournies à l'occasion de l'audition des représentants de l'OFP du 2 février 1998, les développements suivants ont été planifiés en matière de liaisons en ligne au RIPOL :

a) développement des liaisons avec les offices cantonaux de la circulation routière pour la consultation en matière de recherche de véhicules,
b) liaisons avec d'autres représentations suisses à l'étranger (Los Angeles, Londres, Lagos) pour leurs tâches consulaires (voir procès-verbal du Comité de projet RIPOL du 9.7.1997, chiffre 3, page 2 ; *Ausschreibung von Personen, ungeklärte Straftaten, Sachfahndung*),
c) développement des liaisons avec les services étrangers d'Interpol en ce qui concerne la recherche de véhicules et d'objets,
d) développement des liaisons pour la « plate-forme » cantonale *Ostschweiz* (concordat relatif à la collaboration intercantonale en matière de tâches de police criminelle),
e) développement des liaisons des polices communales.

32 DOSIS

321 Bases et principes légaux

Les bases légales suivantes sont déterminantes dans le domaine du système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants (DOSIS) :

1. Loi fédérale sur les stupéfiants et les psychotropes (Loi sur les stupéfiants, LStup, RS 812.121, en particulier l'article 30 LStup),
2. Loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC, RS 172.213.71, en particulier les articles 11, 1er alinéa, 12, 2e alinéa, 13, 1er alinéa et 15 LOC),
3. Ordonnance sur le système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants (Ordonnance DOSIS, RS 812.121.7) avec le catalogue de données (annexe 1 à l'ordonnance DOSIS),
4. Ordonnance sur les Offices centraux de police criminelle près l'Office fédéral de la police (OOC, RS 172.213.711),
5. Directives du Département fédéral de justice et police sur le système provisoire de traitement des données en matière de lutte contre le trafic illicite de stupéfiants (Directives-Dosis-Département ; abrogées avec la mise en exploitation définitive de l'intégralité de l'application DOSIS et remplacées par le règlement de traitement DOSIS),
6. Directives sur le contrôle du système provisoire de traitement des données en matière de lutte contre le trafic illicite des stupéfiants (Directives-DOSIS-Contrôle ; abrogées avec la mise en exploitation définitive de l'intégralité de l'application DOSIS et remplacées par le règlement de traitement DOSIS),
7. DOSIS - règlement de traitement de l'OFP du 20 décembre 1996, remplacé le 1er avril 1998 par celui du 20 mars 1998.

Ces bases légales permettent de déduire les principes relatifs à l'autorisation, par les autorités fédérales compétentes, d'accès en ligne dans le domaine de la police suivants :

Au niveau de la loi

Dans le cadre de l'Office fédéral de la police (OFP), la Confédération gère un office central chargé de réprimer le trafic illicite des stupéfiants en vertu de l'article 9 LOC et de l'article 29 LStup. Cet office central soutient les autorités de la Confédération, des cantons et des autres Etats dans la prévention et la lutte contre le trafic illicite des stupéfiants (article 9, 1er alinéa

LOC). Les alinéas 1 à 3 de l'article 11 LOC contiennent les principes essentiels du système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants DOSIS. Le législateur donne au Conseil fédéral la compétence générale de confier la gestion d'un système de traitement des données à un office central. A l'aide de ce système, des données sensibles et des profils de la personnalité peuvent être exploités, à condition et aussi longtemps qu'ils s'avèrent nécessaires à l'exécution des tâches incombant à cet office central. De plus, le législateur a décidé qu'un tel système de traitement des données doit être géré séparément des autres systèmes de la police et de l'administration. A l'article 12 LOC, le législateur statue sur la participation des services cantonaux qui, collaborant avec l'office dans le cadre de leurs attributions, sont autorisés à accéder directement, par une procédure d'appel, au système de traitement des données de ce dernier, pour autant que soient prises les mesures de protection et de sécurité nécessaires. Le Conseil fédéral a également reçu la compétence d'autoriser les services cantonaux à introduire eux-mêmes les données. Le Conseil fédéral a, de surcroît, le devoir de régler les modalités de traitement des données par les offices centraux et la coordination des systèmes, le droit d'accès – et ses limites – dont bénéficient les services fédéraux et cantonaux ainsi que la durée de l'archivage des données, le contrôle et les modalités de la protection des données (article 15 LOC).

Au niveau des ordonnances

Avec l'OOC, le Conseil fédéral règle la collaboration avec les offices centraux (article 6 OOC), l'obligation d'informer dans le domaine du trafic illicite de stupéfiants (article 12 OOC), la communication de données à des autorités tenues de fournir des renseignements (article 7 OOC) ainsi que la communication de données à d'autres destinataires (article 8, OOC). Avec l'ordonnance DOSIS, le Conseil fédéral règle en particulier la gestion et l'utilisation par l'Office central de lutte contre le trafic illicite de stupéfiants (office central) près l'Office fédéral de la police du système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants (DOSIS). Ainsi, les principes spécifiques à DOSIS sont réglés dans une ordonnance séparée. En tant que loi spécifique, l'ordonnance DOSIS a la préséance sur l'OOC qui est de portée générale.

DOSIS est donc un système d'information qui ne peut contenir que des données concernant le trafic illicite de stupéfiants. Les tierces personnes ou des indications les concernant ne sont enregistrées que dans la mesure où ces éléments sont nécessaires aux enquêtes (article 3 ordonnance DOSIS). Avec la modification de l'ordonnance DOSIS du 19 novembre 1997, il est dorénavant possible – depuis le 1er janvier 1998 – de gérer les données de base de DOSIS dans un index commun avec les données de bases du système de traitement des données en matière de lutte contre le crime organisé ISOK (article 7, 7e alinéa ordonnance DOSIS). Afin d'éviter les saisies à double de certaines données[1] (désignées de manière particulière dans l'annexe à l'ordonnance DOSIS), il est nouvellement possible de les copier dans l'index central des dossiers ZAN (article 11b, 6e alinéa ordonnance DOSIS). L'OFP règle le détail de cette procédure dans le règlement de traitement. Lors de leur transmission, les données de DOSIS doivent faire l'objet d'un chiffrement de bout en bout (article 6 ordonnance DOSIS).

Les offices suivants peuvent être raccordés à DOSIS au moyen d'une procédure d'appel (article 8, 1er alinéa ordonnance DOSIS) :

- l'office central (c'est-à-dire l'office central de lutte contre le trafic illicite de stupéfiants),
- les brigades des stupéfiants des corps de police des cantons,
- le service de contrôle DOSIS/ISOK,
- le conseiller à la protection des données de l'Office fédéral de la Police,

[1] *En particulier, voir les remarques complémentaires de la prise de position de l'OFP du 22 juillet 1998, page 2, chiffre C/1.*

- le chef de projet et les gestionnaires du système,
- les services de l'Administration fédérale des douanes, uniquement pour le sous-système « Lexique des stupéfiants et modi openrandi » (article 8, 3e alinéa ordonnance DOSIS).

Sur demande, les autorités de poursuite pénale spécialisées des cantons peuvent être raccordées à DOSIS pour des procédures déterminées (article 8, 2e alinéa ordonnance DOSIS). Les utilisateurs ne peuvent toutefois consulter qu'un seul des sept sous-systèmes à la fois [« Personnes et antécédents » (PV), où sont enregistrées des données sur des personnes et leurs antécédents recueillies dans le cadre d'enquêtes relatives à un trafic illicite de stupéfiants ; « Journaux » (JO), où sont enregistrées des données sur toute affaire de trafic illicite de stupéfiants faisant l'objet d'une enquête ; « Contrôle des affaires et des délais » (GT), où est enregistré le suivi des enquêtes en cours menées par l'office central ; « Renseignements généraux » (ER), où sont enregistrées des données utiles à la lutte contre le trafic illicite de stupéfiants ; « Lexique des stupéfiants et modi operandi » (DL) ; « Rapport de situation » (LA), où sont enregistrés des rapports décrivant la situation nationale et internationale en matière de stupéfiants ; « Représentation graphique » (VI), où sont enregistrés des graphiques relatifs aux connexions entre divers réseaux de trafiquants de stupéfiants] (article 8, 5e alinéa ordonnance DOSIS). Si un autre canton est concerné par l'enquête, l'office central ou la brigade des stupéfiants peut étendre l'accès aux données qu'il a saisies à la brigade des stupéfiants du canton concerné (article 9, 3e alinéa ordonnance DOSIS). L'office central et les brigades des stupéfiants des corps de police des cantons saisissent eux-mêmes dans DOSIS les données qu'ils ont recueillies. Ce faisant, ils déterminent les catégories d'antécédents, fixent la durée de conservation et qualifient ces antécédents comme étant fiables ou peu fiables (article 10, 1er alinéa ordonnance DOSIS). Le Service de contrôle de DOSIS/ISOK près l'Office fédéral de la police (service de contrôle) examine si les données saisies sont conformes aux dispositions de la présente ordonnance. Si ce n'est pas le cas, il les corrige ou les efface. En particulier, les données saisies provisoirement font l'objet d'une vérification par le service de contrôle, au besoin en collaboration avec l'organe ayant effectué la saisie. Le service de contrôle confirme l'enregistrement des données ou demande leur correction. L'Office fédéral de la police précise les modalités de cette vérification des données dans le règlement de traitement (article 10, 3e et 4e alinéas ordonnance DOSIS). Les articles 11, 11a et 11b de l'ordonnance DOSIS (en vigueur depuis le 1er janvier 1998) règlent par le détail la communication de données à des autorités tenues de fournir des renseignements (article 11), à d'autres destinataires (article 11a) ainsi que les restrictions de la communication de données (article 11b). En vertu de ces articles, l'office central peut « communiquer » ou « communiquer spontanément » des données personnelles enregistrées dans DOSIS à diverses autorités. La communication, ainsi que le destinataire, l'objet et le motif de la demande de renseignements doivent être enregistrés dans DOSIS (article 11b, 5e alinéa ordonnance DOSIS).

Principes régissant DOSIS

1. **Il doit être géré séparément des autres systèmes d'information**
2. **Il ne peut contenir que des données concernant le trafic illicite de stupéfiants.**
3. **Les données doivent faire l'objet d'un chiffrement de bout en bout de leur transmission.**
4. **Nombre d'utilisateurs limité.**
5. **Il n'est possible de consulter qu'un seul des sept sous-systèmes à la fois.**
6. **Les communications de données doivent être enregistrées dans DOSIS.**

322 Situation actuelle en matière de liaisons en ligne

Nombre d'utilisateurs

Selon la liste chronologique du 26 novembre 1997 des liaisons en ligne avec DOSIS, dont l'actualité a été confirmée lors de l'audition du 2 février 1998,

409 utilisateurs

ont été reliés à DOSIS depuis le 15 janvier 1997 jusqu'à aujourd'hui.

Catégories d'utilisateurs

La légitimité de tous les utilisateurs de DOSIS raccordés au moyen de liaisons en ligne découle de la loi sur les Office centraux de police criminelle de la Confédération et, en particulier, de l'ordonnance DOSIS (article 8 ordonnance DOSIS). Les droits d'accès sont réglés dans la matrice d'accès DOSIS (annexe 2 à l'ordonnance DOSIS).

Réseau et mesures de sécurité

Tous les partenaires raccordés communiquent par le truchement d'infrastructures de la Confédération (LIS/DFJP, WAN-DFJP). La communication est effectuée par TCP/IP (protocoles de communication normalisés). Les mesures de sécurité sont en partie basées sur des logiciels (chiffrages *end-to-end*) et en partie sur une isolation du KOMBV1-LIS au moyen un mur coupe-feu.

323 Procédure de raccordement

Niveau de la loi

Le raccordement en ligne de l'OFP puise ses bases légales dans l'article 11, 1er alinéa LOC. Les services cantonaux qui, dans le cadre de leurs attributions, collaborent avec l'office central sont autorisés à disposer d'un accès en ligne en vertu de l'article 12, 1er alinéa LOC. A l'article 15 LOC, le législateur a délégué au Conseil fédéral les compétences en matière d'organisation de la procédure de raccordement.

Niveau des ordonnances

L'ordonnance sur les Offices centraux de police criminelle près l'Office fédéral de la police ne comprend pas de dispositions de détail au sujet des liaisons en ligne. Elle ne réglemente donc ni les tâches, ni les compétences, ni les responsabilités à ce sujet. Pour l'essentiel, cette ordonnance définit à quelles autorités les offices centraux sont habilités à fournir des données personnelles (articles 6, 7 et 8 OOC). Dans l'ordonnance DOSIS, le Conseil fédéral règle également les principes de l'accès direct aux données de manière accessoire en définissant à l'article 8, 1er alinéa de l'ordonnance DOSIS les services qui y ont accès par liaison en ligne (voir les remarques complémentaires de la prise de position de l'OFP du 22 juillet 1998, page 2, chiffre C/2). Sur demande, des autorités cantonales de poursuite pénale spéciales peuvent également se raccorder à DOSIS pour certaines procédures concrètes (article 8, 2e alinéa ordonnance DOSIS). Les droits d'accès sont réglés dans la matrice d'accès DOSIS (annexe 2 à l'ordonnance DOSIS). Cependant, en ce qui concerne la procédure de raccordement en ligne en tant que telle, l'ordonnance DOSIS ne contient aucune indication. En effet, elle ne dit rien au sujet de l'attribution ou de la délégation de compétences en matière d'octroi d'autorisations au DFJP ou à l'OFP, voire au sujet des tâches, des compétences et des responsabilités qui y sont liées.

Niveau de la mise en œuvre

Seules les dispositions du 3e alinéa de l'article 4 des directives sur le système provisoire de traitement des données en matière de lutte contre le trafic illicite de stupéfiants de 1994 (Directives-DOSIS-Département, qui ne sont plus en vigueur) précisent que les demandes d'autorisation d'accès doivent être agréées par le chef de l'office central ou par son

suppléant. La réalisation de l'accès au système DOSIS est effectuée par le Centre de calcul et par l'administrateur DOSIS. Avec la mise en service de l'exploitation définitive de l'intégralité de l'application DOSIS, ces directives provisoires ont été remplacées par le règlement de traitement DOSIS du 20 décembre 1996. Un nouveau règlement de traitement DOSIS du 20 mars 1998, qui tient compte de diverses modifications de l'organisation structurelle et de l'organisation procédurale, est entré en vigueur le 1er avril 1998. Le règlement de traitement de l'OFP du 20 décembre 1996 traite de la procédure d'accès et des questions qui y sont liées de manière détaillée. A l'article 10, 2e alinéa de la section 2 (utilisateurs et accès), il est pour la première fois expressément défini que les demandes d'autorisation des commandements (des polices cantonales) doivent être agréées par le responsable DOSIS des offices centraux (sur délégation de la Direction de l'OFP). Actuellement, cette fonction est assumée par le chef de l'Office central du crime organisé (voir article 1er, lettre f du règlement de traitement du 20 mars 1998). Les demandes d'accès sont transmises à l'administrateur DOSIS. Ce dernier les gère et en coordonne la réalisation. Il transmet au centre de calcul les demandes concernant la mise en place d'accès au système principal dudit centre et la fourniture des logiciels TAXI et DOSIS-Mail. Il introduit lui-même les paramètres de l'accès de chaque utilisateur du système (article 10, 3e alinéa règlement de traitement). Les autorisations individuelles d'accès nécessaires au personnel du centre de calcul qui travaillent sur le système DOSIS sont attribuées directement par le centre de calcul (article 10, 4e alinéa règlement de traitement).

324 Exploitation et maintenance

L'OFP a été raccordé à DOSIS en janvier 1993 (voir annexe 2). Actuellement, 58 utilisateurs de l'OFP sont enregistrés dans le système et son autorisés à l'utiliser. Les corps de police des cantons sont venus s'y raccorder successivement depuis septembre 1994. En 1984 : LU (1.9.1994), SG (1.10.1994), TG (1.10.1994) et AG (1.11.1994) ; en 1995 : GE (1.3.1995), BE (1.4.1995), VD (1.4.1995) et TI (1.7.1995) ; en 1996 : aucun raccordement ; en 1997 : BS (23.4.1997), GR (23.4.1997), BL (6.5.1997), ZH (30.5.1997), OW, SO, UR, VS, ZG, police municipale de Zurich (tous le 10.9.1997), FR et NE (les deux le 1.10.1997), SZ (13.10.1997), GL (27.10.1997), JU (29.10.1997), SH (5.11.1997), AI et AR (les deux le 11.12.1997) ; en 1998 : NW (19.1.1998).

Les tâches et les responsabilités en matière d'exploitation courante et de maintenance sont réglées dans l'ordonnance DOSIS, dans les Directives-DOSIS-Contrôle (édictées par l'Office central stupéfiants près l'OFP) ainsi que dans le règlement de traitement de l'OFP (édicté par l'OFP). Il est possible de renvoyer le lecteur à ces textes de base dans la mesure où, en ce qui concerne la question principale du présent rapport, il n'est pas indispensable de procéder à une présentation systématique des points qui y sont réglés.

Comme cela ressort du Rapport CCF, il est notoire que des applications parallèles dans l'administration fédérale et les cantons sont développées dans certains secteurs de la police. La banque de données DOSIS est, de l'avis de plusieurs cantons, peu compatible avec une activité policière efficace. Cela provient notamment du fait que sa coordination avec ISOK n'est devenue légalement possible qu'à partir de 1998 (révision partie C dans le paquet « registres des personnes ») et qu'elle est soumise à des règles rigoureuses quant à la protection des données. Les raisons principales qui empêchent DOSIS d'être un instrument fonctionnel de recherche répondant aux attentes des corps de police sont les suivantes : limitation à un seul secteur de la criminalité (trafic de drogues), durée relativement brève des entrées (2 ans), difficultés d'utilisation des dossiers de l'enquête préliminaire (contrairement à ceux de l'instruction judiciaire). Un système élaboré par le secteur privé pour les cantons (le système ABI qui est proposé par d'anciens collaborateurs du Centre de calcul du DFJP), caractérisé par une observation beaucoup moins rigoureuse de la législation sur la protection des données, pourrait prochainement concurrencer (ABI est sur le point d'être utilisé dans 19 cantons) le système de la Confédération (Rapport CCF, page 26, chiffre 32).

325 Participation aux coûts

L'ordonnance DOSIS règle le financement du système d'information DOSIS (article 20 ordonnance DOSIS) de manière analogue à la réglementation concernant le RIPOL (article 22 ordonnance RIPOL). La Confédération finance la transmission des données jusqu'au distributeur principal (calculateurs nodal, de commutation) sis dans les cantons. Les cantons assument les frais d'acquisition et d'exploitation de leurs appareils ainsi que les frais d'installation et d'exploitation de leur réseau de redistribution. Les autres dépenses, notamment les prestations de la Confédération dans le domaine de l'informatique et des télécommunications, ne sont pas facturées. En matière d'acceptabilité et de mise en œuvre il convient, dans ce domaine, de faire la même remarque que celle déjà faite sous le point 315 (voir également Rapport CCF, pages 32 et 33).

326 Cantons et autres accès externes à l'administration fédérale

Les 409 utilisateurs de DOSIS sont répartis de la manière suivante : 351 utilisateurs (85.8 pour cent) sont des corps de police des cantons et 58 utilisateurs sont des collaborateurs de l'OFP (14.2 pour cent).

Utilisateurs de DOSIS			
EXTERNES à l'administration fédérale	**85.8%**	**=**	**351 utilisateurs**
INTERNES à l'administration fédérale	**14.2%**	**=**	**58 utilisateurs**

Nidwald et les deux demi-cantons d'Appenzell sont raccordés au système. Toutefois, il est prévu que ces liaisons ne deviennent opérationnelles qu'une fois la phase de formation des collaborateurs achevée (article 12 règlement de traitement de l'OFP). Ceci devrait être le cas entre-temps, si bien qu'actuellement, DOSIS compte de 3 à 5 utilisateurs supplémentaires.

327 Perspectives de développement

Selon la lettre de l'OFP du 5 décembre 1997 adressée à l'Organe parlementaire de contrôle de l'administration, tous les services cantonaux de lutte contre le trafic illicite de stupéfiants disposent d'accès en ligne au système DOSIS (page 5 de cette lettre). Avec effet au 1er janvier 1998, le Conseil fédéral a également mis en vigueur les modifications de l'ordonnance DOSIS du 19 novembre 1997. La base légale au sens formel se trouve à l'article 11, 1er alinéa LOC. Toutefois, selon la disposition du 3e alinéa de ce même article, l'exploitation de DOSIS doit demeurer séparée de celle d'ISOK et de l'index central des dossiers (ZAN). L'OFP relève que cette situation provoque des problèmes en matière de lutte contre le crime organisés qui sont difficiles à résoudre car les différents genres de délits ne peuvent pas être traités dans la même banque de données. Etant donné cette situation, le Conseil fédéral a, dans son message concernant la création et l'adaptation de bases légales applicables aux registres des personnes (modification du CP, de la LCR et de la LOC), proposé la révision de l'article 11, 1er alinéa LOC. Cette révision a pour objet de permettre aux Offices centraux de police criminelle rattachés à l'OFP d'exploiter une banque de données unifiée correspondant à leur nouvelle structure organisationnelle et à leurs méthodes de travail. Ce projet comporte quatre parties qui concernent toutes des banques de données personnelles informatisées :

- Partie A : gestion des dossiers personnels de l'OFP.
- Partie B : informatisation du casier judiciaire.
- Partie C : traitement des données personnelles par les offices centraux de police criminelle.

- Partie D : registre des véhicules et détenteurs de véhicules et registre des mesures administratives frappant les conducteurs de véhicules.

Le projet a pour but de permettre de créer ou de réviser les bases légales au sens formel dans les délais (voir article 38, 3e alinéa LPD). En effet, une exploitation rationnelle de ces banques de données personnelles tenant compte de l'évolution technologique est nécessaire pour ces quatre parties.

Le système DOSIS est plus particulièrement concerné par la partie C. Cette partie prévoit la transformation des offices centraux de l'OFP en un centre national et international d'information, d'analyse, de coordination et d'investigation. Les fonctions actuelles de ces offices centraux seront regroupées au sein d'une structure organisationnelle unique qui sera composée d'une unité criminalistique, d'une unité opérationnelle et d'une unité logistique (message, pages 6 et 7, chiffre 114.2). Proposée dans la partie C, la modification de l'article 11, 1er alinéa LOC a pour objet de donner aux collaborateurs des Offices centraux de police criminelle rattachés à l'OFP l'accès aux systèmes DOSIS et ISOK. Cette solution est une solution intermédiaire en attendant que soit développé et mis en service le produit informatique qui succédera aux systèmes DOSIS et ISOK (message, page 8, chiffre 114.5). Là aussi, il s'agira de séparer rigoureusement l'exploitation du nouveau système informatisé commun des Offices centraux de police criminelle rattachés à l'OFP de l'exploitation des autres banques de données de la police et de l'administration (message, page 19, chiffre 23).

Au 31 décembre 1997, pratiquement tous les services cantonaux de lutte contre le trafic illicite de stupéfiants étaient raccordés au système DOSIS si bien que la question des demandes d'accès ne devrait plus revêtir une grande importance. Toutefois, le message du Conseil fédéral (paquet « registres des personnes ») indique que l'instauration d'un système commun d'information dans le domaine de la poursuite pénale est également prévue dans la Convention sur la mise en place d'un Office européen de police (Convention Europol du 27 novembre 1995, JO no C 316, page 1). Le Conseil européen a approuvé la convention sur la base de l'article K.3 du Traité de l'Union européenne du 26 juillet 1995 et a recommandé aux Etats membres de la ratifier. La création d'une base légale formelle à l'appui du futur système commun d'information s'avère donc judicieux, également dans l'optique de la coopération avec les forces de police étrangères. Il est donc possible de conclure que le produit informatique unifié qui succédera aux systèmes DOSIS et ISOK pourra être mis en communication avec des autorités étrangères si le législateur élabore les bases légales formelles nécessaires. Du point de vue de l'évolution des raccordements en ligne et de la pratique en la matière, ce fait donne une importance croissante à la réglementation de la procédure permettant à l'autorité compétente de délivrer de telles autorisations de raccordement.

328 Résumé et appréciation du RIPOL et de DOSIS

1. La délégation continue des tâches, des compétences et des responsabilités, jusqu'à la l'unité administrative hiérarchiquement la plus basse, constitue la caractéristique principale qui marque la question de l'octroi des autorisations d'accès aux systèmes d'information RIPOL et DOSIS.

   Alors que les droits d'accès et de mutation sont réglés individuellement jusqu'au niveau de chaque champ (annexe à l'ordonnance RIPOL) et que le règlement d'utilisation et de maintenance de l'OFP de mai 1987 présente de manière détaillée les modalités en matière de développement et de maintenance dans le cadre du projet RIPOL, les dispositions de détail concernant la procédure d'autorisation (description des processus), les listes d'opérations (check-lists) ou les directives de travail correspondantes font défaut. Seul le chiffre 713 du règlement d'utilisation et de maintenance de l'OFP de mai 1987 fixe que l'OFP décide des raccordements des

utilisateurs fédéraux du projet. En revanche, le règlement est muet en ce qui concerne les demandes de raccordement des utilisateurs cantonaux et communaux, bien que ces derniers soient beaucoup plus nombreux. De plus, la procédure d'autorisation en tant que telle, les principes régissant les raccordements, la documentation et le classement des décisions de raccordement ne sont pas réglés non plus.

DOSIS permet également d'enregistrer des données personnelles et des profils de la personnalité digne de protection. C'est d'ailleurs ce qui a motivé le législateur à exiger expressément que ce système soit géré séparément des autres systèmes de la police et de l'administration. Le législateur est donc très exigent en ce qui concerne le traitement et l'utilisation de ces données sensibles. Le Conseil fédéral n'a pas tenu compte de ces exigences élevées en matière de raccordements. Bien que l'article 15 de la LOC l'exige de lui, le Conseil fédéral n'a édicté aucune réglementation explicite en ce qui concerne les tâches, les compétences, les responsabilités et les principes à observer pour l'octroi d'autorisations d'accès, ni dans l'OOC, ni dans l'ordonnance DOSIS. Ce n'est qu'au niveau de l'administration (Directives-DOSIS-Département et règlement de traitement de l'OFP) que les principes correspondants ont été définis. A ce niveau, on trouve une délégation de compétences supplémentaire en faveur de la dernière unité hiérarchique. En effet, la compétence décisionnelle du directeur de l'OFP est déléguée au responsable de chaque système concerné. Au vu des perspectives de développement et d'extension, notamment la possibilité d'accès par des forces de police étrangères (Convention Europol), il est impératif d'élaborer une réglementation claire de la procédure de raccordement, des tâches, des compétences, des responsabilités ainsi que des principes que l'autorité compétente en matière d'autorisation doit expressément respecter.

2. En ce qui concerne les autorisations d'accès, les principes mis en place dans les dispositions de droit supérieur (lois, ordonnances) menacent de se perdre au fur et à mesure de la délégation des responsabilités vers le bas. En effet, une telle délégation en faveur d'une unité opérationnelle peut conduire à des interprétations et des défenses d'intérêts différentes de celles qui avaient motivé le législateur à l'origine. La délégation continue des tâches, compétences et responsabilités ainsi que l'inscription de cas en cas de ces principes originels dans diverses décisions (octrois d'autorisation d'accès) au plus bas niveau hiérarchique font que ces principes finissent par ne plus être observés.

3. La volonté politique du législateur de déléguer les compétences en matière d'autorisations d'accès (cadre général) devient de plus en plus imprécise et de moins en moins claire au fur et à mesure des étapes de délégation vers le bas puisque le cadre et les facteurs d'influence des prochains niveaux de délégation viennent s'y superposer.

4. Une délégation vers le bas des compétences en matière d'autorisation d'accès en ligne va dans le sens diamétralement opposé au degré de sensibilité des données dans le domaine de la police. Plus la sensibilité des données à traiter est élevée (niveau de protection des données ; données particulièrement dignes de protection ; profils de la personnalité), moins il serait souhaitable de déléguer vers le bas la compétence en matière d'autorisation d'accès en ligne.

5. Plus la compétence en matière d'autorisation d'accès en ligne est déléguée vers le bas, plus le risque de conflits d'intérêts pour l'autorité compétente en matière d'autorisation augmente. En raison de ses intérêts – légitimes – plaidant en faveur d'une large utilisation de son système d'information (voir les remarques complémentaires de la prise de position de l'OFP du 22 juillet 1998, pages 3 et 4, chiffre 4), elle s'expose bien plus vite au reproche de succomber à la tentation d'évaluer de manière exagérément positive les motifs présentés par le demandeur de l'autorisation d'accès.

6. Au niveau du dernier échelon opérationnel d'une unité administrative il y a un contact direct (groupes de travail, commissions intercantonales, engagements communs etc.) entre les demandeurs et l'autorité compétente en matière d'autorisation (autorité concédante). Ce fait n'est pas propice à promouvoir l'indépendance de cette autorité. En effet, dans le cadre de l'examen des délicates conditions d'autorisation qui ne permettent un accès direct aux données que pour l'accomplissement des tâches légales (article 3, 3e alinéa ordonnance RIPOL), il n'est pas possible d'attendre d'une telle autorité concédante qu'elle fasse preuve du sens critique nécessaire en matière de nécessité, de proportionnalité et d'opportunité vis-à-vis d'une unité de même niveau hiérarchique et accomplissant des tâches semblables (voir les remarques complémentaires de la prise de position de l'OFP du 22 juillet 1998, pages 3 et 4, chiffre 4). Dans ce domaine très sensible que sont les banques de données des organes de police, la garantie de l'indépendance de l'autorité en matière d'autorisation d'accès en ligne revêt une importance toute particulière.

7. Il arrive parfois que des projets pilotes démarrent sans bases légales formelles en matière de réalisation et de mise en place de systèmes d'information gérant des données sensibles (par exemple : VOSTRA, EVA ou dans le domaine du blanchiment de l'argent sale). De tels systèmes se développent avec le raccordement successif de nouveaux utilisateurs et l'extension de ses fonctions. Dans ces conditions, il est souvent difficile d'identifier et de délimiter l'étape finale qui sépare le projet pilote de la mise en œuvre définitive du système d'information.

8. Le fait qu'avec le RIPOL et DOSIS, la Confédération met ses propres systèmes d'information à disposition mais que les tâches de police sont en grande partie assumées par les cantons présente des difficultés supplémentaires. A moins qu'une compétence légale n'ait été expressément créée, cette organisation de la surveillance à moitié centralisée et à moitié fédéraliste (Georg Kreis, Staatsschutz in der Schweiz, Verlag Paul Haupt Bern, 1993, p. 206) rend toute intervention directe des autorités fédérales compétentes en matière d'autorisation difficile pour toute question relative aux structures et aux procédures cantonales. Les transferts en ligne de données ont des effets directs sur l'organisation procédurale des services cantonaux. Les données techniques et celles relatives aux applications influencent les structures administratives et ont des répercussions qui peuvent être importantes au niveau de l'autonomie cantonale en matière d'organisation (voir Rapport CCF, page 38). Pour cette raison, les possibilité d'évaluation et d'influence de l'autorité fédérale concédante sont limitées, en particulier dans le cadre de l'examen de la question de la nécessité, de la proportionnalité et de l'opportunité d'un raccordement en ligne d'un service cantonal ou communal. Il y a ainsi un rapport conflictuel difficile à gérer entre le responsable des données et l'organisme cantonal ou communal. Le premier doit garantir le respect de toutes les exigences en matière de raccordement en ligne alors que le second est responsable et autonome en ce qui concerne les tâches, les compétences et les responsabilités correspondantes ainsi qu'en matière d'organisation structurelle et procédurale.

9. Dans ce sens, le responsable des données ne peut pas non plus contrôler si l'autorité cantonale ou communale demanderesse répond à une volonté politique et si la demande de raccordement fait suite à un accord de l'autorité politique responsable. Une telle décision ne pourrait être atteinte qu'au moyen d'une procédure d'autorisation cantonale.

   Dans ce contexte, l'**ordonnance lucernoise relative aux principes en matière de sécurité et de procédure d'autorisation dans le domaine des transferts électroniques de données** du 23 avril 1996 (*Verordnung über die Sicherheitsgrund-sätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches*

vom 23. April 1996, SRL Nr. 39b, Sicherheitsverordnung LU) peut être citée comme exemple. Cette ordonnance prévoit que chaque raccordement d'unités administratives du canton au réseau de communication nécessite une autorisation du chef du département concerné. L'octroi d'une autorisation d'accès exige un examen des risques accompagné de propositions de mesures. De plus, le Préposé cantonal à la protection des données doit être entendu et le responsable informatique du département concerné est responsable de la réalisation et de la mise en œuvre conforme du raccordement. Ainsi, l'autorité qui fait la demande pour un raccordement en ligne s'assure d'une part que le respect des prescriptions et des principes légaux fasse l'objet d'un examen et d'autre part, que le raccordement en question ait bien été sanctionné par une unité administrative indépendante et d'un rang hiérarchiquement supérieur.

10. Le cadre technique général (banques de données, Internet et Intranet) favorise l'échange direct de données entre services spécialisés de la Confédération et des cantons. La voie hiérarchique par l'unité administrative supérieure (instance de conduite) ne revêt plus que peu, voire plus aucune importance car les contacts entre les responsables de la conduite et ceux de l'informatique ne sont pas suffisants. C'est en effet pour cette raison que les instruments nécessaires à la gestion et à l'identification des problèmes ne sont ni créés, ni mis en place. Il est plus simple et plus rapide de trouver des solutions présentant un haut degré d'utilité au niveau technique. Dans ce contexte, le fait d'associer l'instance de conduite à la décision est (notamment pour des raisons de manque de connaissances de l'environnement technique) de plus en plus souvent considéré comme gênant, ralentissant et générateur d'obstacles (voir également Rapport CCF, pages 28 et 29). Ainsi, il est possible que la pratique en matière de raccordements en ligne s'oriente de plus en plus en fonction de ces aspects techniques et que l'on tienne de moins en moins compte des aspects de nécessité, de proportionnalité et d'opportunité des liaisons en ligne.

11. L'expert n'a trouvé aucune directive en matière d'autorisation d'accès en ligne pour les représentations suisses à l'étranger et les services d'Interpol. Le processus d'autorisation correspondant semble avoir été fixé par les secrétariats généraux du DFJP et du DFAE.

12. Les compétences et les unités organisationnelles énumérées dans le règlement d'utilisation et de maintenance de l'OFP de mai 1987 ainsi que dans les instructions de l'Office fédéral de la police concernant la mise en service de RIPOL 2 du 25 juin 1990, ne correspondent plus aux structures organisationnelles actuelles, ce qui, d'une part, gêne la transparence dans le domaine des tâches, des compétences et des responsabilités et, d'autre part, favorise le développement irresponsable d'un domaine échappant aux contraintes administratives et juridiques.

329 Recommandations et propositions de mesures au sujet du RIPOL et de DOSIS

1. Le législateur doit prendre conscience avec plus d'acuité de cette problématique de délégation de compétences. L'évolution technologique continue qui caractérise le domaine de la communication exige du législateur, donc de celui qui rédige les lois, qu'il fasse appel à des notions juridique très concises et univoques excluant toute multiplication insidieuse des accès en ligne au-delà de la volonté initiale du législateur. Les clauses générales de délégation de compétences doivent être analysées avec précision afin d'en saisir les effets. La volonté politique en matière d'octroi d'autorisations doit être formulée avec une précision qui permette au législateur de définir clairement et sans équivoque jusqu'à quel niveau hiérarchique il consent à déléguer des compétences permettant d'octroyer des autorisations en matière d'accès en ligne. Si le législateur veut parvenir à imposer un nombre restreint de raccordements en ligne, il doit éviter les clauses générales du genre de celle de l'article 351bis, 3^{e} alinéa, lettre h CP (« autres autorités judiciaires et administratives »)

2. Les unités administratives (office fédéral, division, section etc.) elles-mêmes utilisatrices d'un système d'information ne doivent pas être en même temps autorité concédante en matière de raccordement en ligne si cela risque de provoquer des conflits d'intérêts ou de donner une telle impression. Une unité administrative hiérarchiquement supérieure est mieux à même d'assumer le rôle d'autorité concédante indépendante dans la mesure où elle ne défend pas d'intérêts propres.

3. Le DFJP doit contrôler la délégation générale des compétences jusqu'au bas de la hiérarchie et dans tous les domaines concernés. Les autorisations d'accès en ligne doivent être octroyées par une instance concédante adéquate et indépendante qui soit consciente tant de l'importance et de la portée de sa décision que de la sensibilité des données traitées. L'exigence minimale devrait être que tous les premiers raccordements en ligne d'une unité administrative fédérale, cantonale ou communale ne puissent être autorisés qu'au niveau hiérarchique de la direction de l'office fédéral concerné. Ainsi, en ce qui concerne les représentations suisses à l'étranger et les services d'Interpol (RIPOL : conventions internationales) ou d'autres services de police étrangers (DOSIS : Convention Europol), le DFJP doit désigner une instance concédante hiérarchiquement conforme ayant des intérêts compatibles avec cette fonction. Le cas échéant, il doit engager une modification des ordonnances correspondantes du Conseil fédéral.

4. Le DFJP doit fixer les procédures d'autorisation en matière de raccordement en ligne au moyen de diagrammes (description des processus), de manière la plus homogène possible pour tous les offices fédéraux concernés. Ces descriptions doivent au moins avoir le statut de directives du département et s'inspirer des standards de la norme ISO. De plus, elles doivent également être harmonisées par rapport aux descriptions de processus actuels du Centre de calcul du DFJP.

5. Le DFJP doit étudier quelles exigences minimales les autorités concédantes et les instances de surveillance cantonales et communales doivent remplir afin de garantir un traitement conforme à la loi et à la sensibilité des données ainsi que le respect des principes de nécessité, de proportionnalité et d'opportunité. Ces exigences doivent être intégrées dans des textes législatifs idoines.

6. Lorsqu'il y a traitement de données personnelles particulièrement dignes de protection, le DFJP doit, au moyen d'une réglementation adéquate, veiller à l'élaboration de la base légale formelle nécessaire avant l'initialisation de tout projet informatique dans le domaine de la police. De plus, afin de préciser explicitement et formellement les exigences minimales que les projets pilotes de l'administration fédérale traitant des données sensibles doivent respecter, le DFJP, en collaboration avec le Préposé à la protection des données, doit examiner l'opportunité d'ajouter une disposition correspondante dans la loi fédérale sur la protection des données.

7. Le DFJP doit également examiner dans quelle mesure l'exécution des bases légales en matière de raccordements en ligne ainsi que le respect et l'actualisation des mesures techniques et organisationnelles de protection pourraient être garantis par le biais de contrats d'exploitation liant l'utilisateur (l'unité administrative fédérale, cantonale ou communale qui exploite les données du système) au responsable des données (l'organe fédéral compétent).

8. Dans le cadre de la Conférence des chefs des départements cantonaux de justice et de police, le DFJP doit discuter avec les directeurs cantonaux concernés (conseillers d'Etat) de la problématique des demandes d'accès en ligne formulées par les unités administratives du bas de la hiérarchie. Il s'agit de déterminer des standards minimaux

communs en matière de procédures d'autorisation cantonales en tant qu'étape préalable aux demandes déposées auprès des autorités fédérales compétentes.

9. L'OFP doit adapter le règlement d'utilisation et de maintenance de l'OFP de mai 1987 ainsi que règlement de traitement DOSIS du 20 décembre 1996 aux circonstances effectives et aux conditions juridiques actuelles (modifications de l'organisation, modification de l'ordonnance DOSIS entrée en vigueur le 1er janvier 1998, notamment de l'article 4 du règlement de traitement concernant la provenance des données). Ce faisant, il doit tenir compte des principes que le DFJP doit encore fixer selon le point 3 des présentes recommandations. La procédure d'autorisation en matière de raccordements en ligne, la question de l'unité administrative compétente, les conditions devant faire l'objet d'un examen et l'archivage des décisions correspondantes doivent être réglés d'entente avec le DFJP. En outre, dans la mesure du possible, les règlements doivent tenir compte de la nouvelle organisation structurelle de l'OFP (offices centraux de police criminelle). Cette exigence a été partiellement remplie par l'élaboration du nouveau règlement de traitement DOSIS du 20 décembre 1996.

10. En ce qui concerne les raccordements en ligne aux systèmes informatiques de la Confédération, l'Office fédéral de l'informatique (OFI) doit examiner s'il convient de compléter le manuel de gestion de projets HERMES 95 de manière à créer un soutien durable pour les mesures proposées ci-dessus et afin d'assurer la transparence, l'efficacité et la qualité lors de la réalisation des liaisons en ligne dans le cadre des projets informatiques de la Confédération.

33 ISIS et ISIS-PLUS

331 Bases et principes légaux

Sûreté intérieure (ISIS)

a) Ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat du 31 août 1992 avec modification du 2 décembre 1996 (RS 172.213.60).
b) Ordonnance concernant le traitement des données personnelles lors de l'application de mesures préventives dans le domaine de la protection de l'Etat du 14 juin 1993 (RS 235.14).
c) Directives sur la mise en application de la protection de l'Etat du 9 septembre 1992 avec modification du 22 décembre 1993.
d) Directives du DFJP sur le système informatique provisoire de données relatives à la protection de l'Etat (directives ISIS) du 31 août 1992.
e) ISIS-Bearbeitungsrichtlinien des Chefs der Bundespolizei vom 1.2.1995 (Weisung Nr. 082) mit Anhang 1 vom 22. Mai 1997 (Vollzugsweisung betreffend Registrierung der Mitgliedschaft bei staatsschutzrelevanten Organisationen/Gruppierungen), Anhang 2 vom 1.6.1994 (Check- und Punkteliste gesicherte/ungesicherte Vorgangsdaten) und Anhang 3 (undatiert; Richtlinie über Zuordnung von Datenbank und Vorgangskategorie).
f) Weisung des Chefs der Bundespolizei über die Erfassung von Personen/Organisationen in den Datenbanken STA/NSS vom 21.9.1995 (Weisung Nr. 086) mit Memos vom 6.10.1995 und 24.2.1997 zu Weisung Nr. 086.

En résumé, ces bases légales permettent de déduire les principes suivants :

331.1 Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

En ce qui concerne les bases légales, il convient de remarquer tout d'abord que, malgré le non-aboutissement du référendum facultatif et la décision correspondante de la Chancellerie fédérale (voir FF 1997 IV 1427 et ss.), la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) du 21 mars 1997 n'avait pas encore été mise en vigueur par le Conseil fédéral au moment de la rédaction du présent rapport. Selon les informations fournies par la Chancellerie fédérale et l'Office fédéral de la justice, il s'agissait d'attendre le résultat de la votation populaire sur l'initiative « SOS » avant de mettre la LMSI en vigueur. Cette votation a été fixée au 7 juin 1998. En cas de refus de l'initiative, la loi n'entrerait en vigueur que le 1er octobre 1998 au plus tôt, voire le 1er janvier 1999. Entre-temps, le Conseil fédéral a décidé de faire entrer la LMSI en vigueur au 1er juillet 1997. Les dispositions d'exécution correspondantes (ordonnances du Conseil fédéral) devraient être prêtes en même temps (voir également point 357). Le contenu de ces ordonnances n'est pas encore connu. La LMSI apporte une nouvelle base juridique comprenant des principes correspondants relatifs à la pratique en matière d'autorisation d'accès et de maniement du système de traitement des données concernant la protection de l'Etat.

En vertu de l'article 11, 1er alinéa de la LMSI, le Conseil fédéral règle par voie d'ordonnance les faits et les constatations que les cantons ainsi que les autorités et offices mentionnés à l'article 13 sont tenus d'annoncer spontanément. Il fixe l'étendue du devoir d'information et la procédure de communication des renseignements. Les informations peuvent être recueillies par le biais :

- de l'exploitation de sources accessibles au public,
- de demandes de renseignements,
- de la consultation de documents officiels,
- de la réception et de l'exploitation de communications,
- d'enquêtes sur l'identité ou le lieu de séjour de personnes,
- de l'observation de faits, y compris au moyen d'enregistrements d'images et de sons, dans des lieux publics et librement accessibles,
- du relevé des déplacements et des contacts de personnes.

Les informations ainsi recueillies doivent être traitées selon les principes de l'article 15, 1er alinéa LMSI. Les organes de sûreté ne peuvent traiter des données sensibles et établir des profils de personnalité que conformément à l'ordonnance (article 15, 2e alinéa LMSI). L'office fédéral [service de police du Ministère public de la Confédération (Police fédérale)] traite au moyen d'un système d'information électronique (= base légale formelle pour le système d'information ISIS) les données dont l'accès rapide doit être garanti en permanence. Le système ISIS ne peut être rendu accessible, au moyen d'une procédure d'appel, qu'aux personnes exerçant des tâches définies par la présente loi au sein de l'office fédéral, aux autres autorités de police et de poursuite pénale de la Confédération ainsi qu'aux organes de sûreté des cantons. La définition des conditions de raccordement des organes de sûreté des cantons est déléguée au Conseil fédéral, les droits d'accès sont réglés par le département (article 15, 3e alinéa LMSI). Dans le système d'information, les données de la police judiciaire et les données recueillies en dehors d'une enquête de police judiciaire doivent être traitées séparément. Ce système d'information doit être géré séparément des autres systèmes d'information de la police ou de l'administration (article 15, 4e alinéa LMSI). Les cantons traitent conformément aux prescriptions de la Confédération les données qu'ils reçoivent durant l'exécution de la présente loi. Ils les conservent séparément des données cantonales (article 16, 1er alinéa LMSI). Lorsque les organes de sûreté des cantons gèrent leur propre système d'information automatisé, les prescriptions relatives au système d'information de la Confédération sont applicables par analogie. Le règlement d'exploitation du système cantonal doit être approuvé par le département (article 16, 2e alinéa LMSI). Lorsque les organes de sûreté des cantons traitent des données en vertu de la présente loi, ils sont soumis au droit fédéral sur la protection des données (article 16, 3e alinéa LMSI).

La nouvelle loi prévoit également la possibilité de procéder à des contrôles de sécurité relatifs à des personnes (section 4 LMSI). Dans certaines conditions prévues par la loi, le Conseil fédéral peut prévoir des contrôles de sécurité à l'égard d'agents de la Confédération, de militaires et de tiers collaborant à des projets classifiés relatifs à la sûreté intérieure ou extérieure (article 19, 1er alinéa LMSI). Les cantons peuvent également assujettir leurs agents à un contrôle de sécurité lorsque ceux-ci coopèrent directement à des tâches de la Confédération définies par cette loi (article 19, 2e alinéa). Le Conseil fédéral désigne un service spécialisé chargé de procéder aux contrôles de sécurité en collaboration avec l'office fédéral (article 21 LMSI).

La section 6 est consacrée aux dispositions relatives à l'organisation. Selon ces dispositions, le contrôle parlementaire est assuré par la Délégation des commissions de gestion (article 25, 1er alinéa LMSI). Le Conseil fédéral veille à ce que la légalité, l'opportunité et l'efficacité de l'activité de l'office fédéral soient contrôlés. Le DFJP établit un plan de contrôle annuel qu'il coordonne avec les contrôles parlementaires (article 26, 1er alinéa LMSI). Le Conseil fédéral fixe également les exigences minimales pour le contrôle applicables dans les cantons. L'exécution des contrôles incombe aux cantons (article 26, 3e alinéa LMSI). L'office fédéral doit renseigner en permanence les chefs des départements cantonaux de police et les organes de sûreté sur les mesures prises ou planifiées en vertu de la LMSI (article 27, 3e alinéa LMSI).

331.2 Ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat (RS 172.213.60)

Pour la raison déjà évoquée ci-dessus, l'ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat (Ordonnance ISIS) du 31 août 1992 est actuellement encore la base légale déterminante pour les questions d'accès en ligne. Cette ordonnance est fondée sur les dispositions des chiffres 8 à 10 de l'article 102 de la Constitution fédérale (RS 101), sur l'article 24 de la loi fédérale sur la protection des données (RS 235.1) ainsi que sur les articles 15, 17, 100 et ss. de la loi fédérale sur la procédure pénale (RS 312.0). Le Conseil fédéral a prolongé la durée de validité de cette ordonnance du 2 décembre 1996 au 31 décembre 1999 (article 24, 2e alinéa ordonnance ISIS). *Il n'y a donc pas de base légale formelle* pour la mise en place et l'exploitation du système de traitement des données *ISIS et* donc *pour le traitement des données et des données sensibles au sens de la loi sur la protection des données*. La LMSI crée les bases légales correspondantes (article 15, 3e alinéa LMSI).

En vertu de l'article 1er de l'ordonnance ISIS, le service de police du Ministère public de la Confédération (Police fédérale) exploite un système provisoire de traitement des données relatives à la protection de l'Etat (ISIS). En vertu du 4e alinéa de l'article 3 de l'ordonnance ISIS. Le DFJP fixe dans des directives les données qui peuvent être mémorisées. Il y énonce les différentes catégories de données. Ces directives (directives ISIS) datent du 31 août 1992. Seuls les agents de la Police fédérale sont autorisés en tant qu'utilisateurs d'ISIS. Par ailleurs, le Procureur général de la Confédération et son substitut sont habilités à interroger les banques de données. D'autres agents du Ministère public de la Confédération peuvent, pour accomplir des tâches légales, demander l'accès à certaines données dans les cas suivants :

a) certains agents du Service juridique, pour collaborer au déroulement de procédures pénales intéressant ou non la protection de l'Etat, ainsi que pour exécuter des tâches administratives ;
b) certains agents des Services centraux, pour exécuter des tâches administratives ;
c) certains agents du Service de sécurité de l'administration fédérale, pour exécuter des tâches de police de sécurité.

Le département peut, dans des cas particuliers, autoriser des agents de l'Office fédéral de la police à consulter certaines données des banques « protection de l'Etat » et « procédures pénales n'intéressant pas la protection de l'Etat », pour accomplir des tâches prévues par la loi (article 4 ordonnance ISIS). Le département édicte des directives concernant le droit des utilisateurs visés à l'article 4 d'accéder aux différentes données (données de base et catégories d'antécédents) et concernant les formes de traitement des données (afficher, introduire, imprimer, éliminer). Le droit d'accès doit être spécialement fixé pour chaque catégorie d'antécédents (article 5, 3e alinéa ordonnance ISIS). Le département doit également édicter des directives concernant l'interrogation simultanée par le biais de plusieurs clés de recherche (article 8, 2e alinéa ordonnance ISIS), concernant la durée de conservation des différentes catégories de données (article 13, 3e alinéa ordonnance ISIS) ainsi que sur les mesures organisationnelles et techniques contre le traitement non autorisé des données et sur le protocole automatique des données (article 20, 2e alinéa ordonnance ISIS). Les données d'ISIS ne peuvent être reportées dans d'autres banques de données ni par le biais d'installations de communication ni au moyen de supports de données (article 11 ordonnance ISIS). Le chef de la Police fédérale assume la responsabilité d'ISIS. Le service compétent du Centre de calcul DFJP est responsable de la maintenance et de la sécurité, ainsi que du respect des droits d'accès (article 23, 1er et 2e alinéas ordonnance ISIS).

331.3 Directives sur le système informatique provisoire de données relatives à la protection de l'Etat (directives ISIS du 31 août 1992)

La saisie des données, le contrôle de qualité, les catégories de données, les droits d'accès, le protocole automatique ainsi que de divers points supplémentaires sont réglés dans les directives ISIS du DFJP du 31 août 1992. Ces directives ne présentent qu'un intérêt marginal en ce qui concerne l'accès en ligne proprement dit. Ainsi, l'article 2, 2e alinéa lettre d contient une précision concernant la consultation (appel direct) de certaines catégories de données par l'Office fédéral de la police qui y est raccordé. Cette disposition permet au Procureur général de la Confédération ou au chef de la Police fédérale d'autoriser la consultation directe des principaux renseignements biographiques mémorisés dans les banques de données « protection de l'Etat » et « procédures pénales n'intéressant pas la protection de l'Etat ». Le directeur de l'Office fédéral de la police détermine, en accord avec le procureur général de la Confédération, quels sont les agents autorisés à consulter des données directement. Les processus d'interrogation qui font simultanément appel à plus de trois clés de recherche dans un champ de données doivent avoir été préalablement approuvés par le chef de la Police fédérale ou par ses remplaçants ; la demande à cette fin doit mentionner le but de l'interrogation et la durée de l'autorisation (article 4, 2e alinéa directives ISIS). Les services de la Confédération et des cantons qui fournissent des données sont également concernés par les dispositions de l'article 7 de ces directives. Le Service de contrôle de la Police fédérale communique, au service ayant fourni les données, l'effacement des données d'ISIS aux fins de la destruction des données et documents tenus parallèlement (article 7 directives ISIS). L'ordonnance concernant le traitement des données personnelles lors de l'application de mesures préventives dans le domaine de la protection de l'Etat complète les dispositions concernant le traitement de données personnelles par les organes cantonaux chargés de la protection de l'Etat en disposant que les cantons doivent protéger les documents relatifs à la protection de l'Etat (documents du Ministère public de la Confédération) conservés sur leur territoire contre l'accès de personnes non autorisées. Ces données doivent être conservées à l'écart des autres informations de police. Celles qui sont mémorisées sur des supports électroniques doivent bénéficier de mesures de sécurité adéquates. Les cantons règlent l'accès aux données et aux documents (article 5, 2e alinéa ordonnance concernant le traitement des données personnelles lors de l'application de mesures préventives dans le domaine de la protection de l'Etat). Sur réquisition de la Police fédérale, les cantons détruisent les données personnelles devenues inutiles pour la protection fédérale de l'Etat (article 5, 4e alinéa ordonnance concernant le traitement des données personnelles lors de l'application de mesures préventives dans le domaine de la protection de l'Etat).

331.4 Modèle de règlement d'exploitation par système TED à l'attention des cantons

En avril 1994 déjà, la Police fédérale avait élaboré un modèle de « règlement d'exploitation par système TED » à l'attention des cantons et y avait réglé les principes de la collaboration entre la Confédération et les cantons dans le domaine des tâches fédérales de protection de l'Etat. Ces principes peuvent être illustrés grâce à l'exemple lucernois : « *EDV-Betriebs-ordnung des Spezialdienstes der Kantonspolizei Luzern für das Projekt INSEL* » du 23 août 1994.

Ce règlement fixe que l'organe cantonal chargé de tâches fédérales de protection de l'Etat (c'est-à-dire le « *Spezialdienst der Kantonspolizei Luzern* ») exploite un système informatisé de traitement des données intitulé « *INSEL* ». Le projet « *INSEL* » permet de traiter

a) les données relatives aux procédures pénales relevant de la juridiction fédérale,
b) les données relatives aux mesures préventives de la protection fédérale de l'Etat,
c) les données relatives à l'accomplissement de tâches de police de sécurité sur mandat général du Ministère public de la Confédération.

Les données touchant à la protection fédérale de l'Etat (sur les plans préventif et répressif) sont traitées dans une banque de données déterminée et indépendamment des autres données. Le « journal des dossiers » correspondant doit également être tenu de manière séparée de la banque des données relative à la protection de l'Etat. Le droit général d'accéder aux champs contenant des informations d'ordre général (article 3, 2e alinéa modèle de règlement) est réglé séparément à l'annexe 1. Les données touchant à la protection fédérale de l'Etat ne peuvent être reportées dans d'autres banques de données, ni par le biais d'installations de communication, ni au moyen de supports de données. Après l'effacement d'un bloc de données, les documents afférents sont détruits. L'archivage des documents relatifs à la protection de l'Etat incombe au Ministère public de la Confédération. L'organe cantonal chargé de tâches fédérales de protection de l'Etat (*Spezialdienst der Kantonspolizei Luzern*), le chef du département et le Préposé à la protection des données du canton de Lucerne portent la responsabilité du projet « *INSEL* ». Le règlement d'exploitation par système TED a été signé par le commandant de la police cantonale de l'époque. Le DFJP a approuvé ce règlement le 23 août 1994.

332 Situation actuelle en matière de liaisons en ligne

Nombre d'utilisateurs

Selon la liste chronologique des liaisons en ligne avec ISIS, document non daté dont l'actualité a été confirmée lors de l'audition du représentant de la Police fédérale du 11 février 1998

200 utilisateurs

ont été reliés à ISIS depuis décembre 1993 jusqu'à aujourd'hui.

Catégories d'utilisateurs

La légitimité de tous les utilisateurs raccordés découle de l'ordonnance ISIS (article 4, 1er alinéa et 2e alinéa, lettres a à c ainsi que 3e alinéa ordonnance ISIS). **Seuls des services de la Confédération sont raccordés à ISIS. Pour l'instant, aucun service cantonal ne s'est raccordé** (**ISIS-PLUS**, à ce propos, voir également point 337 ci-dessous). Le système d'information ISIS est avant tout un système interne à la Police fédérale. Il est utilisé par la Police fédérale (102 raccordements), par le Procureur général de la Confédération et son substitut (2 raccordements), par le service juridique (5 raccordements), par les services centraux (8 raccordements) ainsi que par le service de sécurité de l'administration fédérale (7 raccordements). L'OFP est la seule unité administrative externe à la Police fédérale qui y

est raccordée. Selon la documentation du service de contrôle de la Police fédérale du 11 février 1998, 76 personnes disposent d'un accès direct à ISIS (50 personnes de la Division Offices centraux et 26 personnes de la section Interpol). En s'appuyant sur l'article 5, 3e alinéa de l'ordonnance ISIS, le DFJP fixe les droits d'accès dans ses directives sur le système informatique provisoire de données relatives à la protection des données (directives ISIS) du 31 août 1992.

La Police fédérale dispose de terminaux extérieurs permanents dans les villes de Bâle, de Fribourg, de Genève et de Zurich. Selon les données de la Police fédérale du 19 février 1998 (remise ultérieure de documents à l'expert), ces terminaux sont situés dans des locaux des commandements des polices cantonales respectives. Les liaisons de ces terminaux extérieurs sont assurées au moyen de lignes standard et les transmissions de données sont chiffrées au moyen d'un *Gretacoder*. Les terminaux sont installés dans des locaux indépendants et leur accès est strictement réservé aux agents de la Police fédérale. **Il n'y a pas d'accès de tiers externes à l'administration fédérale**. En cas de menace spéciale, ISIS peut, pour une durée limitée, être mis à disposition de certains agents de polices cantonales qui assument ou contribuent à des tâches relatives à la protection de l'Etat (pour plus de détails à ce sujet, voir ci-dessous point 336).

Réseau et mesures de sécurité
Tous les partenaires raccordés communiquent par le truchement d'infrastructures de la Confédération (LIS/DFJP). La communication est effectuée par TCP/IP (protocoles de communication normalisés). A l'intérieur de cette infrastructure, la Police fédérale est isolée au moyen d'un *Karl-Bridge*, l'Office fédéral de la police reçoit les données chiffrées *end-to-end* au moyen d'une *Kryptobox* et d'une ligne *end-to-end*.

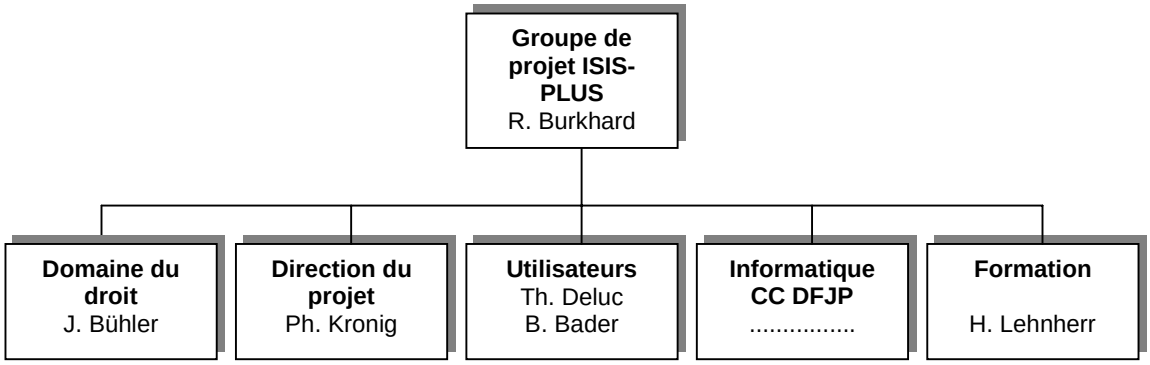
333 Procédure de raccordement

Etant donné que seuls le responsable des données (Police fédérale) et l'Office fédéral de la police sont actuellement raccordés à ISIS, la question des pratiques en matière de raccordements en ligne ne se pose pas (encore) dans la même mesure que pour les autres systèmes d'information dans le domaine de la police. L'OFP a été raccordé à ISIS en vertu de l'article 4, 3e alinéa de l'ordonnance ISIS et de l'article 3, 2e alinéa, lettre d des directives ISIS. Les directives ISIS fixent expressément que, en accord avec le Procureur général de la Confédération, le *directeur de l'OFP* détermine les agents autorisés à consulter (appeler) directement des données.

Avec l'élargissement de l'utilisation d'ISIS et l'important élargissement des catégories d'utilisateurs aux organes de protection de l'Etat des cantons et des villes (ISIS-PLUS), la procédure de raccordement en ligne doit être réglementée (à ce sujet, voir point 339 ci-dessous).

334 Exploitation et maintenance

Le service compétent du Centre de calcul DFJP est responsable de la maintenance et de la sécurité, ainsi que du respect des droits d'accès (article 23, 2e alinéa ordonnance ISIS). Parallèlement, une organisation de projet est en train de préparer le raccordement des cantons et des villes à ISIS dans le cadre du projet ISIS-PLUS. Ce groupe de projet élabore le concept de développement du projet ainsi que les adaptations nécessaires des bases légales (voir point 337 Perspectives de développement ci-dessous).



335 Participation aux coûts

Actuellement, la question de la participation aux coûts du système d'information ISIS n'est pas très importante puisque ce système est exclusivement exploité par des services de la Confédération. La réglementation de la participation aux coûts des cantons et des villes qui utiliseront ISIS n'est pas encore définie. Toutefois, l'article 28 de la LMSI constitue une base légale permettant de rembourser aux cantons les prestations qu'ils ont fournies dans ce domaine. En ce qui concerne les coûts de mise en place et d'exploitation d'ISIS (-PLUS), les mêmes réflexions que pour le RIPOL ou DOSIS devraient être déterminantes. Les systèmes centraux d'information de la Confédération sont soutenus et exploités en commun par les cantons uniquement dans la mesure où les coûts de mise en œuvre et d'exploitation ne sont pas facturés. Naturellement, ce principe s'applique tout particulièrement dans le domaine d'ISIS puisque ce système d'information automatisé permet avant tout de coopérer dans le cadre de tâches de la Confédération. Le rapport du Ministère public de la Confédération et du Centre de calcul du DFJP du 13 mai 1996 concernant les développements d'ISIS [raccordements externes des cantons (ISIS-PLUS)] permet de constater qu'il est prévu que les cantons et les villes doivent supporter les coûts de l'infrastructure nécessaire alors que la Confédération (Ministère public de la Confédération) assure les coûts de maintenance et de réparation (page 3 du rapport).

336 Cantons et autres accès externes à l'administration fédérale

Comme cela a déjà été précisé au point 332 ci-dessus, seuls des services de la Confédération sont actuellement raccordés à ISIS. En cas de menaces spéciales, des services de police cantonaux, qui assument ou contribuent à des tâches relatives à la protection de l'Etat, peuvent être raccordées ISIS, toutefois pour une durée limitée seulement.

Le raccordement du Ministère public du canton de Bâle-Ville lors de la cérémonie commémorative du 1er Congrès sioniste de Bâle en 1897 est un exemple de raccordement en ligne provisoire d'autorités cantonales à ISIS. Cette cérémonie commémorative s'est déroulée à Bâle du 25 au 31 août 1997. Ce cas concret a été décrit par la Police fédérale à l'attention de l'expert.

La Police fédérale coordonne la recherche d'informations sur les menaces potentielles et gère une « plate-forme » permettant de les évaluer de manière continue afin d'informer les autorités responsables. Dans ce domaine, la Police fédérale fait principalement appel à ISIS. Dans le cas de la cérémonie commémorative du 1er Congrès sioniste, il était nécessaire de pouvoir disposer, à Bâle même, d'un accès direct à ISIS de manière à pouvoir accéder aux données à temps et en fonction des besoins. Il a été nécessaire de faire appel au soutien du Ministère public du canton de Bâle-Ville pour qu'il soit possible d'assurer un accès sans faille aux données. Les principales règles de collaboration et d'accès ont été arrêtées dans un accord écrit spécial passé entre le Ministère public de la Confédération (Police fédérale) et le

Ministère public du canton de Bâle-Ville pour la durée du 25 juin au 2 septembre 1997. Ainsi, cet accord précise

- le nom de tous les fonctionnaires de police du canton de Bâle-Ville disposant d'un droit d'accès,
- la compétence de la Police fédérale qui détermine la nature des droits d'accès de ces fonctionnaires de police,
- l'instruction par la police fédérale des fonctionnaires de police nommés dans l'accord,
- l'interdiction de toute transmission de données consultées à des tiers sans autorisation,
- l'obligation pour les fonctionnaires de police nommés dans l'accord de signer une déclaration de discrétion,
- la subordination des fonctionnaires de police nommés dans l'accord à l'autorité et aux instructions du chef de la Police fédérale pour la durée de leurs interventions,
- le droit disciplinaire et les autres conditions applicables.

Au moyen de la demande d'accès du 15 juillet 1997 sur le formulaire idoine (« *ISIS Account Antrag* »), le suppléant du chef de la Police fédérale a communiqué le détail des droits d'accès octroyés (« consultation » dans le cas présent) au superviseur responsable du système.

Par cette procédure, l'octroi d'accès en ligne pour une période limitée dans le temps à des fonctionnaires de police d'un canton chargés de tâches relatives à la protection de l'Etat est institutionnalisé de manière tout à fait opportune, transparente et compréhensible. Les tâches, les compétences et les responsabilités sont clairement réglées dans l'accord précité. En revanche, la définition à caractère obligatoire et revêtant la forme écrite de cette procédure d'autorisation d'accès en ligne sous forme d'acte législatif (ordonnance, directive ou autre) fait défaut. Ce n'est que par ce biais qu'il est possible de garantir que des raccordements en ligne d'autorités de police cantonales limités dans le temps soient toujours établis selon la même procédure sur la base des mêmes documents (formulaires, listes de contrôle) et selon les mêmes critères d'évaluation (nécessité, proportionnalité et opportunité). Comme cela a déjà été constaté pour d'autres systèmes d'information dans le domaine de la police, force est de constater que dans le domaine couvert par ISIS, l'unité administrative de la Confédération directement intéressée et concernée est également l'autorité concédante pour les raccordements de tiers en fonction de ses propres objectifs, besoins et tâches. Il n'y a pas d'autre instance compétente en matière d'autorisation.

337 Perspectives de développement

Point de vue législatif

Les dispositions d'exécution de la LMSI constituent en fait une révision de l'ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat (ordonnance ISIS). Ce texte législatif doit également contenir les dispositions d'exécution en matière de raccordement des cantons au système d'information ISIS-PLUS. La planification correspondante du DFJP prévoit que toutes les dispositions d'exécution basées sur la LMSI soient présentées au Conseil fédéral en un seul paquet afin que le complexe législatif relatif à la protection de l'Etat puisse également entrer en vigueur le 1er octobre 1998. Selon les responsables de la planification de la Police fédérale, cet objectif implique l'horaire suivant : élaboration de l'ordonnance ISIS et consultation interne jusqu'à fin mai 1998, procédure de consultation externe (Préposé fédéral à la protection des données notamment) et modifications éventuelles jusqu'à fin juillet 1998, consultation des offices et modifications éventuelles jusqu'à août 1998 (lettre de la Police fédérale du 19 février 1998).

Point de vue informatique

Le programme d'action « Sûreté intérieure » 1994 prévoyait déjà de raccorder les cantons à ISIS. La base légale pour le raccordement en ligne (par procédure d'appel) d'autres autorités de police et de poursuite pénale de la Confédération ainsi que d'autres organes de sûreté

des cantons a été intégrée dans la LMSI (article 15, 3e alinéa LMSI). De l'avis de la Police fédérale et du Ministère public de la Confédération, il n'y a que le raccordement des cantons à ISIS qui puisse leur donner la possibilité de renoncer à leurs propres systèmes d'information dans le domaine de la protection de l'Etat. Ce n'est que de cette manière qu'il est possible de réduire le risque de mélanger les données du canton avec celles de la Confédération. Par diverses interventions, la Conférence des commandants des polices cantonales de Suisse ainsi que les commandants de divers corps de police cantonaux ont exigé que le raccordement de leurs services spéciaux à ISIS soit réalisé le plus rapidement possible (projet de révision de l'ordonnance ISIS interne au DFJP à l'attention du Conseil fédéral du 22 octobre 1996). Basé sur l'ébauche de concept de développement d'ISIS du 13 mai 1996, dans le cadre d'ISIS-PLUS, il est prévu de raccorder 9 cantons et villes à titre d'essai (Ministère public du canton de Bâle-Ville, les corps de police des cantons de Fribourg, Genève, Lucerne, Saint-Gall, Tessin, Vaud et Zurich ainsi que la ville de Berne). En particulier, ce raccordement à titre d'essai concernera également les banques de données (sous-systèmes) « protection de l'Etat », « procédures pénales n'intéressant pas la protection de l'Etat », et « documentation ». Le système de gestion actuel des utilisateurs doit permettre d'assurer une réglementation sélective des accès. Comme jusqu'à présent, la saisie et le contrôle des données seront assurés par le Ministère public de la Confédération (service préexploitation et service de contrôle). Les cantons et les villes ne sont pas autorisés à modifier les données. Dans ce cas également, les données transitent par le réseau national WAN-DFJP et sont ensuite envoyées par les réseaux locaux LAN, par TCP/IP, aux terminaux autorisés. Au niveau cantonal, 50 collaborateurs devraient être raccordés au total. Du point de vue organisationnel, il est prévu que le chef de la Police fédérale garde la responsabilité d'ISIS. L'accès à ISIS doit être réglé dans l'ordonnance et les directives ISIS, raison pour laquelle ces deux textes législatifs doivent faire l'objet d'une adaptation. Dans le cadre des mesures de sécurité et de la réglementation des droits d'accès aux diverses banques de données (sous-systèmes) de chaque utilisateur, il est expressément prévu que les demandes d'accès à ISIS-PLUS doivent être signées par le chef de la Police fédérale et par le commandant de la police cantonale concernée.

Par sa décision préliminaire du mois de novembre 1996, le chef du Département fédéral de justice et police a reporté le raccordement d'organes cantonaux et municipaux supplémentaires à l'entrée en vigueur de la LMSI. Ce report est lié à la décision du Conseil fédéral d'attendre le résultat de la votation populaire au sujet de l'initiative « SOS » avant de mettre la LMSI en vigueur (voir point 331 ci-dessus).

338 Résumé et appréciation

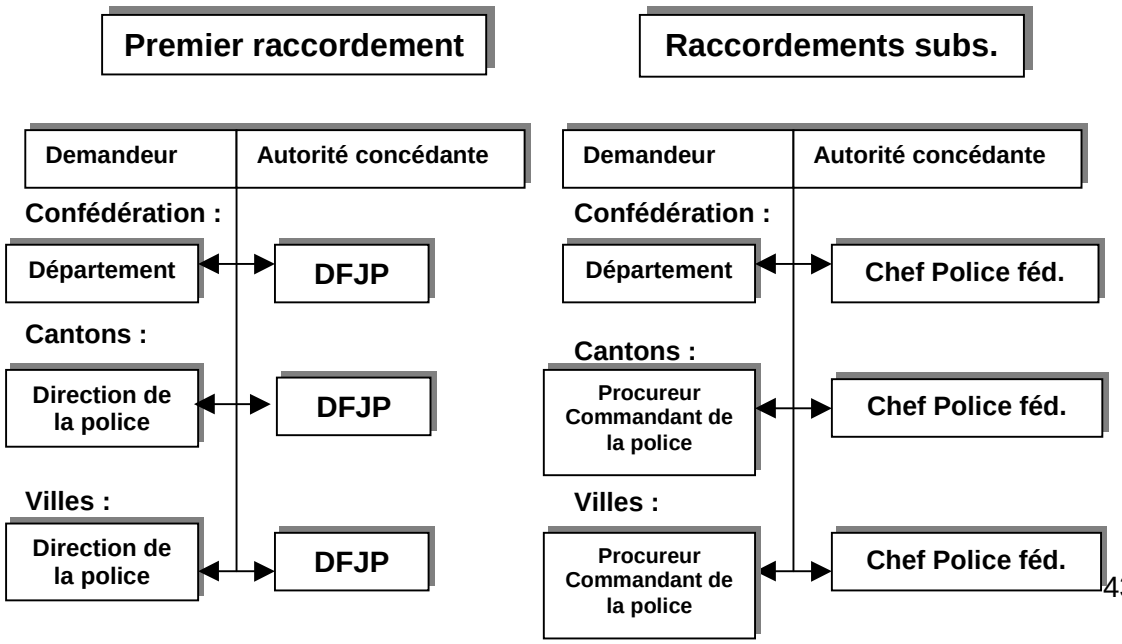
1. Au sein de l'administration fédérale, le système d'information ISIS est avant tout utilisé par le responsable des données lui-même, c'est-à-dire par la Police fédérale. La Police fédérale dispose également de quatre terminaux extérieurs situés dans les villes de Bâle, Fribourg, Genève et Zurich. Il s'agit de liaisons en ligne exclusivement à la disposition d'agents de la Police fédérale. L'OFP est la seule unité administrative extérieure à la Police fédérale (76 utilisateurs) qui utilise ISIS. Actuellement, il n'y a aucun autre organe, fédéral ou cantonal, raccordé en permanence à ISIS.

2. La question de la pratique relative à l'autorisation en matière de raccordements en ligne ne se posera concrètement aux organes compétents qu'une fois la LMSI en vigueur. Les premiers raccordements seront probablement réalisés à la fin de 1998 ou au début de 1999, lorsque les dispositions d'exécution de la LMSI auront été mises en vigueur. Ainsi, dans le domaine sensible couvert par ISIS, il est encore possible de régler clairement la procédure, les tâches, les compétences, les responsabilités ainsi que les points devant être examinés à l'occasion des demandes de raccordement en ligne.

3. Il en va pour ISIS comme des autres domaines couverts par les systèmes d'information de police : les principes régissant les raccordements en ligne mis en place par les

dispositions de droit supérieur (lois, ordonnances) menacent de se perdre au fur et à mesure de la délégation des responsabilités correspondantes vers le bas. En effet, une telle délégation à une unité opérationnelle peut conduire à des interprétations et des défenses d'intérêts différentes de celles qui avaient motivé le législateur à l'origine. En outre, il est possible qu'une telle pratique provoque des conflits d'intérêts (utilisateur du système, responsable du contenu des banques de données et instance d'autorisation en même temps). La délégation continue des tâches, compétences et responsabilités ainsi que l'inscription de cas en cas de ces principes originels dans diverses décisions (octrois d'autorisation d'accès) au plus bas niveau hiérarchique, font que ces derniers finissent par ne plus être observés. Il serait judicieux que les critères décisionnels importants en matière d'autorisation de raccordements en ligne, la procédure et les compétences soient concentrés et fixés de manière harmonisée par une unité administrative hiérarchiquement adéquate. Ceci est d'autant plus nécessaire que, en ce qui concerne les autorités de police cantonales qui assument temporairement des tâches de la Confédération en matière de protection de l'Etat, la Police fédérale dispose déjà d'une procédure interne d'autorisation d'accès pour une durée déterminée qui ne fait appel à aucun service indépendant pour examiner la demande et octroyer l'autorisation d'accès en ligne.

4. La procédure d'autorisation des raccordements en ligne d'organes de protection de l'Etat des cantons et des villes qui devra être en place lors de l'entrée en vigueur de la LMSI et de l'extension de l'utilisation du système par ces organes de protection de l'Etat n'est pas encore réglée. Les travaux dans ce domaine ont lieu dans le cadre de la révision de l'ordonnance et ne sont pas encore achevés. Il faut tenir compte du fait que les exigences envers les utilisateurs de l'administration fédérale sont très sévères. Il est vrai que les données qui sont mémorisées et traitées sont tout particulièrement dignes de protection. Au vu de l'importance de ces aspects, il est tout à fait justifié que les autorités politiques (directeurs de la police des cantons ou des villes concernés) soient appelées à intervenir directement dans le cours de la procédure d'autorisation d'accès de leur canton ou de leur ville. Les 3^{e} et 4^{e} alinéas de l'article 7 LMSI pourraient être complétés en prévoyant, du côté des demandeurs, que les détenteurs de la responsabilité politique (chef de département pour la Confédération, directeurs de la police pour les cantons et les villes) soient associés à la demande de *premier raccordement* d'un organe externe de protection de l'Etat et, du côté de l'autorité concédante, la mise en place d'une instance en matière d'autorisation indépendante (par exemple le secrétariat général du DFJP). Les *raccordements subséquents* à réaliser sur la base d'une décision pourraient ensuite faire l'objet d'une demande du commandant de la police ou du procureur général du canton concerné et être aurtorisés par le chef de la Police fédérale (en tant que responsable des données et responsable suprême du système d'information ISIS) .



5. Les organes de protection de l'Etat des cantons et des villes doivent être liés par des règlements d'exploitation des moyens informatiques aux mêmes conditions sévères que celles qui sont appliquées au sein de la Confédération. Ces règlements d'exploitation cantonaux doivent être approuvés par le DFJP (article 16, 2e et 3e alinéas LMSI). Le modèle de règlement d'exploitation par système TED est une très bonne base de départ. Une fois la LMSI en vigueur, il constitue une base légale suffisante pour l'exécution des principes relatifs au organes de protection de l'Etat des cantons et des villes qu'il contient (article 16, 2e alinéa LMSI). Lorsque le législateur le prévoit expressément, il s'avère que de tels règlements d'exploitation permettent au responsable des données et de l'exploitation du système de lier les utilisateurs externes et de leur faire respecter les standards minimaux de la Confédération.

6. De toute évidence, certains cantons gèrent des systèmes d'information automatisés dans le domaine de la protection de l'Etat (préventive et répressive) et dans celui de la procédure pénale en ce qui concerne la juridiction fédérale. Il faut s'intéresser à ces systèmes. En effet, de tels systèmes permettent de traiter des informations relatives à la protection de l'Etat parallèlement à ISIS et sans qu'il y ait de raccordement en ligne avec ISIS. Cette situation conduit à des redondances entre les organes fédéraux et cantonaux de protection de l'Etat avec le risque que les données des différents systèmes (ISIS, systèmes des cantons) ne puissent être tenues à jour et harmonisées qu'au prix d'efforts importants. De plus, sur ordre de la Police fédérale ou à l'expiration de leur durée de conservation, les instances cantonales doivent spontanément effacer les données relatives à la protection de l'Etat et à la procédure pénale (article 15 ordonnance ISIS, article 7 directives ISIS). Le contrôle par la Police fédérale de ces destructions de données dans les systèmes cantonaux est une procédure très lourde. Sur la base des informations obtenues à l'occasion de l'audition du 11 février 1998 du représentant de la Police fédérale, il faut partir du principe que, actuellement, personne n'est en mesure de contrôler le respect des principes contenus dans tous ces règlements d'exploitation relatifs aux services spéciaux cantonaux. La raison principale provient du manque de personnel en mesure d'effectuer ces contrôles (note d'entretien de l'expert du 11 février 1998). Ce fait est préoccupant dans la mesure où la réglementation au niveau fédéral de l'exploitation d'ISIS est très stricte. Les cantons enregistrent et exploitent également des données relatives à la protection de l'Etat. En revanche, le respect de ces réglementations restrictives (en particulier en ce qui concerne la destruction de données sur ordre de la Police fédérale) n'est pas garanti au niveau cantonal alors même qu'elles concernent des tâches de la Confédération.

7. Avec le raccordement des organes de protection de l'Etat des cantons et des villes au système d'information ISIS au moyen de liaisons en ligne, il est possible de concentrer les données dans un système unique. Les mesures de contrôle peuvent être réduites lorsque les systèmes décentralisés des cantons et des villes ne contiennent plus de données relatives à la sécurité de l'Etat. En outre, le contrôle du respect des dispositions en matière de protection des données devrait également s'en trouver simplifier puisqu'il est alors possible de réglementer et de gérer l'accès et la consultation de ces données de manière harmonisée et centralisée. Il est donc souhaitable de raccorder rapidement les organes cantonaux et municipaux assumant des tâches de la Confédération en matière de protection de l'Etat, tout en effaçant simultanément les informations relatives à la protection de l'Etat mémorisées de manière décentralisée.

8. La disposition de l'article 3, 2e alinéa, lettre d des directives ISIS du DFJP selon laquelle le directeur de l'Office fédéral de la police détermine les agents autorisés à consulter (appeler) directement des données en accord avec le *Procureur général de la Confédération* est pour le moins imprécise. Au vu des bases légales en vigueur, en tant que responsable des données, seul le chef de la Police fédérale (article 26, 1er alinéa

ordonnance ISIS) a le pouvoir de décision en matière de raccordements. Il en assume la responsabilité alors que le Procureur général de la Confédération en assume la surveillance. Dans le cadre d'ISIS, le Procureur général de la Confédération n'est qu'un utilisateur (article 4, 2e alinéa ordonnance ISIS). En tant qu'utilisateur, il ne peut donc pas avoir de pouvoir décisionnel définitif en matière d'autorisation d'accès. Le directeur de l'OFP ne peut pas « déterminer » les agents de l'OFP qui ont le droit d'accéder aux données. Dans le cadre de ses compétences, il peut tout au plus décider – de manière interne – pour quels collaborateurs de l'OFP il est nécessaire de présenter une demande de raccordement en ligne à la Police fédérale. Seul le chef de la Police fédérale est habilité à examiner les conditions d'un tel raccordement et à octroyer l'autorisation d'exploiter les données d'ISIS. Pour cette raison, il serait nécessaire de préciser la lettre d du 2e alinéa de l'article 3 des directives ISIS du DFJP, en tentant en particulier compte des explications concernant l'instance indépendante en matière d'autorisation (voir point 338, lettre 3 ci-dessus).

9. Alors que dans d'autres domaines (RIPOL, DOSIS) les questions relatives au financement et à la répartition des coûts entre la Confédération et les cantons sont réglées dans le cadre de l'ordonnance, en ce qui concerne ISIS il n'y a, jusqu'à présent, pas de disposition assez précise à ce sujet. Au niveau de la loi, la LMSI (article 28) ne règle que les prestations financières allouées aux cantons pour les prestations qu'ils ont fournies sur mandat de la Confédération. Les questions de financement doivent être réglées à l'occasion de la révision de l'ordonnance ISIS et de son adaptation à la LMSI. A ce propos, les résultats de l'examen du CCF contenus dans son rapport (Rapport CCF, pages 32 et suivantes) ainsi que les principes déjà en vigueur actuellement (article 22 ordonnance RIPOL, article 20 ordonnance DOSIS) doivent être intégrés dans une réglementation correspondante des questions de financement.

339 Recommandations et propositions de mesures

1. Le DFJP doit fixer les tâches, les compétences et les responsabilités (autorités compétentes pour l'octroi d'autorisations) en matière de raccordement en ligne des organes de protection de l'Etat de la Confédération, des cantons et des villes. Il doit également définir la procédure (procédure d'autorisation et de demande d'autorisation), les critères à la base de l'examen de la demande (raisons justifiant la demande de raccordement), les exigences minimales en matière de documentation (décision de raccordement formelle) ainsi que les questions relatives à l'archivage (archivage de l'autorisation). Ce faisant, il doit prévoir une délégation des compétences en matière d'autorisation qui soit conforme tant du point de vue hiérarchique que de celui de la responsabilité. C'est-à-dire que, du côté des demandeurs, il faut notamment intégrer les responsables politiques (directeurs de la police) à la demande présentée en faveur du premier raccordement d'organes externes de protection de l'Etat de la Confédération, des cantons ou des villes et, en ce qui concerne l'autorité concédante, il faut déterminer une instance indépendante compétente en matière d'autorisation.

2. Les systèmes d'information décentralisés des cantons ou des villes dans le domaine de la protection de l'Etat doivent être rapidement remplacés en procédant à des raccordements en ligne à ISIS. Le cas échéant, les données mémorisées de manière décentralisée doivent être effacées.

3. En se basant sur l'article 16, 2e alinéa LMSI, le DFJP doit réviser le modèle de règlement d'exploitation par système TED afin de l'adapter aux nouvelles prescriptions de la LMSI.

4. A l'occasion de l'adaptation de l'ordonnance ISIS à la LMSI, le DFJP doit également réglementer les questions liées au financement et à la répartition des coûts entre la Confédération et les autres organes de protection de l'Etat (cantons et villes).

5. Le DFJP doit préciser le contenu de l'article 3, 2e alinéa, lettre d dans le sens des explications sous le point 338, lettre 8 ci-dessus.

34 RCE

341 Bases et principes légaux

Séjour et établissement des étrangers

a) Loi fédérale sur le séjour et l'établissement des étrangers du 26 mars 1931 (LSEE avec modification, état le 11 novembre 1997, RS 142.20),
b) Règlement de la loi fédérale sur le séjour et l'établissement des étrangers du 1er mars 1949 (RSEE avec modification, état le 1er octobre 1996 RS 142.201),
c) Ordonnance concernant l'entrée et la déclaration d'arrivée des étrangers (OEArr du 14 janvier 1998, état le 3 février 1998, RS 142.211),
d) Ordonnance concernant la déclaration du départ des étrangers du 20 janvier 1971 (avec modifications, état le 1er octobre 1996, RS 142.212),
e) Ordonnance sur le Registre central des étrangers du 23 novembre 1994 (ordonnance RCE avec modifications, état le 1er avril 1996, SR 142.215),
f) Autres ordonnances sans rapport direct avec la question des raccordements en ligne (RS 142.241, RS 142.281, RS 142.291, RS 143.5 et RS 823.21).

En résumé, ces bases légales permettent de déduire les principes suivants :

341.1 Loi fédérale sur le séjour et l'établissement des étrangers

A l'article 25 LSEE, dans le cadre des dispositions transitoires et finales, le législateur a accordé au Conseil fédéral les compétences d'édicter les prescriptions nécessaires à l'exécution de la LSEE. Il exerce la haute surveillance sur l'application des prescriptions fédérales relatives à la police des étrangers. Il est en particulier autorisé à régler

> La collaboration des autorités de police des étrangers avec d'autres autorités, notamment les offices de placement, ainsi que les attributions de l'Office fédéral du développement économique et de l'emploi (OFDE) dans ses relations avec les offices cantonaux de placement, en ce qui concerne le marché du travail.
> (Article 25, 1er alinéa, lettre d).

L'Office fédéral des étrangers (OFE) exerce, dans le domaine de la police des étrangers, toutes les fonctions non dévolues à une autre autorité fédérale (article 15, 3e alinéa LSEE).

Chaque canton désigne une autorité cantonale de police des étrangers (police cantonale des étrangers). Celle-ci exerce toutes les fonctions relatives à la police des étrangers qui ne sont pas dévolues à une autorité fédérale ou que la législation cantonale n'attribue pas à une autre autorité (article 15, 1er alinéa LSEE). Les cantons édictent les dispositions nécessaires à l'exécution de la présente loi sur leur territoire; ils désignent les autorités compétentes, dont ils fixent les droits et les obligations (article 25, 3e alinéa LSEE).

Il n'y a pas encore de base légale formelle régissant la réalisation et l'exploitation d'un système d'information automatisé relatif aux étrangers (Registre central des étrangers : RCE) ainsi que le raccordement d'unités administratives de la Confédération et des cantons à ce système.

Suite à un arrêté du Conseil fédéral sur la procédure d'asile du 20 juin 1997, la loi sur la protection des données du 19 juin 1992 a été modifiée à son article 38. En effet, l'alinéa 4 (nouveau) prévoit que : « Pour ce qui concerne le domaine de l'asile et des étrangers, le délai fixé au 3e alinéa est prorogé jusqu'à la date d'entrée en vigueur de la loi sur l'asile

totalement révisée ainsi que de la modification de la loi fédérale sur le séjour et l'établissement des étrangers. »

341.2 Ordonnance sur le Registre central des étrangers (ordonnance RCE)

L'Office fédéral des étrangers (OFE) tient en collaboration avec les services fédéraux intéressés et les cantons, un registre automatisé des étrangers (Registre central des étrangers; RCE) (article 1er ordonnance RCE). Le RCE a pour but de rationaliser le travail des autorités de police des étrangers, d'effectuer les contrôles prescrits par la législation sur les étrangers, de tenir la statistique sur les étrangers et, dans des cas particuliers, de faciliter l'entraide administrative (article 2 ordonnance RCE). L'office fédéral recueille les données personnelles sur les étrangers nécessaires à l'exécution des tâches prescrites par la législation ou les fait recueillir par diverses autres autorités (article 3, 1er alinéa ordonnance RCE), soit :

- Les cantons et les communes (article 4)
- L'Office fédéral de la police (article 5, 1er alinéa, lettre a)
- L'Office fédéral des réfugiés (article 5, 1eralinéa, lettre b)
- L'Office fédéral du développement économique et de l'emploi (article 5, 1er alinéa, lettre c)
- L'Office fédéral de la statistique (article 5, 1er alinéa, lettre d)
- Les représentations suisses à l'étranger (article 5, 1er alinéa, lettre e)
- Les postes-frontière (article 5, 1er alinéa, lettre f)

Les données personnelles peuvent être annoncées aux stations de données reliées à l'ordinateur central (*on-line*), par lots sur des supports de données électroniques ou par écrit au moyen de formulaires d'annonce de données (article 6 ordonnance RCE). L'office fédéral détermine les conditions dans lesquelles les données personnelles peuvent être communiquées par voie informatique et dans ce cas de quelle manière elles doivent être vérifiées avant leur transmission (tests de plausibilité). L'office fédéral édicte des directives relatives à la communication des données personnelles (article 6, 2e et 3e alinéas ordonnance RCE).

341.3 L'OFE est autorisé à communiquer les données personnelles par procédure d'appel (article 7 ordonnance RCE) aux autorités suivantes :

Autorité	***Domaine des données pouvant être consultées***
Autorités cantonales et communales de police des étrangers	tout le domaine relevant de leurs compétences
Service de recours du DFJP	instruction des recours
Office fédéral du développement économique et de l'emploi et autorités cantonales et communales du marché du travail	accomplissement des tâches en application de l'ordonnance limitant le nombre des étrangers
Postes-frontière	contrôle des personnes à la frontière et octroi de visas exceptionnels

Représentations suisses à l'étranger	examen des demandes de visas
Centrale de compensation de l'AVS	constitution du numéro AVS
Caisse suisse de compensation	instruction des demandes présentées par des ressortissants étrangers qui ont quitté la Suisse calcul des prestations auxquelles ils ont droit
Office fédéral des réfugiés	tâches au sens de la loi sur l'asile et de la LSEE
Autorités cantonales et communales de police	tâches de contrôle en matière de police des étrangers identification des personnes lors des enquêtes de la police de la sûreté et de la police criminelle
Office fédéral de la statistique	recensement de la population tâches découlant de la loi fédérale sur la statistique fédérale
Ministère public de la Confédération 1. Service des étrangers 2. Police fédérale	 enquêtes de la police politique (interdictions d'entrée et expulsions pour sauvegarder la sécurité intérieure et extérieure de la Suisse) identification des personnes lors d'enquêtes de la police de sûreté et de la police criminelle
Office fédéral de la police 1. Section de la nationalité 2. Bureau central suisse de police 3. Division principale de l'entraide judiciaire et de l'assistance administrative internationale	 tâches prescrites par la loi sur la nationalité identification des personnes dans le cadre de tâches relatives à l'échange intercantonal et international d'informations policières (Services centraux et Interpol) identification des personnes lors de procédures d'extradition entraide judiciaire et assistance administrative poursuite pénale et exécution des peines contrôle des requêtes du RIPOL

341.4 Communication des données personnelles par les cantons et les communes (article 13 ordonnance RCE)

Les autorités ci-dessus ne peuvent communiquer des données personnelles recueillies ou utilisées en application de la LSEE à d'autres autorités qu'à la condition que le secret de fonction et les prescriptions cantonales et communales sur la protection des données le permettent et que l'étranger ne soit pas lésé dans ses intérêts personnels dignes de protection.

341.5 Sécurité des données (article 16 ordonnance RCE)

Toutes les autorités qui collaborant avec le RCE prennent, chacune dans son secteur, les mesures organisationnelles et techniques propres à assurer la sécurité des données. L'office fédéral émet des prescriptions en matière de sécurité des données et se charge de la coordination en conformité avec les recommandations de l'Office fédéral de l'informatique. Les données personnelles, les programmes et la documentation relative à ces programmes doivent être protégés afin d'empêcher que des personnes non autorisées y aient accès, ou qu'ils soient volés ou indûment modifiés ou détruits.

342 Situation actuelle en matière de liaisons en ligne

Nombre d'utilisateurs

Selon la liste chronologique des liaisons en ligne avec le RCE du 27 janvier et dont l'actualité a été confirmée lors de l'audition des représentants de l'Office fédéral des étrangers du 3 février 1998,

ont été reliés au RCE depuis septembre 1988 jusqu'à aujourd'hui.

En outre, plus de 10'000 utilisateurs sont raccordés au RCE via leur raccordement au RIPOL (accès limité au RCE, voir le point 316 ci-dessus).

Catégories d'utilisateurs

La légitimité de tous les utilisateurs raccordés découle de l'ordonnance RCE (article 1er, article 7, 1er et 2e alinéas ordonnance RCE). Toutefois, aucun motif juridique n'est indiqué pour les 26 raccordements du Centre de calcul du DFJP. Ces raccordements ne découlent ni de la LSEE, ni du RSEE, ni de l'ordonnance RCE. Ils ont simplement été mis service pour l'entretien, l'exploitation et la maintenance de l'application RCE. D'ailleurs le CC DFJP ne figure pas parmi les unités administratives ayant le droit d'accéder au système énumérées à l'annexe 1 (catalogue de données).

Du point de vue de la structure des utilisateurs, ils est frappant de constater qu'en plus des services de la Confédération et des services cantonaux (police des étrangers), divers services des habitants de villes (Berne, Bienne, Coire, Saint-Gall, Thoune, Winterthur, Zurich) et de communes (St. Moritz, Arosa, poste de police d'Engelberg, office du travail de la ville de Zurich, office du travail de la ville de Winterthur, Chavannes-près-Renens, bureaux régionaux des étrangers de Bellinzone, Mendrisio, Faido, Gordola, Chiasso, Biasca, Locarno, Magadino, Taverne, Lugano, Cevio, Caslano, les préfectures de Romont, Morat, Estavayer-le-Lac, Tafers, Châtel-St-Denis, Bulle, ainsi que les contrôles des habitants d'Adliswil, d'Uster et d'Yverdon) y sont également raccordés. Parmi les utilisateurs raccordés au RCE, les communes fribourgeoises et tessinoises sont bien représentées. Des raccordements en ligne supplémentaires pour divers contrôles des habitants (Emmenbrücke, Kriens, Fällanden, Köniz, Le Locle, Wettingen) n'ont pas encore été réalisés. Actuellement, 70 communes ou villes sont reliées au RCE (voir le document de l'OFE intitulé « *Rücklauf der Umfrage Mutationsmeldungen* » du 27 janvier 1998).

Réseau et mesures de sécurité
Au sein de l'administration, les données transitent sur les réseaux du département ou de la Confédération. Elles sont en grande partie chiffrées au moyen de logiciels *end-to-end*. Par le truchement du WAN-DFJP, les raccordements des cantons relient le Centre de calcul du DFJP aux dispositifs centraux de commutation (nœuds centraux) sis dans les chefs-lieux cantonaux. Les données sont chiffrées par des moyens matériels (*Gretacoder* ou autres). Sur les réseaux cantonaux, les données sont à nouveau chiffrées au moyen de logiciels *end-to-end*.

343 Procédure de raccordement

Avec l'article 6 de l'ordonnance RCE, le Conseil fédéral établit qu'il appartient à l'office fédéral (OFE) de déterminer les conditions dans lesquelles les données personnelles peuvent être communiquées par voie informatique et, dans ce cas, de quelle manière elles doivent être vérifiées avant leur transmission (tests de plausibilité). L'OFE doit édicter des directives relatives à la communication des données personnelles par les instances fédérales, les cantons et les communes ainsi que par les représentations suisses à l'étranger. Il doit approuver les formulaires d'annonce de données (article 6, 2e et 3e alinéas ordonnance RCE).

Le règlement de traitement de l'OFE du 16 novembre 1995 règle les détails dans le cadre du traitement des données dans le RCE. Toutefois, ce règlement ne contient pas de description explicite de la procédure d'autorisation en matière de nouveaux accès ou d'extension d'accès existants au RCE. Il est cependant possible de déduire certains principes en partant de l'organisation de projet RCE, de la description des tâches, des dispositions en matière de contrôle et de droits d'accès ainsi que des exigences en matière de sécurité.

343.1 Organisation structurelle

L'organisation structurelle du projet RCE est la suivante :

La commission de projet RCE
- dirige, planifie, coordonne et surveille le déroulement du projet,
- assure la communication des informations sur l'état du projet RCE à la direction de l'OFE,
- définit les priorités en tenant compte des exigences des utilisateurs et des ressources disponibles et
- examine les nouvelles exigences du point de vue de la protection des données et des prescriptions en matière de sécurité des données.

Commission de projet RCE

- Chef de projet utilisateurs (présidence)
- Chef de projet informatique
- Chef informatique DFJP
- Chef du Développement de systèmes CC DFJP
- Représentant Division centre d'exploitation OFI
- Représentant du groupement des chefs de police des étrangers
- Conseiller à la protection des données et conseiller à la sécurité des données OFE
- Chef suppléant registre central des étrangers OFE

Le groupe de projet RCE-3
- examine et assure les conditions de protection et de sécurité des données,
- élabore les spécifications de détail,
- planifie l'engagement des ressources,
- élabore les bases décisionnelles à l'attention de la commission RCE et
- qualifie les résultats.

Groupe de projet RCE-3

- Chef de projet informatique (présidence)
- Chef de projet utilisateurs
- Suppléant du chef de projet utilisateurs
- Représentants des utilisateurs externes par genre d'utilisateurs (représentants des PE, des communes, des offices du travail, des postes-frontière)
- Conseiller à la protection des données et conseiller à la sécurité des données OFE

Le groupe de travail *Annonces*

- ***examine les demandes et octroie les autorisations d'accès,***
- optimise les systèmes d'annonces et de mutation (du point de vue organisationnel et technique),
- est responsable de la planification de l'introduction.

Groupe de travail système d'annonces

- Chef de projet utilisateurs
- Chef de projet informatique
- Chef suppléant registre des étrangers OFE
- Représentants des services de PE cantonaux et communaux
- Représentant de l'association des chefs de contrôle des habitants et de police des étrangers
- Représentant du CC DFJP Techniques de systèmes et exploitation IT
- Télématique et engineering

Le groupe de travail II / RCE-3

- formule des demandes de modifications et d'exigences du point de vue des utilisateurs,
- fixe les priorités en matière d'exigences des utilisateurs et
- examine les résultats atteints par les développeurs du système en la matière.

Groupe de travail II / RCE-3

- Chef de la section Ressources (présidence)
- Chef de projet utilisateurs
- Chef de projet informatique
- Chef informatique DFJP
- Représentants des services de PE cantonaux et communaux
- Représentant de l'association des chefs de contrôle des habitants et de police des étrangers
- Représentant du CC DFJP, Techniques de systèmes et exploitation IT
- Télématique et engineering
- Représentants OFE (conseiller à la protection des données de l'OFE, division entrée et séjour, section RCE
- Représentant de l'ODR

343.2 Organisation procédurale

L'authentification de l'installation technique et l'identification des utilisateurs s'effectue dans le système général de gestion des utilisateurs du CC DFJP qui fonctionne sur l'ordinateur principal (*host*) TANDEM. Ce n'est qu'ensuite qu'il est possible d'accéder au masque de base du RCE (chiffre 2.5 du règlement de traitement RCE[1]). Le profil d'accès du catalogue de données définit les droits d'accès des diverses unités organisationnelles aux champs de données. Les niveaux d'accès fixent le genre d'accès : uniquement droit de consulter ou droit de consulter et de procéder à des mutations. De plus, les droits de consultation et ceux de mutation peuvent être limités à certaines catégories de personnes. Le profil d'accès de

1 *Bearbeitungsreglement für das zentrale Ausländerregister (ZAR), n'existe qu'en version allemande.*

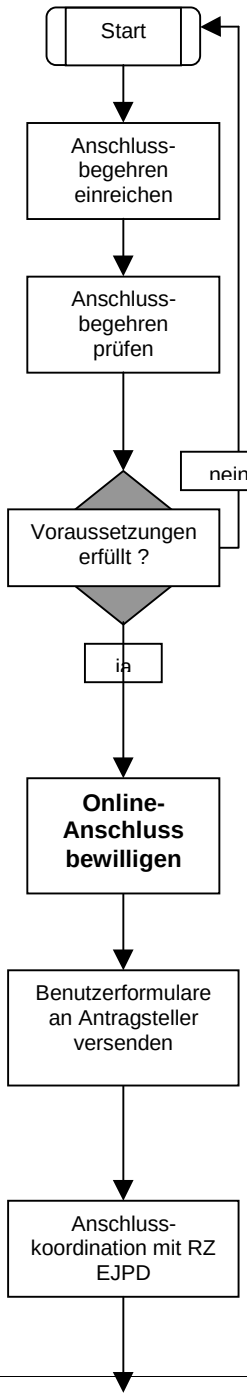
chaque utilisateur du système est limité par son appartenance à une unité organisationnelle. Chaque unité organisationnelle ne reçoit que les droits d'accès qui sont indispensables à l'exécution de ses tâches légales. Au sein de chaque unité organisationnelle, le profil d'accès de chaque collaborateur est défini en fonction des tâches que ce dernier doit assumer. La remise des droits d'accès, qui, en complément au catalogue des données en annexe à l'ordonnance RCE, est défini à l'annexe 3 du règlement de traitement, dans le tableau des accès en ligne par fonction et par utilisateur, est assurée par la section RCE de l'OFE. La section RCE peut également déléguer la remise des droits d'accès aux agents de liaison du RCE qui sont intégrés aux unités organisationnelles (chiffre 2.6 du règlement de traitement RCE). En tant que responsable des données, c'est fondamentalement l'OFE qui est responsable du respect des dispositions en matière de protection des données. La responsabilité en matière de protection des données du CC DFJP et des services raccordés au RCE demeure cependant réservée dans leur domaine d'activité (chiffre 1.3 règlement de traitement RCE). Au sein de l'OFE, c'est l'informaticien de l'office qui, en tant que chef de projet utilisateurs, est responsable du RCE (chiffre 1.3 du règlement de traitement RCE). Le conseiller à la protection des données de l'OFE doit être informé de toutes les modifications et projets de développement du RCE ; à cette occasion, il rend les personnes impliquées attentives aux exigences en matière de protection des données (chiffre 1.4 règlement de traitement du RCE.). Il répond aux questions relatives à la loi sur la protection des données dans le cadre de l'utilisation du RCE et contrôle régulièrement que les remises des droits d'accès sont bien conformes aux dispositions de l'ordonnance (voir également les directives relatives à l'octroi de conseils en matière de protection des données au DFJP). Les décisions de principe sont prises par la direction de l'office. Selon le chiffre 6 des directives provisoires relatives à la journalisation des communications de données du registre central des étrangers effectuées à l'aide d'une procédure d'appel du 2 novembre 1994, le conseiller à la protection des données de l'OFE doit présenter au Secrétaire général du DFJP un rapport annuel sur les contrôles qu'il a effectués.

L'audition du responsable du RCE du 3 février 1998 a permis à ce dernier de décrire la procédure de mise en place d'un **nouvel** accès en ligne. Les unités organisationnelles intéressées à un raccordement (administration fédérale, cantonale ou communale) doivent présenter une demande d'accès écrite à la section RCE de l'OFE. Le groupe de travail restreint *Annonces* (CC DFJP / OFE) planifie les raccordements et examine les unités organisationnelles intéressées du service concerné du point de vue des restrictions en matière de protection des données. Cette demande est examinée en suivant les instruction d'une liste de contrôle (check-list, document « raccordementrce.doc »). C'est la direction qui prend la décision pour les demandes de nouveaux accès ou celles qui sont politiquement délicates voir listes de contrôle RCE-3 – nouveaux raccordements au RCE-3 du 18 février 1998). Toutes les autres décisions sont prises par la personne de contact de l'OFE (chef RCE). Dans ses explications complémentaires du 20 mai 1998, l'OFE range les raccordements à l'étranger et les raccordements d'autorités de police dans la catégorie des demandes politiquement délicates (qui ressortissent donc à la compétence décisionnelle du directeur). Le conseiller à la protection des données de l'OFE, le cas échéant le Préposé à la protection des données, prend position au sujet des demandes d'accès. En cas de décision positive, la section RCE (Division Projets informatiques) fait parvenir les formulaires nécessaires au demandeur (formulaires de l'OFE : « Demande de raccordement », « Questionnaire relatif au profil des services raccordés », « Gestion des utilisateurs », « Mutation de l'effectif », « Gestion des profils d'accès » et « Signature »). Une fois les formulaires complétés et rentrés, la Division Projets informatiques de la section RCE de l'OFE prend contact avec le CC DFJP afin de fixer le délai de raccordement. Ensuite, la Division Formation et soutien aux utilisateurs de la section RCE de l'OFE informe le demandeur au sujet du délai de raccordement, de la formation et de la mise en service. L'infrastructure du système est recensée et les profils des utilisateurs sont transmis au responsable de la formation sous pli cacheté. Après quoi, la procédure de test avec les nouveaux profils des services raccordés et les numéros d'utilisateurs pour les tests est

exécutée et les personnes concernées sont convoquées pour la formation. Aucun droit d'accès en ligne n'est libéré tant que la formation appropriée des utilisateurs ayant obtenu un droit d'accès n'est pas terminée. A la fin de sa formation, le nouvel utilisateur reçoit une enveloppe cachetée contenant son numéro d'identification et son mot de passe personnel. Durant la période de démarrage, la section RCE de l'OFE (Formation et soutien aux utilisateurs) surveille l'exploitation en phase de production.

Selon les directives provisoires relatives à la journalisation des communications de données du registre central des étrangers effectuées à l'aide d'une procédure d'appel du 2 novembre 1994, le conseiller à la protection des données de l'OFE doit contrôler le fichier d'enregistrement journalier au CC DFJP une fois par mois (chiffre 2.8 règlement de traitement RCE). En outre, le Secrétaire général du DFJP doit présenter un rapport annuel de ses contrôles relatifs au RCE (chiffre 6 des directives). En tenant compte des réponses fournies par l'OFE le 20 mai 1998 à la suite des questions complémentaires de l'expert, il appert qu'avec l'introduction d'un enregistrement journalier des accès au RCE ainsi que d'une nouvelle procédure de contrôle, le conseiller à la protection des données dispose depuis le 1er janvier 1998 d'un accès direct aux fichiers d'enregistrements journaliers. Les directives du 2 novembre 1994 sont encore en vigueur. Elles devront cependant également être adaptées à cette nouvelle procédure. Le contrôle est effectué selon le manuel de l'utilisateur du CC DFJP, par sondages réguliers, en cas de soupçons ou sur demande particulière. De tels contrôles ne donnent pas lieu à la rédaction d'un rapport. Il semblerait toutefois qu'une lettre standard ait été élaborée et que le conseiller à la protection des données de l'OFE l'enverrait aux services contrôlés lorsque les résultats du contrôle impliquent la prise de mesures. Alors qu'un rapport annuel écrit avait été remis au Secrétariat général du DFJP en 1996, en 1997, le Préposé à protection des données du DFJP n'a été informé qu'au moyen de divers rapports oraux.

Bundesamt für Ausländerfragen	Bewilligungsverfahren für Online-Anbindung ZAR	Prozess 0xx

Input	Ablauf	Beschreibung und Hilfsmittel	Verant-wortung	Output
Verwaltungs-internes Anschluss-gesuch Verwaltungs-externes Anschluss-gesuch (Kantone, Gemeinden etc.)		Jede (bundesverwaltungsinterne oder bundesverwaltungsexterne) Organisations-einheit, die Anschluss an ZAR wünscht, stellt ein schriftliches Gesuch mit kurzer Begründung an die Sektion ZAR des BFA. Die Arbeitsgruppe Meldewesen ZAR prüft, ob alle rechtlichen und tatsächlichen Voraussetzungen für einen Online-Anschluss gegeben sind. **Checkliste x00.** **(ZAR3-Neuanschluss)** **Checkliste X00.001b** **(raccordementrce.doc)** Der Datenschutzberater BFA (allenfalls der Eidg. Datenschutzbeauftragte) nehmen Stellung zum Gesuch Die Arbeitsgruppe Meldewesen ZAR fällt eine Entscheidung und • informiert die Direktion BFA • holt einen Bewillilgungsentscheid der Direktion BFA ein, wenn ein Neuanschluss oder ein politisch heikler Erweiterungsanschluss zu entscheiden sind. **Checkliste x00.002** **(Entscheidzuständigkeit Direktion BFA).** Sektion ZAR versendet die Benutzerformulare an Gesuchsteller. **Formular 1:** Anschlussbegehren **Formular 2:** Fragebogen Amtsstellenprofil **Formular 3:** Benutzerverwaltung **Formular 4:** Bestandesmutationen **Formular 5:** Zugriffsprofilverwaltung **Formular 6:** Unterschrift Sektion ZAR koordiniert die Anschlussarbeiten mit dem RZ EJPD.	Gesuchsteller für Online-Anschluss Arbeitsgruppe Meldewesen ZAR des BFA Datenschutz-berater BFA Eidg. Daten-schutzbeauf-tragter Arbeitsgruppe Meldewesen ZAR Direktion BFA Sektion ZAR Abteilung EDV-Projekte Sektion ZAR Abteilung EDV-Projekte RZ EJPD	Anschluss-begehren Vorprüfung Anschluss-voraussetzung Stellungnahme Anschluss-entscheid Anschluss-entscheid Anschlussplan Aktivitätenplan Terminplan Ressourcenplan
Anmelde-begründung Gesuchsteller				

Anschlussplan Aktivitätenplan Terminplan Ressourcen-plan	Mitteilung an Gesuchsteller	Sektion ZAR orientiert den Gesuchsteller über Anschlusstermin, Schulung und Produktionsaufnahme	Sektion ZAR Abteilung pro-jektbezogene Ausbildung und Beratung	Anschlussplan
	Informationssystem ZAR bereitstellen und parametrisieren	Die Systeminfrastruktur, die Benutzerprofile sowie die notwendigen Zugriffs-berechtigungen werden durch die Sektion ZAR erfasst. Das RZ EJPD erstellt die Systembetriebsbereitschaft und schliesst den Gesuchsteller über die Kommunikationsinfrastruktur an ZAR an.	Sektion ZAR RZ EJPD	Zugriffsrechte, Amtsstellenprofil Organisations-struktur, Datenkommuni-kation und Verschlüsselung
	Systemtests durchführen	Sektion ZAR und RZ EJPD koordinieren und führen die vorbereitenden Systemtests mit dem neuen Amtsstellenprofil und den Test-User-Nummern durch. Die definitive Betriebsbereitschaft wird erstellt.	Sektion ZAR RZ EJPD	Testprotokolle Betriebsbereit-schaft
	Benutzerschulung durchführen	Sektion ZAR führt mit den Benutzern der neu angeschlossenen Organisations-einheit die obligatorische Benutzer-schulung durch.	Sektion ZAR Abteilung pro-jektbezogene Ausbildung und Beratung	Benutzer-schulung und –einführung
	Benutzerkennzahl und Passwort übergeben	Uebergabe der Benutzerkennzahl und des persönlichen Passwortes an jeden neuen ZAR-Benutzer in verschlossenem Couvert an der Benutzerschulung.		Benutzer-kennzahl Benutzer-passwort
	Aufnahme Produktivbetrieb	Die neu angeschlossene Organisationseinheit nimmt nach Abschluss der Schulung den Produktivbetrieb auf.	Neue Organisations-einheit	Produktivbetrieb
	Ende			
Version 1.0	**Was** Prozesserstellung	**Wann erstellt** **Von wem** 13.4.1998 FI	**Geprüft** 20.4.1998 xy	**Freigabe** 30.4.1998 zz

Tableau : Description possible de la procédure sur la base des opérations connues effectuées en vue d'une mise en place d'un accès en ligne au RCE.

La version adaptée et actualisée par l'OFE à l'occasion de sa prise de position dans le cadre de la procédure de consultation interne se trouve dans le document « Supplément 1, Evaluation et résumé de la procédure de consultation interne » du 30 juillet 1998.

344 Exploitation et maintenance

Le RCE-3 est géré en tant que projet. Les organes responsables du projet font l'objet du point 343.1 (Organisation structurelle) ci-dessus. Les adaptations et les développements en cours sont regroupés et harmonisés par le groupe de projet RCE-3 et le groupe de travail II / RCE-3. Le Centre de calcul du DFJP est responsable de la maintenance et de l'exploitation du calculateur central ainsi que de l'infrastructure de communication. Les unités cantonales compétentes sont responsables des calculateurs nodaux (de commutation) et de l'infrastructure de redistribution sur leur territoire. Les unités organisationnelles utilisatrices se chargent du respect des mesures organisationnelles et techniques de sécurité.

Lors de l'audition du responsable du RCE qui a eu lieu le 3 février 1998, il est clairement ressorti que le manque de bases légales et de compétences organisationnelles fait qu'il est difficile d'imposer aux autorités cantonales et communales qu'elles prennent des mesures organisationnelles et techniques de protection et de sécurité des données. Il n'y a pas de bases légales instituant une obligation d'inspection des utilisateurs externes à l'administration fédérale afin de contrôler s'ils respectent les mesures de protection et de sécurité. L'OFE procède donc par « visites de courtoisie » auprès des utilisateurs du RCE. Il ne peut influencer le respect de ces principes que par le biais de discussions informelles et en sensibilisant les utilisateurs au sujet de leur responsabilité.

Dans son rapport des 22 décembre 1997 et 9 février 1998 (Rapport CCF), le Service de contrôle administratif du Conseil fédéral parvient à des conclusions semblables. Des incidents ont mis en évidence que la protection des données personnelles à contenu sensible n'est pas toujours assurée, car les droits d'accès des utilisateurs périphériques sont insuffisamment réglés (Rapport CCF, chapitre 41, chiffre 12, page 37).

345 Participation aux coûts

Les cantons participants et les autres autorités raccordées au système RCE prennent en charge les frais d'acquisition et d'exploitation de leurs appareils. La Confédération finance l'installation et l'utilisation des lignes jusqu'à un raccord central de commutation (distributeur principal) au chef-lieu du canton. Les cantons prennent en charge les frais d'installation et d'exploitation des lignes secondaires nécessaires sur leur territoire. Les stations de données prévues pour un usage externe à la Confédération doivent répondre aux prescriptions techniques des installations informatiques de la Confédération. Le département fixe les détails (article 21, 1er et 2e alinéas ordonnance RCE).

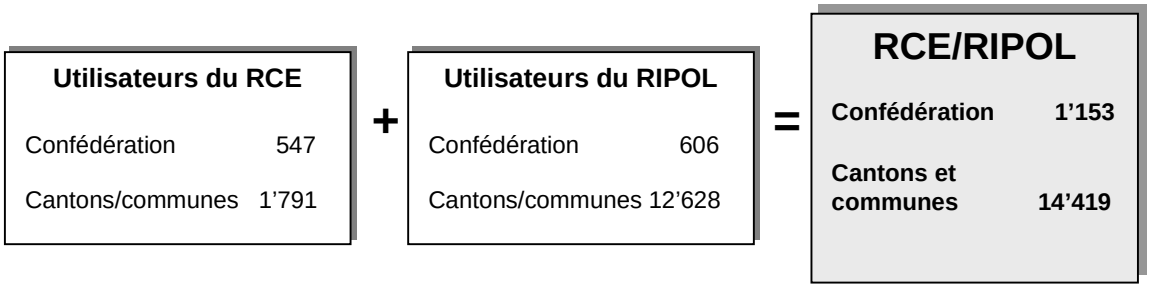
346 Cantons et autres accès externes à l'administration fédérale

Les 2'338 utilisateurs internes (Confédération) et externes (cantons/communes) raccordés au système d'information du RCE sont répartis de la manière suivante : 547 utilisateurs (23.4 pour cent) sont au service de la Confédération ou de la Principauté du Liechtenstein (Landesverwaltung Fremdenpolizei / Passamt Liechtenstein) et 1'791 utilisateurs sont des collaborateurs des unités administratives cantonales ou communales (76.6 pour cent).

Utilisateurs du RCE		
EXTERNES à l'administration fédérale	**76.6% =**	**1'791 utilisateurs**
INTERNES à l'administration fédérale	**23.4% =**	**547 utilisateurs**

Cependant, le nombre de ces raccordements doit être revu à la hausse étant donné que le système de recherches informatisées RIPOL permet à ses utilisateurs d'accéder au RCE. Selon les explications du responsable OFE du RCE fournies lors de l'audition du 3 février 1998, les utilisateurs du RIPOL, en particulier les autorités de police, peuvent accéder de manière limitée au RCE-3 directement depuis le RIPOL.

La présentation sous le point 316 ci-dessus (système de recherches informatisées RIPOL) recense 12'628 utilisateurs externes à l'administration fédérale (cantons et communes, soit le 95.4 pour cent de tous les utilisateurs) raccordés au RIPOL. En outre, 24 représentations suisses à l'étranger et 30 services d'Interpol sont également raccordés au RIPOL.



Le traitement préalable des données du RCE est effectué au moyen de masques de saisie du RIPOL séparés. La consultation des données est limitée à celles qui sont directement liées au droit des étrangers (étrangers – statut activé, décisions d'entrée, refoulements à la frontière). Selon les indications fournies par l'OFE, ceci vaut pour l'Office fédéral des réfugiés, les autorités de police des villes, les postes-frontière, le service des recours du DFJP, le CC DFJP, l'Office fédéral de la police, les services de police cantonaux, le Ministère public de la Confédération, les autorités de police des communes, l'Office fédéral des étrangers. Ainsi, avec la liaison du RIPOL au RCE, près de 15'000 utilisateurs peuvent avoir accès au RCE. Depuis le 1er septembre 1997, sur la base d'une décision de la Commission fédérale de la protection des données du 27 juin 1997, tous les accès au RCE / RCE-RIPOL doivent être enregistrés dans un journal. Un numéro d'identification personnel assorti d'un mot de passe donne accès au RCE (le système oblige les utilisateurs de modifier ce mot de passe tous les deux mois). L'entrée dans le système est enregistrée. Lors du traitement de données du RCE, la date et l'heure de la dernière mutation ainsi que l'utilisateur qui en est responsable (ID de l'utilisateur) sont enregistrés (règlement de traitement du RCE du 16 novembre 1995, chiffre 2.5).

347 Perspectives de développement

Le 28 août 1997, l'OFE a procédé à une consultation interne au sujet de la révision de l'ordonnance RCE. Cette révision est devenue nécessaire à cause de la mise en service planifiée des deux nouveaux sous-systèmes EVA (***E**lektronische **V**isum**A**usstellung* soit établissement de visas par des moyens informatiques) et EPOS (***E**lektronisches **P**ersonenregistratur **O**nline **S**ystem* soit enregistrement des personnes par des moyens informatiques). Ces deux sous-systèmes sont des applications du RCE, ce qui permet de les réglementer dans le cadre de l'ordonnance RCE. L'objet d'EVA (*Elektronische VisumAusstellung*) est de réaliser un système d'information permettant de saisir les demandes de visas et d'établir ces derniers électroniquement (voir rapport de concept, résumé pour la gestion, page 5). Il prévoit de raccorder en ligne les représentations suisses à l'étranger. Les liaisons du calculateur du CC DFJP avec les représentations suisses à l'étranger seront établies à partir d'un calculateur de commutation situé au CC DFJP. Les autres services autorisés à émettre des visas, c'est-à-dire les postes-frontière, les autorités de police des étrangers des cantons, l'Office fédéral des étrangers et l'Office fédéral des réfugiés sont directement raccordés au calculateur du CC DFJP. La principale innovation découlant de ces logiciels est de permettre à l'Office fédéral des affaires économiques extérieures, à l'Office fédéral de la police et au Ministère public de la Confédération de pouvoir consulter les données relatives aux demandes de visas par voie électronique. Selon les explications accompagnant le projet de révision, il ne s'agit pas d'un accès en ligne puisque les données ne sont communiquées que de cas en cas (transmission des visas, voir rapport de concept, page 32, chiffre 4.1.1.5). En outre, il est prévu de saisir les rapports de contrôle aux frontières dans le RCE afin que les autorités compétentes puissent y accéder en ligne. Ceci implique une extension du catalogue de données du RCE qui comprendra de nouveaux champs de données. Il a également été prévu d'y raccorder la Commission suisse de recours en matière d'asile (encaissement des frais de procédure). De plus, il faut charger l'OFE d'édicter les mesures techniques et organisationnelles permettant de prévenir tout

traitement non autorisé des données et de procéder à la journalisation automatique des accès (nouvel article 17, 2e alinéa ordonnance RCE).

Dès avril 1999, l'OFE ainsi que les autorités de police des étrangers du canton de Berne, la police de l'aéroport de Zurich, le poste-frontière de Basel-Weil et les représentations suisses de Londres et de Moscou participeront à un essai d'exploitation pilote de la nouvelle application EVA.

En réponse aux questions complémentaires de l'expert du 14 avril 1998, l'OFE a, par lettre du 20 mai 1998, fourni un certain nombre de compléments relatifs aux perspectives de développement du RCE. La poursuite du développement du RCE a été bloquée par le Secrétariat général du DFJP (lettre du 3 décembre 1997) étant donné que les projets de développement du RCE et l'évaluation du RCE devaient être coordonnés et réalisés dans le cadre d'un nouveau projet « *Ausländer 2000* ». L'OFE, notamment par lettre du 4 février 1998, a bien essayé de faire revenir le Secrétariat général sur sa décision. En résumé, l'OFE a développé les arguments suivants :

- Nécessité objective en rapport avec une limitation des profils de mutation (autorités cantonales de police des étrangers et Police fédérale) impérative pour des raisons de sécurité et de protection des données.
- Elimination des redondances (saisies à double, transferts en temps réel, Grenzkontrollrapporte, interfaces électroniques avec autorités communales de police des étrangers => introduction de boîtes aux lettres électroniques).
- Adaptation urgente de statistiques dans le domaine des interdictions d'entrée en Suisse.
- Rationalisation des procédures de travail (notamment dans le domaine du traitement des données concernant les membres de la famille ainsi qu'en matière de décisions cantonales d'expulsion).
- Situation pas satisfaisante du fait que l'Office fédéral de la statistique est mieux à même (moyens techniques plus modernes) que l'OFE (normalement compétent en la matière) de traiter les données sur les étrangers (transmises par l'OFE) et de fournir des renseignements plus précis et plus complets.
- Les procédures de traitement actuelles (approvisionnement, enregistrement et distribution des informations) sont obsolètes ; certains logiciels exploités datent du début des années 70, les procédures sont trop compliquées et les coûts liés à l'exploitation et à la maintenance sont proportionnellement trop élevés.
- Selon les directives du chef du DFJP xx registermässig erfasste Namensschreibweise nach Zivilstandsrecht doit être garanti/e d'ici à fin 2000.
- La réalisation du projet AVOR permettra de réaliser des recettes annuelles de près de 2 millions de francs, ce qui, à moyen terme, permettra de couvrir largement les coûts de l'investissement.

Une révision partielle de l'ordonnance RCE est prévue pour le milieu de l'automne 1998. Cette révision permettra de créer les bases légales pour les systèmes complémentaires EVA, EPOS et AVOR. A cette occasion également, des dispositions liées à la révision partielle de la LSEE seront intégrées à l'ordonnance, notamment dans le domaine de la protection des données.

Il a été prévu de réaliser les deux systèmes complémentaires EVA et EPOS durant le 1er trimestre 1999. A ce jour, il n'y a aucun rapport entre ces développements (réalisation de ces systèmes complémentaires EVA et EPOS) et le système. Il n'y a d'ailleurs aucun plan quant à la réalisation du système « *Ausländer 2000* ». Le Secrétariat général du DFJP a prévu une discussion générale à ce sujet.

348 Résumé et appréciation

1. La procédure d'autorisation de raccordement en ligne n'est réglée que par le règlement de traitement de l'OFE, et ceci de manière rudimentaire. Pour le RCE comme pour les autres systèmes d'information dans le domaine de la police, les principes régissant les raccordements en ligne mis en place par les dispositions de droit supérieur (loi, ordonnance) menacent de se perdre au fur et à mesure de la délégation des responsabilités vers le bas. En effet, une telle délégation de compétences à des unités opérationnelles peut conduire à ce que les pondérations, les interpolations et la défense d'intérêts des utilisateurs supplante la volonté initiale du législateur. De plus, le manque d'indépendance de l'instance compétente en matière d'autorisation peut provoquer des conflits d'intérêts (utilisateur du système, responsable du contenu des banques de données et instance d'autorisation en même temps). Il serait judicieux que les critères décisionnels importants en matière d'autorisation de raccordement en ligne, la procédure et les compétences soient concentrés et fixés de manière harmonisée par une unité administrative hiérarchiquement adéquate. Il faut également accorder une plus grande importance au principe d'indépendance de l'instance compétente en matière d'autorisation.

2. La procédure d'autorisation des accès en ligne gagnerait en compréhension et en clarté si les processus d'autorisation étaient décrits sous forme de tableau tel celui présenté au point 343.2 ci-dessus. Dans ce domaine complexe, les tâches, les compétences et les responsabilités ne peuvent être fixées clairement et imposées que si les procédures sont expliquées de manière compréhensible au moyen de descriptions textuelles et synoptiques. Une telle présentation aurait l'avantage de régler de nombreux points en suspens et de répondre à de nombreuses questions, tant au sein de l'administration que vis-à-vis du public.

3. L'OFE édicte des directives en matière de sécurité à l'attention des organismes utilisateurs. Par manque de bases légales et à défaut de compétences en la matière, l'OFE – qui est responsable des données – ne parvient pas à les faire respecter par les unités organisationnelles cantonales et communales. Il n'y a pas de bases légales qui permettent au responsable des données d'effectuer des inspections de sécurité auprès de ces unités organisationnelles utilisatrices du système. Du point de vue de la sécurité, cette situation augmente les risques d'exploitation relatifs au système informatisé du RCE. Dans ces conditions, il ne faut recourir qu'avec parcimonie à la possibilité d'accorder des droits d'accès aux agents de liaison des unités organisationnelles cantonales ou communales (chiffre 2.6 du règlement de traitement RCE). Il serait possible de réglementer les compétences en matière de contrôle au niveau de la loi. Ainsi, par exemple, dans la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC) du 7 octobre 1994, le législateur a prévu la collaboration entre autorités fédérales et cantonales (article 12 LOC). En outre, dans les dispositions finales, il a chargé le Conseil fédéral de régler les modalités de traitement des données par les offices centraux ainsi que la coordination des systèmes, le droit d'accès dont bénéficient les services fédéraux et cantonaux, et les limites de cet accès ainsi que la durée de l'archivage des données, *le contrôle et les modalités de la protection des données* (article 15 LOC).

4. Les demandes d'accès au RCE sont présentées par les responsables opérationnels des unités organisationnelles cantonales ou communales. Les responsables de l'OFE ne contrôlent pas si les unités hiérarchiquement supérieures ou les détenteurs de l'autorité politique (les conseillers d'Etat, les chefs de départements, les conseillers communaux) sont au courant de la demande et si elles ont expressément donné leur accord. En outre, le service responsable de l'OFE a de la peine à examiner la nécessité du raccordement demande et si ce dernier respecte le principe de la proportionnalité. De plus, par manque

de bases légales et par manque de compétences en la matière, il n'aurait aucun moyen d'influencer l'environnement procédural et structurel des unités organisationnelles qui présentent une demande d'accès.

5. En ce qui concerne l'essai d'exploitation pilote de la nouvelle application EVA qui va démarrer en avril 1999, il convient, une fois de plus, d'examiner en détail dans quelle mesure de tels essais pilotes qui, à plus long terme, entreront en service et seront exploités régulièrement, nécessitent une base légale spécifique. Pour autant que le niveau de l'ordonnance soit adéquat, une réglementation correspondante devrait être intégrée dans le cadre de la révision en cours de l'ordonnance RCE. Pour le reste, le lecteur est renvoyé aux explications des point 328 (chiffre 7) et 329 (chiffre 6), qui concernent la proposition d'élaborer une base légale formelle relative aux projets pilotes de l'administration fédérale traitant des données sensibles.

6. Sur la base des documents fournis, l'expert n'a pas trouvé de base légale pour les 26 raccordements du Centre de calcul du DFJP. Une telle base légale devrait également figurer expressément dans l'ordonnance RCE puisqu'il s'agit des accès des chefs de projets et des administrateurs du système limités au cadre de leurs tâches en matière de développement, d'exploitation et de maintenance de l'application du RCE. Il est possible de procéder à cette réglementation d'une manière semblable à celle de la nouvelle ordonnance du 16 mars 1998 sur le Bureau de communication en matière de blanchiment d'argent (OBCBA) entrée en vigueur le 1er avril 1998. L'article 9, 2e alinéa, lettre f prévoit expressément que cette catégorie de personnes (chefs de projets, administrateurs de systèmes) peut bénéficier d'un droit d'accès.

7. La liste chronologique des raccordements en ligne au RCE permet de constater que certaines villes et communes comptent un nombre élevé d'accès (contrôle des habitants de la ville de Zurich : 134 utilisateurs). Il faudrait examiner la proportionnalité et la nécessité de ces accès en fonction de leur intensité d'utilisation effective qui ressort du nombre de fois que les utilisateurs accèdent au système (nombre d'ouvertures de session (*log-in*)]. Le cas échéant, il faudrait discuter de la réduction de leur nombre avec les unités organisationnelles concernées.

8. Etant donné la nouvelle procédure de contrôle ainsi que l'accès direct aux données des fichiers d'enregistrement journaliers des accès au RCE du conseiller à la protection des données de l'OFE qui a été mis en service le 1er janvier 1998, les directives provisoires relatives à la journalisation des communications de données du registre central des étrangers effectuées à l'aide d'une procédure d'appel du 2 novembre 1994 doivent impérativement être révisées dans les meilleurs délais.

9. Le DFJP doit examiner si la pratique actuelle de mise en œuvre de ces directives provisoires relatives à la journalisation des communications de données du registre central des étrangers effectuées à l'aide d'une procédure d'appel du 2 novembre 1994 par les conseillers à la protection des données des offices cités – dans le cas présent de l'OFE – est conforme à l'esprit et à la lettre de cette réglementation. Si aucun rapport écrit n'est rédigé sur les contrôles mensuels des fichiers d'enregistrement journaliers et que l'on abandonne le principe du rapport annuel écrit que les conseillers à la protection des données doivent adresser au Préposé à la protection des données du DFJP (ce qui était encore de mise en 1996) en se contentant de rapports oraux, la procédure perd en transparence et en clarté. En effet, il devient à la fois difficile de prouver que ces contrôles ont été entrepris et de documenter la conformité ou les lacunes constatées durant ces contrôles. Cette situation affaiblit la position du DFJP vis-à-vis du public ainsi que celle des conseillers à la protection des données au sein de l'administration. Dans ce domaine, il convient d'examiner cette situation avec l'OFI puisque, selon le chiffre 7 des directives du 2 novembre 1994, ces dernières seront appliquées tant que la décision du

Conseil fédéral du 29 juin 1994 concernant la définition de formes adéquates de journalisation des accès aux banques de données contenant des données particulièrement dignes de protection n'aura pas été exécutée par l'OFI. Le Préposé fédéral à la protection des données devrait également être consulté à ce sujet.

349 Recommandations et propositions de mesures

1. Le DFJP doit définir la procédure d'autorisation d'accès en ligne pour les autorités qui collaborent au RCE, les critères devant faire l'objet d'un examen (raisons de la demande de raccordement), les exigences minimales en matière de documentation (autorisation formelle) ainsi que le classement (archivage des autorisations). Ce faisant, il doit prévoir une délégation des compétences en matière d'autorisation conforme tant du point de vue hiérarchique que de celui de la responsabilité. De plus, en ce qui concerne l'autorité concédante, il faut déterminer une instance indépendante compétente en matière d'autorisation. En matière de raccordements en ligne dans le domaine de la police, il serait judicieux de définir et d'imposer à tous les services concernés de respecter des descriptions de processus unifiés communs à tous les services concernés.

2. Le DFJP doit examiner s'il est opportun d'élaborer une base légale permettant au responsable des données de procéder à des inspections afin de vérifier que les organismes cantonaux et communaux qui utilisent le RCE respectent bien les prescriptions en matière de sécurité et de protection des données.

3. Au moyen de normes légales, le DFJP doit veiller à ce que des bases légales soient élaborées avant le lancement de tout projet informatique pilote dans le domaine de la police ayant pour but de traiter des données dignes de protection. En outre, en collaboration avec le Préposé fédéral à la protection des données, il doit examiner s'il faut réglementer explicitement la réalisation de projets pilotes en ajoutant une disposition complémentaire dans la loi sur la protection des données. Cette disposition constituerait alors une base légale fixant les exigences minimales que les projets de l'administration fédérale doivent respecter lorsque des données sensibles sont traitées.

4. Le DFJP doit veiller à la mise en place d'une base légale suffisante pour les 26 accès au RCE du CC DFJP.

5. Le DFJP doit examiner la pratique actuelle en matière de procédure de rapport et d'exécution des contrôles des fichiers d'enregistrement journaliers des accès au RCE par le conseiller à la protection des données, les offices fédéraux et le Préposé à la protection des données du DFJP conformément aux directives provisoires relatives à la journalisation des communications de données du registre central des étrangers effectuées à l'aide d'une procédure d'appel du 2 novembre 1994. Il est nécessaire de garantir plus de clarté et une meilleure transparence en la matière en consignant les observations dans des rapports écrits, en accord avec l'OFI et le Préposé fédéral à la protection des données.

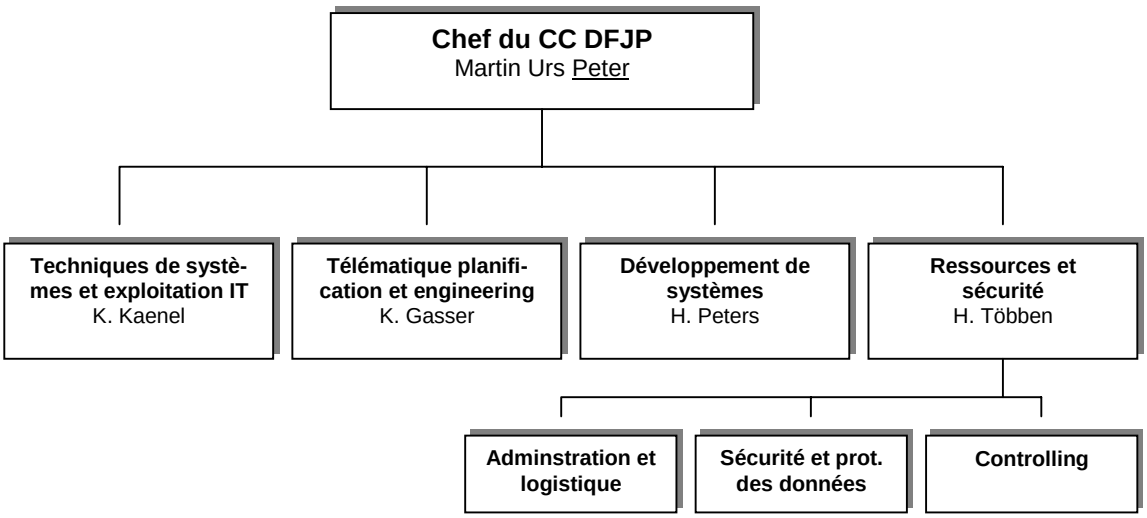
6. En se basant sur l'intensité d'utilisation effective qui ressort du nombre de fois que les utilisateurs accèdent au système [nombre d'ouvertures de session (*log-in*)], l'OFE doit examiner la proportionnalité et la nécessité des raccordements au RCE existants. Le cas échéant, il faudrait discuter de la réduction de leur nombre avec les unités organisationnelles concernées.

35 Centre de calcul du DFJP

A la suite de l'audition du responsable du RCE à l'Office fédéral des étrangers, l'expert s'est également entretenu avec le chef de l'unité Ressources et sécurité du Centre de calcul du DFJP (CC DFJP). Cet entretien a principalement concerné les tâches du CC DFJP dans le domaine du développement, de l'exploitation et de la maintenance des applications informatiques dans le domaine de la police, la participation au raccordement technique des nouveaux utilisateurs, la sécurité au centre de calcul et dans le domaine de l'infrastructure du réseau ainsi que de la question de la simultanéité de deux réseaux fédéraux (KOMBV et WAN-DFJP). Les informations principales découlant de cet entretien sont résumées dans les points ci-dessous.

351 Organisation structurelle

Le Centre de calcul du DFJP sis Industriestrasse 1 à Zollikofen est dirigé par le chef CC DFJP. Il est subdivisé en quatre unités



En matière de raccordements en ligne, ce sont surtout les unités *Développement de systèmes* et *Ressources et sécurité* qui sont concernées.

L'unité *Développement de systèmes* assure la planification, la conception, le développement, la mise en œuvre et la maintenance des applications. Le groupe DS1 (Développement de systèmes 1) est spécialisé dans le développement d'applications tournant sur la plate-forme TANDEM. C'est cette unité qui est responsable du Registre central des étrangers trilingue (RCE), du développement d'EVA (*Elektronische VisumAusstellung*) et de VOSTRA (***vo****llautomatisiertes* ***Stra****fregister*, soit casier judiciaire informatisé). Le groupe DS3 est responsable du système de recherches national RIPOL et de la nouvelle carte d'identité (CI95). Pour sa part, le groupe DS4 est responsable de toutes les applications en matière d'enquêtes pour les services de police criminelle (DOSIS, ISIS, ISOK etc.).

L'unité *Ressources et sécurité* est chargée, à l'interne, d'assurer une administration et une logistique optimale vis-à-vis des utilisateurs. Cette unité s'occupe des fonctions transversales telles que le domaine des alarmes, les commandes, le budget, la publication assistée par ordinateur, la réception, les finances, le bâtiment, la gestion des opérations, l'organisation des cours de formation, la gestion du matériel, la gestion du personnel et les relations publiques. C'est également ce service qui reçoit, qui coordonne et qui traite les demandes d'accès en ligne des utilisateurs externes ainsi que les formulaires de demande de nouvel accès des offices fédéraux du DFJP. Le groupe *Sécurité et protection des données* est

responsable de la détection et de l'évaluation des risques dans l'environnement informatique. Afin d'être mieux à même d'assumer les nombreuses tâches en matière de sécurité, la capacité dédiée à ces tâches a été augmentée. Elle est passée de 50 pour cent à 250 pour cent au 1er avril 1998. Ce groupe a notamment pour mission de proposer des mesures de sécurité, de les mettre en œuvre en collaboration avec les autres domaines et de contrôler qu'elles soient bien respectées. En outre, il est également chargé de coordonner les mesures préventives en matière de protection de la personnalité et des droits fondamentaux des personnes dont les données sont traitées. Pour sa part, le *Controlling* est, responsable de la comptabilité analytique du CC DFJP. En outre, il assiste la direction du centre de calcul en matière de gestion et de contrôle de la rentabilité des projets et des applications informatiques.

352 Organisation procédurale, traitement des demandes d'accès

Le Centre de calcul du DFJP dispose d'un manuel d'organisation qui décrit les processus principaux du CC DFJP en tant que prestataire de services. Les procédures de raccordement des utilisateurs aux diverses applications sont décrites sous Description des procédures, « Demandes de raccordement LAN/WAN » et « Demandes de raccordement exploitation ». Les descriptions de processus datent du 15 juin 1995 et ont été modifiées pour la dernière fois le 21 juin 1995. Elles sont restées en vigueur depuis le 15 juin 1995. Ces descriptions de processus, qui compléteraient avantageusement les descriptions de processus correspondants des offices fédéraux responsables des données, présentent les diverses activités que le CC DFJP doit assumer, pas à pas, et nomme les collaborateurs qui en sont responsables. Ces descriptions constituent une image de toutes les activités du CC DFJP qui sont nécessaires pour la mise en œuvre d'un raccordement en ligne. Elles sont contrôlables et peuvent donc être constamment améliorées.

353 Implantation du Centre de calcul du DFJP

353.1 Appréciation de la sécurité sur le site de Zollikofen

En 1996, la direction du CC DFJP a fait procéder à un audit de sécurité de l'ensemble des domaines d'activité du centre de calcul. C'est la version 1.1 datée du 24 mai 1996 de ce rapport confidentiel qui a été présenté à l'expert. Il a été rédigé par la société externe mandatée pour effectuer cet audit (BDS Berz Droux Scherler AG, Ingenieurunternehmung / Sicherheitsberatung de Berne) et contient une analyse détaillée des points faibles ainsi qu'un catalogue de mesures qui permettrait d'atteindre un niveau de sécurité minimum ou optimal.

De la discussion avec le responsable Ressources et sécurité du CC DFJP du 3 février 1998, il ressort que ce dernier est d'avis que le lieu d'implantation et l'infrastructure du CC DFJP ne répondent pas, respectivement pas encore aux plus hautes exigences en matière de sécurité. Ces dires sont corroborés par le rapport du 24 mai 1996 rédigé par la société BDS AG. Selon les conclusions de ce rapport, au moment de sa rédaction, il était possible de parvenir jusqu'à la porte d'entrée du centre de Zollikofen sans effraction. Des actes de sabotage ou de vengeance pourraient être commis en quelques minutes. A Zollikofen, les temps d'intervention de la police étaient – et sont probablement encore – trop longs. La protection contre les incendies était lacunaire sur les deux sites d'implantation (notamment l'isolement coupe-feu), l'installation de climatisation de Zollikofen n'avait pas été réalisée dans les règles de l'art si bien qu'en cas d'incendie, des gaz corrosifs auraient pu parvenir jusque dans la salle des machines. La société d'audit est parvenue à la conclusion que **le niveau de sécurité constaté dans le domaine de la sécurité physique du CC DFJP n'était pas acceptable et devait impérativement obliger les responsables à prendre immédiatement des mesures**.

Le 1er juillet 1997, la Délégation des commissions de gestion a visité le CC DFJP à Zollikofen. Elle a ainsi pu constater elle-même que les mesures de sécurité habituelles liées

aux personnes (contrôle d'entrée, sas, badges etc.) sont appliquées et fonctionnent bien. Le CC DFJP a élaboré un concept de zone pour la protection de l'entrée du centre. Physiquement, les collaborateurs du centre disposent d'un badge personnel qui leur permet d'accéder à l'intérieur du centre de calcul. Le cœur du CC DFJP, les salles des machines, est protégé par deux portes spéciales dont l'alarme est directement reliée au service de sécurité de l'administration fédérale ou à la police (pour de plus amples détails sur les mesures et les installations techniques de sécurité voir la prise de position du CC DFJP du 22 juillet 1998, page 2). En revanche, elle a également relevé les caractéristiques peu favorables du bâtiment, notamment sa situation à proximité de la ligne de chemin de fer Bern – Olten (risque lié au transport de matières dangereuses) ainsi que la vue depuis l'extérieur (façade de fenêtres) dans les locaux de production et la salle des machines. A l'époque déjà, cette situation avait soulevé la question de la vulnérabilité des locaux de production du CC DFJP en cas d'action terroriste ou criminelle. Des applications informatiques très sensibles fonctionnent dans les locaux de production. Le rapport sur l'audit de sécurité de la société BDS AG, qui, au chapitre 5, propose environ 20 mesures dans le domaine de la sécurité physique, parvient finalement à la conclusion que l'élimination des points faibles constatés au chapitre 5 impliquerait un **changement de lieu d'implantation**. Toutefois, cette proposition est qualifiée de mesure irréalisable (chiffre 5.1.4, page 20 du rapport d'audit).

353.2 Mise en œuvre des mesures

Le rapport sur l'audit de sécurité de la société BDS AG ainsi que la prise de position de la direction du CC DFJP du 28 février 1998 à l'attention de l'expert permettent cependant de constater que la mise en œuvre de plusieurs des mesures proposées a déjà été entreprise. Partiellement, les mesures font déjà partie intégrante de projets en cours du CC DFJP ou peuvent y être intégrées. En outre, les cadres du CC DFJP avaient pris ou initié un certain nombre de mesures immédiates, déjà durant l'audit effectué par la société BDS AG. Avec le regroupement de plusieurs services informatiques différents et la mise en service de plusieurs projets, le CC DFJP a connu une forte croissance. Au moyen de mesures individuelles, cette croissance a conduit à la réalisation d'une protection des applications et des systèmes informatiques au-dessus de la moyenne. En revanche, il n'a pas été possible d'élaborer une vue d'ensemble de la sécurité informatique, ce que, plus tard, la société BDS AG a qualifié de point faible dans l'organisation. La nomination d'un préposé à la sécurité constitue la première pierre d'une nouvelle conception. La direction du département a été sensibilisée et le projet sécurité du CC a été lancé.

L'adaptation de l'organisation du CC DFJP au 1er septembre 1997 a permis d'apurer les structures et d'allouer 200 pour cent d'un poste de travail en faveur de la protection et de la sécurité des données. De l'avis de la direction du CC DFJP, cette amélioration devrait permettre de réaliser le reste des mesures du rapport d'audit de la société BDS AG qui sont encore en suspens dans le cours de 1998. Un deuxième contrôle confié à une société indépendante est prévu afin de contrôler la réalisation conforme de ces mesures de sécurité au CC DFJP. Suite à la mise à disposition de certaines personnes clé au service du projet NOVE-IT (réorganisation de l'informatique dans l'administration fédérale), la réalisation d'un deuxième examen de la sécurité par une société indépendante n'aura probablement lieu qu'en 1999. (Remarque de la direction du CC DFJP : *« Hier sei angemerkt, dass Exponenten von Nove-IT Sicherheitsbedenken und Sicherheitsmassnahmen weniger hoch gewichten als das RZ EJPD und teilweise grundsätzlich in Frage stellen* »).

Au moment de la rédaction du présent rapport, des travaux sont en cours au Centre de calcul de Zollikofen ainsi qu'au Bundesrain 20. Ces travaux ont pour objet de mettre en œuvre certaines mesures de sécurité à des coûts acceptables. La direction des travaux prévoit que, sur les deux sites, les travaux seront terminés à la fin de la 16e semaine 1998 (en ce qui concerne l'état d'avancement des travaux, voir la prise de position du CC DFJP du 22 juillet 1998, page 2). En outre, selon les déclarations de la direction du CC DFJP, la direction du DFJP aurait décidé d'abandonner le site d'implantation de Zollikofen à moyen

terme. Le Secrétaire général du DFJP en a informé le Centre de coordination des constructions civiles par lettre datée du 30 septembre 1996 :

« Bedingt durch die immer stärkere Abhängigkeit der Verwaltung von der Informatik muss die Departementsleitung der Informatiksicherheit heute deutlich mehr Gewicht zumessen. Bundesrat Koller hat mich deshalb persönlich mit dem Projekt RZ-Sicherheit beauftragt, welches auch eine externe Sicherheitsüberprüfung durch die Firma Berz Droux Scherler AG (BDS) des Rechenzentrums beinhaltete. Gestützt auf diese Ueberprüfung hat das EJPD die folgenden Grundsatzentscheide gefällt :

- *Angesichts der knappen Finanzlage des Bundes und der ins HOZ (Gewerbezentrum Hostettler Zollikofen) investierten Bundesgelder bleibt das RZ EJPD längstens bis zum Ablauf des Mietvertrages im Jahre 2006 an der Industriestrasse 1.*
- *Sollte aber der Vermieter in der Uebergangsphase einem unverträglichen Mitmieter (z.B. Technodancing) Räumlichkeiten im HOZ vermieten, müsste ein vorzeitiger Standortwechsel erfolgen oder die betreffenden Räume durch den Bund übernommen werden.*
- *Die durch die externe Ueberprüfung aufgedeckten physischen Mängel sind nach Möglichkeit zu beheben. Der KBZ (Koordinationsstelle Bauwesen Zivil) werden hierzu die Vorschläge der BDS zur Realisierung beantragt.*
- *Der KBZ wird beantragt in ihren Bedarfsplänen einen neuen Standort für das RZ EJPD spätestens auf das Jahr 2006 hin aufzunehmen. Beim neuen Standort sind die betrieblichen und sicherheitsmässigen Bedürfnisse des Rechenzentrums EJPD vollumfänglich abzudecken.*
- *Sollte allenfalls früher ein geeignetes Gebäude frei werden (zum Beispiel durch Aufgabe eines anderen Rechenzentrums) kann das RZ EJPD mit einer Vorlauffrist von mindestens einem Jahr den Standort wechseln. »*

En conclusion, la direction du CC DFJP constate que la sécurité du centre de calcul peut être décrite et qualifiée de la manière suivante :

- excellente formation et très bonne sensibilisation des collaborateurs
- très bonne situation dans le domaine technique
- bonne base du point de vue organisationnel
- lacunes identifiées dans le domaine de la construction (site de Zollikofen)

Il faut accorder une attention particulière à la sécurité du site de Zollikofen. En matière de sécurité, les standards de construction du centre de calcul de Zollikofen sont insuffisants. Le lecteur attentif de la presse spécialisée n'aura pas manqué de remarquer l'article choc paru dans la *Handelszeitung* du 4 février 1998 (édition numéro 6, page 53, rubrique *News*). Cet article décrit des tests réalisés par l'armée suédoise avec la « bombe électronique ». Cette « bombe » ne fait aucun bruit, elle prend aisément place dans un attaché-case et elle a une puissance destructrice fatale. L'armée suédoise a réalisé ses tests avec une « bombe électronique » de fabrication russe. Elle détruit tout ordinateur à proximité. En fait, cette « bombe » est un appareil qui coûte moins de 100'000 dollars et qui est capable d'émettre de coutres impulsions de micro-ondes atteignant jusqu'à dix gigawatts, ce qui représente la puissance de dix réacteurs nucléaires. La bombe a une portée de quelques douzaines de mètres ; des modèles plus importants parviennent à quelques centaines de mètres. Elle existe également sous forme de pistolet. Cette arme « silencieuse » peut être utilisée contre n'importe quel type d'ordinateur, qu'il soit à bord d'un avion de combat, dans un centre de calcul, dans une banque ou dans une centrale nucléaire. Les impulsions d'énergie grillent littéralement tous les circuits électroniques à sa portée. Ce type d'engin est particulièrement dangereux dans les mains de terroristes. Selon les experts en matière d'armement, une telle arme n'a encore jamais été utilisée. Toutefois, l'article précise que plusieurs pays ont acquis cette technologie. Depuis la guerre du Golfe, les *missiles Cruse* de l'armée américaine seraient équipés de tels systèmes (Handelszeitung 4. février 1998, page 53).

De l'avis de l'Office fédéral de l'informatique, la consolidation prévue des centres de calcul de l'administration fédérale devrait rapidement permettre un transfert du CC DFJP, par exemple dans les locaux protégés du Département fédéral de la défense, de la protection de

la population et des sports DDPS (voir prise de position de l'OFI du 22 juillet 1998, page 1, chiffre 2).

354 Niveau de la sécurité au Centre de calcul du DFJP

354.1 Politique de sécurité (Security Policy)

Dans le domaine de la sécurité informatique, le CC DFJP a mis en œuvre une politique de sécurité (*le document intitulé Security Policy, n'existe qu'en version allemande*) pour l'ensemble du centre de calcul. Ce document définit les responsabilités, les tâches et les compétences dans tous les domaines de la sécurité informatique et décrit les principes en matière de sécurité ainsi que l'organisation nécessaire à leur respect. La direction du CC DFJP est responsable de la sécurité informatique de l'ensemble du centre de calcul. Elle définit et procède continuellement à la mise à jour de la politique de sécurité du CC DFJP. Cette politique de sécurité informatique est fondée sur les quatre pierres angulaires suivantes :

- **Disponibilité** (fiabilité, stabilité, et sauvegarde des données),
- **Confidentialité** (accès protégés, protection contre les écoutes),
- **Intégrité** (exactitude des données),
- **Clarté, transparence** (audits, *log-in*).

Toutes les mesures de sécurité du CC DFJP doivent respecter les principes de la légitimité, de proportionnalité, de la nécessité et de l'opportunité. La direction du CC DFJP procède périodiquement à des contrôles (contrôles de performances, de qualité, de délais et contrôle des processus de travail notamment) afin de garantir l'application de la politique de sécurité. Un préposé à la sécurité est responsable de toutes les descriptions, directives, prescriptions et mesures (portefeuille de sécurité). Les supérieurs hiérarchiques sont responsables de la mise en œuvre et du respect de la politique de sécurité et des prescriptions en vigueur dans leur domaine et pour leur groupe de collaborateurs. Dans le cadre de l'exécution de ses tâches, chaque collaborateur doit observer les principes de la politique de sécurité ainsi que les prescriptions en vigueur.

Dans le domaine des systèmes et du personnel de production, il est nécessaire d'atteindre le plus haut niveau de sécurité. Les données des systèmes exploités doivent être protégées contre toute consultation, modification ou copie par des personnes non autorisées. Elles doivent également l'être contre les accès par les membres du personnel d'exploitation, de maintenance et de développement. Les données ne doivent être transmises ou rendues accessibles que sur demande écrite du responsable des données. Les tests avec des données d'exploitation ne peuvent être effectués qu'avec l'accord du responsable des données et chaque utilisateur doit être autorisé au moyen d'une identité et d'un mot de passe personnels. Dès que des systèmes de formation ou de test contiennent des données, les dispositions de sécurité qui s'appliquent sont les mêmes que celles de la production. Chaque fonction de sécurité doit être enregistrée dans un fichier d'enregistrement journalier et ces fichiers journaliers doivent pouvoir être analysés.

354.2 Mise en œuvre des mesures

Dans sa prise de position du 28 février 1998, la direction du CC DFJP souligne expressément que la mise en vigueur de la politique de sécurité du CC DFJP (*Security Policy*) du 19 août 1997, l'élaboration du portefeuille de sécurité et la réorganisation au sein du CC DFJP au 1er septembre 1997 ont permis de mettre en œuvre des mesures importantes qui avaient été proposées à l'issue l'audit de sécurité réalisé par la société BDS AG. Ainsi, la directive de sécurité l'Office fédéral de l'informatique S02 du 19 avril 1995 concernant la Protection de base des systèmes et applications informatiques serait réalisé à 90 pour cent. L'émulation TAXI a été développée pour les applications installées sur le

système principal qui fonctionnent aussi bien sur les systèmes TANDEM que DEC. Elle intègre un chiffrement logiciel *end-to-end*. Les accès au système TANDEM CC sont individuels pour chaque collaborateur du CC et passent par le produit de sécurité SECOM. La protection des accès de la salle des machines à Zollikofen sera renforcée au moyen de transformations réalisées au cours de la semaine 14/1998. Les temps d'intervention sur le site de Zollikofen ne peuvent pas être réduits. Les isolations coupe-feu du bâtiment de Zollikofen ont été améliorées dans le courant du printemps 1997. Des transformations seront entreprises au Bundesrain durant la semaine 12/1998 et un nouveau contrôle sera effectué à Zollikofen durant la semaine 15/1998. L'installation de climatisation à Zollikofen sera transformée conformément aux mesures proposées durant les semaines 11 à 16/1998. De plus, la protection contre les surtensions et la mise à terre du distributeur principal ont également fait l'objet d'un contrôle. Pour le reste, la direction du CC DFJP prend position de manière détaillée au sujet de certaines mesures proposées dans le rapport sur l'audit de sécurité et présente l'état de leur mise en œuvre.

354.3 Appréciation finale du niveau de la sécurité

En résumé, il est possible de constater que la réalisation d'un audit de sécurité du CC DFJP par une société indépendante a permis de tirer des conclusions importantes en la matière. En particulier en ce qui concerne le centre de calcul de Zollikofen, il a révélé la nécessité d'entreprendre un certain nombre de transformations du bâtiment. Mais il a également révélé la nécessité de prendre des mesures considérables dans le domaine logique ainsi qu'en ce qui concerne l'organisation procédurale. Des mesures ont été initialisées au niveau organisationnel et en ce qui concerne le personnel avec le renforcement du domaine Ressources et sécurité. La réalisation progressive des mesures de détail est en cours et se trouve en bonne voie d'achèvement.

(Sur proposition de la section compétente, la Commission a décidé de ne pas publier ce passage par des motifs de sécurité de l'Etat)

La mise à l'abri des banques de données et de l'infrastructure du système contre les accès et les manipulations non autorisées de données par des collaborateurs du CC DFJP est également en bonne voie. Avec le programme de sécurité SECOM – qui est activé sur tous les systèmes TANDEM (prise de position du CC DFJP du 26 février 1998, page 4, chiffre 4.3) – la directive de sécurité S02 Protection de base des systèmes et applications informatiques, du 19 avril 1995 serait réalisée à 90 pour cent. Il faut cependant souligner qu'il est nécessaire de surveiller continuellement tout ce qui a trait à la sécurité et de faire procéder à des contrôles par une instance indépendante. En effet, même les applications les plus sures ont toujours des « *super-superusers* » dont les droits d'accès donnent toute latitude en matière de manipulation du système et des données. Les mesures correspondantes au niveau de l'organisation structurelle (domaine Ressources et sécurité)

ont été prises depuis le 1er septembre 1997 et, ici également, les contrôles peuvent être effectués régulièrement. La planification d'un nouvel audit de sécurité par une société indépendante permet de s'assurer de la mise en œuvre des mesures de sécurité ainsi que de leur adaptation continuelle. L'expert estime que la décision de reporter ce nouvel audit de sécurité à 1999 au plus tôt – pour des raisons d'allocation prioritaire des ressources en faveur du projet NOVE- IT – n'est pas pertinente.

355 Contrôle de sécurité des collaborateurs du CC DFJP

Les collaborateurs du CC DFJP, en tant que responsables de systèmes, opérateurs, analystes, programmeurs, chefs de projets, spécialistes en communications et autres fonctions, sont en contact direct avec toute l'infrastructure informatique, les programmes importants, les données sensibles et les applications développées et en cours de développement dans le domaine de la police. Dans le cadre de leurs fonctions ils acquièrent ainsi une bonne connaissance et une bonne vue d'ensemble des structures, modèles, données, procédures ainsi que d'autres informations importantes dans un domaine sensible des tâches de l'Etat. Des personnes ont également été attribuées au CC DFJP afin de soutenir les divers offices fédéraux en matière d'informatique (par exemple en 1995 pour la Section Analyse criminelle voir courrier du CC DFJP du 31 mai 1995 adressé au Secrétariat général du DFJP). En effectuant les tâches que l'on attend d'eux, les collaborateurs du CC DFJP remplissent l'une ou plusieurs des conditions de l'ordonnance relative aux contrôles de sécurité dans l'Administration fédérale du 15 avril 1992 (RS 172.013). Conformément aux dispositions de l'article 2 de cette ordonnance, sera soumis à un contrôle de sécurité celui qui, dans le cadre des fonctions prévues :

a) ...
b) a régulièrement accès à des secrets touchant à la sûreté intérieure ou extérieure de la Confédération et est exposé à des actes d'espionnage ;
c) ...
d) exerce une activité ayant trait à la lutte contre l'espionnage, le terrorisme ou le crime organisé ;
e) est susceptible. En tant que collaborateur au sein d'un organe chargé des contrôles de sécurité, de porter gravement atteinte aux droits de la personnalité des personnes concernées en raison de l'accès régulier qu'il a à des données méritant une protection particulière.

Le Conseil fédéral approuve la liste des fonctions pour lesquelles les candidats sont soumis à un contrôle de sécurité (article 2, 2e alinéa de l'ordonnance).

Cette liste ne comporte toutefois le nom d'aucun des collaborateurs du CC DFJP bien que, en raison de leurs fonctions, ces derniers remplissent une ou plusieurs des conditions impliquant un contrôle de sécurité. La direction du CC DFJP a déjà rendu le Secrétariat général du DFJP attentif à cette situation (voir courrier de la direction du CC DFJP du 31 mai 1995 adressé au Secrétariat général du DFJP). Dans ce même courrier, la direction du CC DFJP communique également sa décision de soumettre tout le personnel (interne et externe) du CC DFJP (y compris le personnel du service domestique) au contrôle de sécurité. Toutefois, depuis lors, aucune démarche concrète n'a été entreprise dans ce sens. Par lettre du 10 février 1998, le chef du personnel du Secrétariat général du DFJP a indiqué à la direction du CC DFJP qu'en vertu de l'ordonnance du 15 avril 1992 ainsi qu'au vu de la liste des offices sensibles en matière de sécurité du DFJP, il n'était pas possible de soumettre les employés du CC DFJP à un contrôle de sécurité d'une manière générale.

L'expert n'est pas de cet avis. D'une part, selon les définitions de l'article 2 de l'ordonnance relative aux contrôles de sécurité dans l'Administration fédérale, les conditions pour un contrôle de sécurité sont réunies, parfois même à plusieurs titres. D'autre part, elles découlent également des caractéristiques inhérentes au développement, à l'exploitation, à la maintenance et à la gestion d'applications et de banques de données dans le domaine de la police. Il suffit au DFJP de proposer au Conseil fédéral de compléter ladite liste en y incluant tous les collaborateurs du CC DFJP. Les justifications pour cette demande ont été fournies

par écrit il y trois ans déjà. La mise à jour de cette liste et le contrôle de sécurité des collaborateurs du CC DFJP devraient être réalisés le plus rapidement possible.

356 Raccordement des représentations suisses à l'étranger

La liste chronologique de ces raccordements en ligne dans le domaine couvert par le RIPOL élaborée par l'OFP en date du 26 novembre 1997 permet de constater que des représentations suisses à l'étranger (24) et des services Interpol (30) sont raccordés au RIPOL par le réseau WAN-DFJP/KOMBV4 ou par le réseau WAN-DFJP/SITA via TCP/IP, X.25 et ISDN. Le chiffrement serait assuré en partie par des logiciels (*end-to-end*) et/ou par des chiffrement des liaisons (Back-Bone WAN-DFJP).

(Sur proposition de la section compétente, la Commission a décidé de ne pas publier ce passage par des motifs de sécurité de l'Etat)

Pour tous les raccordements, les communications passent par des réseaux de communication par paquets via X.25 (9.6 à 19.2 Kbit/s). Le chiffrement est assuré au moyen d'un chiffrement par paquets *playload* de la société GRETAG (clé 128 bits).

(Sur proposition de la section compétente, la Commission a décidé de ne pas publier ce passage par des motifs de sécurité de l'Etat)

357 KOMBV3 et WAN-DFJP, réseaux de communication parallèles

Personne ne conteste que les applications dans le domaine de la police et l'infrastructure de communication qui leur est nécessaire doivent être protégées par des moyens de sécurité importants afin d'empêcher les tiers non autorisés d'y accéder. Pour cette raison, le DFJP a développé son propre réseau de communication logiquement séparé (WAN-DFJP) , spécialement pour ces applications. Ce réseau constitue un système de communication en forme d'étoile qui relie le CC DFJP à ses 26 partenaires (cantons). Les communications transitant par ce système ont lieu exclusivement entre les autorités cantonales concernées et le CC DFJP. Des communications entre les partenaires eux-mêmes ou vers d'autres réseaux (par exemple Internet) ne sont pas possibles. Pour cette raison, le réseau de communication WAN-DFJP est parfois décrit comme étant un ensemble de réseaux individuels (au sujet de cette problématique, voir la prise de position du CC DFJP du 22 juillet 1998, pages 3 et 4). Dans la plupart des cas, en fonction de l'importance des groupes d'utilisateurs, ce réseau de communication avec les cantons est conduit jusque dans les locaux de la police cantonale. Il y a donc redondance entre ce réseau indépendant dans le domaine de la police et le réseau KOMBV-KTV. Les cantons sont connectés au réseau KOMBV-KTV par le biais de nœuds de commutation installés dans les chefs-lieux cantonaux. Ce réseau de base sert aux échanges de toutes les informations et données en dehors de celles qui concernent le domaine de la police. Cette exploitation en parallèle de deux réseaux fédéraux de communication n'est souvent pas comprise et fait l'objet de critiques, particulièrement de la part les cantons, mais également de celle de certains services de la Confédération. En effet, cette redondance entraîne des dépenses et des coûts supplémentaires (infrastructure, sécurité, compétences, responsabilités etc. à double). Les discussions en matière de sécurité des communications révèle un fossé très net entre les partisans de la protection des réseaux et les partisans de la protection des applications (cryptage des applications elles-mêmes). Les services de police de la Confédération craignent qu'un regroupement des réseaux fédéraux de communication ne garantisse plus la sécurité de leurs applications (voir les chiffres 31, 33 et 36, pages 23 à 34 du Rapport CCF ainsi que la prise de position du CC DFJP du 22 juillet 1998, pages 3 et 4). D'autres organes de la Confédération soulignent que, du point de vue organisationnel, la gestion commune du l'infrastructure IT (réorganisation de l'informatique dans le cadre de la réforme du gouvernement et de l'administration fédérale, projet NOVE-IT) permettrait de regrouper les réseaux KOMBV-KTV et WAN-DFJP (voir prise de position de l'OFI du 22 juillet 1998, page 2, chiffre 2).

L'expert soutient la recommandation du Rapport CCF qui propose d'intégrer les deux réseaux logiquement distincts de la Confédération, KOMBV-KTV et WAN-DFJP. Etant donné que les arguments techniques et les avis des services de la Confédération impliqués divergent fortement, le Conseil fédéral pourrait décider de recourir à une société indépendante spécialisée dans le domaine des communications afin d'apporter plus de sérénité au débat. En effet, cette problématique est caractérisée par un contexte émotionnel. La redondance en matière d'infrastructures de communication de la Confédération n'est guère défendable, ni du point de vue économique, ni de celui de la sécurité. Après plusieurs

années de querelles à ce sujet, le Conseil fédéral doit dans tous les cas trancher très rapidement et prendre une décision univoque, avec ou sans recours aux services d'une société indépendante.

358 Recommandations et propositions de mesures

Au vu de la situation du CC DFJP exposée au chapitre 35 du présent rapport, les quatre mesures / recommandations suivantes s'imposent :

1. Le site du Centre de calcul du DFJP de Zollikofen doit être abandonné le plus rapidement possible. La recherche d'une variante de remplacement doit tenir compte de toutes les possibilités internes et externes de la Confédération.

2. Le Centre de calcul du DFJP doit, le plus rapidement possible, faire à nouveau l'objet d'un audit de sécurité afin de contrôler l'efficacité des mesures qui ont été prises et, le cas échéant, de révéler les lacunes de sécurité subsistantes. En matière d'allocation des ressources, les aspects de la sécurité du Centre de calcul du DFJP priment sur l'exécution du projet NOVE-IT.

3. Conformément à la demande de la direction du Centre de calcul du DFJP, les collaborateurs du centre doivent immédiatement être soumis à un contrôle de sécurité. Le DFJP doit veiller à ce que le Conseil fédéral complète la liste correspondante.

4. Le Conseil fédéral doit, le cas échéant en mandatant une société spécialisée indépendante - clarifier et évaluer les divers arguments pour ou contre l'intégration des deux réseaux de communication de la Confédération KOMBV-KTV et WAN-DFJP. En se basant sur les résultats de cette évaluation, il doit ensuite *rapidement* décider de la suite des opérations (intégration ou maintien de l'exploitation en parallèle).

4 APPRECIATION GENERALE

Le présent rapport d'expertise a présenté et examiné les pratiques des services de la Confédération en matière d'autorisations d'accès en ligne dans le domaine de la police. Seuls quatre systèmes informatiques (RIPOL, DOSIS, ISIS, RCE) et le Centre de calcul du DFJP ont été examinés. Bien que de nombreux autres systèmes d'information comportant également des raccordements en ligne d'utilisateurs tiers soient encore exploités dans le domaine de la police, les résultats de l'analyse de ces quatre systèmes informatiques permettent malgré tout de tirer des conclusions de portée générale.

Jusqu'à présent, la réglementation des autorisations en matière de raccordements en ligne a plutôt été traitée de façon subalterne. Dans tous les domaines, cette question a été résolue soit par une délégation constante jusqu'à l'unité opérationnelle hiérarchiquement la plus basse, soit dans le cadre de la responsabilité opérationnelle de l'unité administrative correspondante. Il n'y a pas de réglementation générale d'un niveau supérieur de la réglementation des autorisations en matière de raccordements en ligne pour tous les systèmes d'information qui tiendrait compte du principe de l'indépendance de l'autorité compétente en matière d'autorisation. Cela ne signifie toutefois pas que les unités administratives responsables ont mal travaillé. En revanche, cela montre que l'on n'a jamais accordé au domaine des autorisations en matière de raccordements en ligne l'importance qui lui revient au vu de la sensibilité des données personnelles et des profils de la personnalité traités dans le cadre des systèmes d'information de la police. Les conditions légales très strictes, préalables à toute exploitation des systèmes d'information de police (nécessité, proportionnalité et opportunité), ne doivent pas être vidées de leur contenu. Elles doivent être garanties dans le cadre d'une procédure clairement définie qui assure le respect à la fois du principe d'indépendance et des prescriptions légales. Lorsque des unités administratives cantonales ou communales assument des tâches de la Confédération, la collaboration avec la Confédération occasionne des difficultés particulières dans le domaine de l'accès aux systèmes d'information de police. Dans ce cas, une procédure d'autorisation d'accès en ligne adéquate doit garantir que l'autorité politique (cantonale ou communale) a pris connaissance et agréé la demande d'accès en ligne formulée par l'autorité qui lui est subordonnée. De plus, dans ce domaine également, les mesures en matière de protection et de sécurité des données doivent également pouvoir être imposées. Ici, comme dans le domaine des projets pilotes traitant des données sensibles d'ailleurs, il est nécessaire d'élaborer de nouvelles bases légales. La nécessité et la proportionnalité des raccordements en ligne existants doivent faire l'objet d'un examen permanent. Les liaisons qui ne sont pas ou qui sont peu utilisées doivent être supprimées. En tant qu'exploitant et concepteur des systèmes d'information de police, le Centre de calcul du DFJP doit être intégré dans toute réflexion d'ensemble. A ce sujet, il est nécessaire d'accorder l'importance nécessaire aux aspects de la sécurité au site actuel d'implantation à Zollikofen, au contrôle de sécurité de tous les collaborateurs du centre, à un audit de sécurité réalisé par une société indépendante ainsi qu'à l'intégration des deux réseaux logiquement distincts de la Confédération, KOMBV-KTV et WAN-DFJP. Les détails des mesures se trouvent aux chapitres « Recommandations et propositions de mesures »

Après rédaction du présent rapport d'expertise et son traitement par la Commission de gestion, tous les documents en possession de l'expert seront remis à l'Organe parlementaire de contrôle de l'administration (OPCA).

Lucerne, le 30 juillet 1998

Lukas Fässler
licencié en droit et avocat

Appendice 1

Évaluation et résumé de la procédure de consultation interne à l'administration

accompagne le rapport d'expert du 30 juin 1998:

Mise en place de liaisons "online" dans le domaine de la police

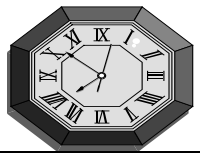
Document	G:\DatALL\Fl\Eigene Dateien 04.98\Eigene Dateien\ONLINE\Nachtrag 1 zum Expertenbericht.doc
Version:	1.0
Date:	20/11/1998
Remplace le document du:	
Auteur:	© Lukas Fässler, licencié en droit, avocat, Hirschmattstrasse 36, 6002 Lucerne
Dernière modification le:	30.7.1998
Autorisés:	Section Autorités de la CdG-CE; OPCA; Offices fédéraux concernés, ainsi que le SG du DFJP et le SG du DF; Lukas Fässler, Lucerne
Distribué le:	1.8.1998

Table des matières

1 INTRODUCTION

Le 30 juin 1998, l'expert a terminé son rapport "Mise en place de liaisons "online" dans le domaine de la police" à l'intention de la section "Autorités" de la Commission de gestion du Conseil des Etats. Les 1er et 2 juillet 1998, l'expert a informé oralement de ses principales conclusions l'Office fédéral de la police, la Police fédérale, l'Office fédéral des étrangers et le Centre de calcul du DFJP. Suite à ses explications, une procédure de consultation interne à l'administration a été lancée. Le délai pour les réponses a été fixé au 23 juillet 1998.

Le tableau suivant montre quels sont les services qui ont été invité à donner leur avis, et lesquels ont fait usage de cette possibilité par écrit:

Invités à donner leur avis	Explications orales de l'expert	Avis rendu par écrit	Remarques
DFJP **Secrétariat général** 2.7.1998	Aucunes	~~22.7.1998 Keine materielle Stellungnahme Weiterleitung der Aemterstellungnahmen~~	Aucunes
DF **Secrétariat général** 2.7.1998	Aucunes	~~Keine~~	Aucunes
Office fédéral de l'informatique 2.7.1998	Aucunes	22.7.1998 ☑	Aucunes
Préposé fédéral à la protection des données 2.7.1998	Aucunes	7.7.1998 ☑	**Prorogation du délai jusqu'au 31.8.1998** 
Centre de calcul DFJP 1.7.1998	Explications orales lors de la remise du rapport le 1.7.1998 à M. Többen	22.7.1998 ☑	Aucunes
Police fédérale	Explications orales lors de la remise du rapport le 1.7.1998 à M. Herrli	21.7.1998 ☑	Aucunes

Office fédéral de la police 2.7.1998	Explications orales lors de la remise du rapport le 1.7.1998 à M. Lobsiger	22.7.1998 	Aucunes
Office fédéral des étrangers 2.7.1998	Explications orales lors de la remise du rapport le 1.7.1998 au directeur, M. Huber	21.7.1998 	Aucunes

2 AVIS EXPRIMES LORS DE LA CONSULTATION

Lorsque les avis exprimés par ces instances fédérales contiennent des compléments ou des adaptations d'ordre matériel ou formel, il en a été tenu compte dans la version 4.0 du rapport de l'expert, daté du 30.7.98.

Pour les argumentations complémentaires ainsi que les avis s'opposant aux propositions de recommandations et de mesures contenues dans le rapport de l'expert, on se reportera aux annexes 1 à 5 du présent résumé.

Pour l'essentiel, les réponses faites par les organes fédéraux consultés ne remettent pas en question le rapport de l'expert, ni dans l'exposé des faits, ni dans les principes, ni dans les recommandations, ni dans les mesures proposées. Ces réponses apportent certes ça et là quelques précisions quant aux procédures, et donnent quelques explications complémentaires sur la situation juridique effective (notamment sur les bases légales entrées en vigueur après que le rapport a été terminé, le 1.7.98 [BWIS]), mais ces renseignements ne remettent nullement en question les conclusions de l'expert.

Il faut ici relever que tout au long de ses travaux, l'expert a pu compter sur la collaboration constructive des responsables des organes fédéraux concernés. Leur aide a été particulièrement précieuse pour rassembler tous les documents nécessaires, pour évaluer la situation actuelle, ainsi que pour les interviews. On notera encore que l'Office fédéral a rendu avec son avis un complément sur la procédure d'autorisation des liaisons "online" (cf. annexe 2 du présent résumé), selon un document préparé par l'expert.

11 Police fédérale

Avis du 21.7.1998

12 Office fédéral des étrangers

Avis du 21.7.1998, avec description de la procédure d'autorisation de liaisons "online"

13 Office fédéral de la Police

Avis du 22.7.1998

14 Centre de calcul du DFJP

Avis du 22.7.1998

15 Office fédéral de l'informatique

Avis du 22.7.1998

16 Préposé fédéral à la protection des données

Avis du 22.7.1998

Lucerne, le 30 juillet 1998

Lukas Fässler,
avocat