Rapport de la Commission de gestion du Conseil des Etats du 19 novembre 1998 «Mise en place de liaisons ‹on line› dans le domaine de la police»

Avis du Conseil fédéral

du 23 juin 1999

Monsieur le Président,
Mesdames et Messieurs,

Le 17 novembre 1998, vous nous avez remis votre rapport «Mise en place de liaisons ‹on line› dans le domaine de la police». Ce rapport contient une motion que le Conseil des Etats a transmise au Conseil fédéral le 17 novembre 1998 et des recommandations formulées par votre commission. Vous avez joint à votre rapport un rapport d'expert du 30 juillet 1998 sur lequel vous nous priez également de prendre position.

Voici l'avis du Conseil fédéral quant à la motion, aux recommandations de la Commission de gestion du Conseil des Etats (CdG-CE) et aux remarques formulées dans le rapport d'expert.

Nous vous prions d'agréer, Monsieur le Président, Mesdames et Messieurs, l'assurance de notre haute considération.

23 juin 1999

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Ruth Dreifuss
Le chancelier de la Confédération, François Couchepin

Avis

1 Remarques liminaires

Le Conseil fédéral tient tout d'abord à remercier les membres de la CdG-CE d'avoir examiné l'important problème que constituent les liaisons «on line» dans le domaine de la police. Les développements technologiques rapides survenus dans les secteurs de l'informatique et des télécommunications ont en effet débouché sur une augmentation massive des moyens informatiques et des liaisons «on line». Le DFJP n'est pas resté à la traîne et a suivi ce développement, mais la mise en place de liaisons «on line» a toujours eu pour seul objectif de permettre aux autorités de police d'effectuer efficacement leurs tâches, tout en protégeant au mieux la personnalité des personnes concernées. Ce développement doit être contrôlé. Aussi, une procédure d'approbation des différentes phases des projets, qui soumet à une décision du comité de projet la mise en œuvre de nouvelles liaisons «on line», a-t-elle été mise en place dans le cadre de la procédure HERMES[1]. Au DFJP, la libération de chaque phase de projet est en outre approuvée par le secrétaire général suppléant chargé de l'informatique.

2 Motion de la CdG-CE

Sur la base de ce rapport, le Conseil des Etats a transmis au Conseil fédéral la motion suivante de sa commission de gestion:

Liaisons «on line». Renforcer la protection pour les données personnelles

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

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

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

Le 8 mars 1999, le Conseil fédéral a transmis aux Chambres fédérales son avis sur la motion de la CdG-CE et a demandé que cette motion soit transformée en postulat. Le Conseil des Etats a adopté cette motion lors de sa séance du 16 mars 1999; il a pourtant tenu compte des explications du chef du DFJP qui ne s'est pas opposé à la motion pour autant que les bases légales demandées pour les liaisons «on line» mises en place dans le cadre d'un projet pilote puissent être contenues dans des

[1] Méthode de conduite et de déroulement des projets informatiques (cf. Manuel «Hermes», OFI, édition 1995).

ordonnances du Conseil fédéral. La réponse intégrale du Conseil fédéral à la motion de la CdG-CE est reproduite ci-dessous:

«Selon le droit actuel, une base légale expresse est nécessaire pour établir une procédure d'appel permettant d'accéder en ligne à une banque de données qui est gérée par un organe fédéral au sens de l'art. 3, let. h, LPD[2] *et qui contient des données personnelles (art. 17, al. 1, et 19, al. 3, LPD). Une base légale expresse dans une loi formelle est même requise lorsque la procédure d'appel rend accessibles des données sensibles ou des profils de la personnalité (art. 19, al. 3, LPD). Le Conseil fédéral interprète ces dispositions comme s'appliquant à tout projet de banque de données, y compris durant la phase pilote. Cela étant, il serait inutile de réviser la LPD pour préciser que les exigences de cette loi valent aussi pour la phase pilote des projets informatiques.*

Pour le Conseil fédéral, il s'agit à l'avenir non pas tant de renforcer les exigences de la LPD en matière de légalité mais plutôt d'optimiser ces exigences. La nécessité d'une base légale formelle expresse pour introduire une liaison avec procédure d'appel sur des données sensibles n'est en effet pas sans poser des problèmes lors de la phase initiale d'un projet. En l'absence de test en grandeur réelle, il est souvent difficile de circonscrire avec précision le cercle des instances administratives fédérales et cantonales, voire, dans certains cas, les personnes privées, susceptibles d'avoir besoin d'accéder par procédure d'appel à une banque de données en création. Le respect strict de l'exigence d'une base légale formelle peut conduire à une réglementation trop large qui crée des attentes chez les instances administratives mentionnées dans la loi et qui rend plus difficile le refus ultérieur d'une demande d'accès en ligne.

Conscient de ce problème, le Conseil fédéral est prêt à proposer une révision de la LPD en vue d'y introduire une réglementation particulière pour la phase pilote d'un projet lorsqu'un motif d'intérêt public important rend indispensable le traitement de données sensibles ou de profils de personnalité avant l'édiction d'une base légale formelle. On pourrait envisager la création d'une norme de délégation dans la LPD permettant de s'appuyer durant cette phase sur une ordonnance du Conseil fédéral, voire sur une autorisation du Préposé fédéral à la protection des données qui serait assortie de charges. Le défaut provisoire de base légale formelle devrait être compensé par d'autres garanties permettant d'assurer la protection des droits des personnes concernées.

Dans la mesure où il ne ressort pas clairement du texte de la motion si la nécessité d'une base légale se réfère à une base légale formelle ou à une base légale matérielle, le Conseil fédéral propose de transformer la motion en postulat.

Actuellement, le champ d'application de la LPD est délimité en fonction de l'organe qui traite les données personnelles. Le traitement de données par les autorités cantonales est en principe régi non pas par la LPD mais par le droit cantonal (art. 2, al. 1, LPD). Peu importe que les données traitées aient été obtenues directement par les autorités cantonales ou que celles-ci les reçoivent par un accès en ligne sur une banque de données gérée par la Confédération. Cette autonomie cantonale en matière de protection des données résulte de l'autonomie organisationnelle cantonale, un principe fondamental du fédéralisme suisse. En matière de protection des

2 Loi fédérale du 19 juin 1992 sur la protection des données (LPD, RS **235.1**).

données, l'autonomie cantonale a cependant été restreinte déjà à plusieurs reprises par le législateur fédéral (cf. 16, al. 2, 37, al. 1, LPD; art. 16, al. 3, LMSI[3]; art. 16, al. 1, 17, al. 1, LSF[4]).

Ces extensions du champ d'application des dispositions fédérales de protection des données montrent que le législateur fédéral tend déjà à éviter que l'autonomie cantonale n'abaisse le seuil de protection des données transmises par la Confédération aux autorités cantonales. La Confédération a en effet la responsabilité de veiller à ne pas communiquer les données personnelles qu'elle gère à des tiers qui ne respecteraient pas les mêmes standards de protection. La sécurité d'un système informatique et la protection des données qui y sont contenues se mesurent à l'aune du maillon le plus faible. Actuellement, le niveau de protection des données est différent d'un canton à l'autre; seuls 17 cantons et demi-cantons ont ainsi adopté une loi de protection des données et tous les cantons n'ont pas encore mis en place une autorité de protection des données comme l'art. 37, al. 2, LPD les y invite. Le large accès en ligne d'autorités cantonales et communales à certaines banques de données fédérales pourrait à l'avenir s'avérer problématique en l'absence d'une harmonisation entre la Confédération et les cantons sur les standards de protection à respecter. De ce point de vue, il ne serait pas inutile de fixer au niveau fédéral le standard à respecter en matière d'accès, d'utilisation, de protection et de contrôle des banques de données fédérales. Il conviendra toutefois d'examiner si ce standard doit prendre la forme de règles fédérales directement applicables ou s'il peut être atteint par des normes supplétives qui ne s'appliquent qu'en l'absence d'une réglementation cantonale correspondante. C'est la raison pour laquelle le Conseil fédéral propose, sur ce point également, de transformer la motion en postulat.

Le Conseil fédéral propose de transformer la motion en postulat.»

3 Recommandations de la CdG-CE

La CdG-CE a formulé douze recommandations auxquelles le Conseil fédéral donne les réponses suivantes.

3.1 Opportunité, proportionnalité et finalité

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

Les principes généraux de la LPD, notamment les al. 2 et 3 de l'art. 4, stipulent que les traitements de données doivent être effectués conformément aux principe de la bonne foi et de la proportionnalité et uniquement dans le but qui est indiqué lors de la collecte des données, qui est prévu par la loi, ou qui ressort des circonstances. Le

3 La loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS **120.4**).
4 Loi sur la statistique fédérale du 9 octobre 1992 (RS **431.01**).

Conseil fédéral a toujours veillé à ce que ces principes soient strictement appliqués lors de l'adoption de dispositions spécifiques réglant la protection des données dans un domaine particulier. Aussi le Conseil fédéral explique-t-il dans chaque message l'opportunité des mesures proposées, qui sont ensuite examinées en connaissance de cause par le Parlement. Dans ce sens, la présente recommandation constitue un rappel de la manière d'examiner la mise en place de liaisons «on line».

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation.

3.2 Contrôle par l'instance compétente

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

L'art. 31 LPD stipule que le Préposé fédéral à la protection des données (PFPD) se prononce sur les projets d'actes législatifs fédéraux qui touchent de manière importante à la protection des données. La mise en place de liaisons «on line» touche sans aucun doute de manière importante à la protection des données, le PFPD est donc chaque fois consulté. En pratique, le PFPD est appelé à donner son avis dans le cadre de la consultation des offices. Si l'avis du PFPD ne peut pas être complètement pris en considération par le département compétent, ce dernier informe le Conseil fédéral de l'avis divergent du PFPD.

La nécessité et les objectifs d'une liaison «on line» sont toujours expliqués dans la proposition au Conseil fédéral, sur laquelle, nous l'avons vu ci-dessus, le PFPD est appelé à se prononcer. Quant aux coûts d'une liaison et aux risques d'utilisation abusive ou d'atteintes à la personnalité, ce sont des éléments qui doivent être définis lors de l'élaboration de tout projet informatique et qui figurent dans les documents établis pour l'approbation des diverses phases du projet.

Le Conseil fédéral estime qu'il n'y a pas lieu de modifier la procédure actuelle. Tous les éléments mentionnés dans la recommandation – nécessité, objectif, coûts, risques – sont contrôlés dans le cadre de la mise en place de liaisons «on line» et le PFPD a accès à toutes ces informations. Le PFPD fixe lui-même son programme de contrôle et décide s'il est opportun de procéder à des contrôles systématiques ou s'il est préférable de procéder par pointage. Ce faisant, il tient compte du principe de la proportionnalité.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation et veillera à ce que le PFPD obtienne toutes les informations nécessaires afin qu'il soit en mesure de contrôler les liaisons «on line» de manière plus appropriée.

3.3 Liaisons «on line»: transparence dans les messages du Conseil fédéral

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

Cette exigence n'est pas nouvelle. En effet, selon l'art. 3, al. 3 LOGA[5], entré en vigueur le 1er octobre 1997, l'activité du Conseil fédéral et de l'administration vise à atteindre les objectifs fixés et répond aux critères d'une bonne gestion. C'est d'ailleurs par souci d'opportunité et de rentabilité que le Conseil fédéral souhaite que dorénavant une attention toute particulière soit attachée à la compatibilité informatique de chaque projet de loi ou d'ordonnance. Cela signifie qu'il faut non seulement tenir compte des applications informatiques existantes ou projetées, mais encore des communications de données et des liaisons «on line». Jusqu'à présent le Conseil fédéral s'est toujours efforcé de remplir les conditions fixées dans la recommandation et d'indiquer dans ses messages toutes les précisions sur les accès envisagés, tant au niveau de leur nécessité et de leur finalité qu'au niveau de leur proportionnalité et de leur étendue, ainsi que sur les autorités auxquelles les accès seraient octroyés. D'ailleurs l'art. 19, al. 3, LPD stipule que lorsqu'une autorité rend accessible au moyen d'une procédure d'appel des données sensibles ou des profils de la personnalité, cela doit être prévu expressément dans une loi au sens formel. A l'avenir, le Conseil fédéral veillera à ce que ses messages reflètent la plus grande transparence possible quant aux liaisons «on line» en préparation.

S'il est possible de transmettre au Parlement des informations qualitatives sur les liaisons «on line» envisagées, il est beaucoup plus difficile de communiquer des informations quantitatives sans avoir procédé préalablement à une exploitation pilote permettant de mieux cerner les besoins réels des utilisateurs potentiels.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation.

3.4 Collaboration et coordination entre la Confédération et les cantons

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

Le Conseil fédéral est conscient du problème soulevé par la recommandation. Nous nous trouvons ici face à un dilemme. Faut-il que la Confédération adopte une réglementation contraignante et peut-être excessive ou faut-il, par souci de fédéralisme, laisser aux cantons le soin de choisir la procédure la mieux adaptée à leur sensibilité politique. Comme la protection des données exige que les liaisons «on line» soient expressément prévues dans les lois et ordonnances (art. 19, al. 3, LPD), chaque fois

5 Loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA; RS **172.010**).

qu'une telle liaison se révélait nécessaire après avoir été examinée sous l'angle de l'opportunité, de la proportionnalité et de la finalité, le législateur fédéral a jusqu'à présent rempli cette exigence en édictant des dispositions autorisant les autorités cantonales à accéder aux systèmes informatiques de la Confédération. Cela étant, les autorités fédérales chargées de la mise en place des liaisons «on line» ne se sont jusqu'ici guère préoccupées de savoir de quelle manière le pouvoir politique cantonal, de son côté, avait approuvé les demandes de raccordement qui leur étaient présentées.

Il apparaît difficile que la Confédération impose une procédure décisionnelle uniforme aux cantons. Le Conseil fédéral estime cependant qu'il est nécessaire que les autorités cantonales prennent une décision politique pour approuver les règles relatives au traitement des données, comme p. ex. le règlement de traitement propre à une application, et l'ampleur des contrôles à effectuer par la Confédération. Cette question mérite d'être examinée avec la Conférence des chefs des département cantonaux de justice et police (CCDJP). Le DFJP transmettra la recommandation à la CCDJP afin que cet objet puisse être porté à l'ordre du jour d'une prochaine réunion.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation conformément aux considérations qui précèdent.

3.5 Procédures d'autorisation pour des liaisons «on line» Principes de base

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

Le Conseil fédéral est d'accord qu'il est nécessaire de fixer des principes de base pour le traitement des demandes d'autorisation relatives à la mise en place des liaisons «on line» dans le domaine de la police. Il estime cependant que cette tâche peut être confiée au département et qu'il n'est pas nécessaire d'édicter ces principes en complétant l'OLPD[6].

Cette recommandation doit être traitée en liaison étroite avec la recommandation précédente.

Avis du Conseil fédéral:

Le Conseil fédéral charge le DFJP d'élaborer un projet de réglementation s'inspirant de cette recommandation et de le soumettre à la CCDJP.

6 Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD, RS **235.11**).

3.6 Contrôle des normes de délégation

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

L'octroi des autorisations d'accès «on line» est une procédure comprenant plusieurs niveaux décisionnels:

a. La décision de principe de raccorder une autorité (p. ex. l'autorité cantonale de police chargée de la lutte contre le trafic illicite de stupéfiants) est prise par le législateur fédéral au niveau de la loi si l'accès permet de consulter des données sensibles ou des profils de la personnalité. Dans les autres cas, la décision de principe est prise au niveau d'une ordonnance du Conseil fédéral.

b. La décision de raccorder un canton déterminé à une application informatique de la Confédération fait l'objet d'un accord entre les autorités politiques de la Confédération et des cantons (cf. recommandation 3.4).

c. Enfin, un troisième type de décision concerne l'autorisation accordée à une personne déterminée d'accéder par le biais d'une liaison «on line» à une application informatique de la Confédération lorsque cette personne appartient à une autorité mentionnée dans la loi ou l'ordonnance.

La présente recommandation concerne ce troisième type de décision, c'est-à-dire les autorisations accordées aux utilisateurs. Le Conseil fédéral n'est pas opposé à ce qu'une instance concédante adéquate et indépendante examine les demandes d'autorisation en faveur des utilisateurs. Il est par contre sceptique si la recommandation de la CdG-CE tend à charger une instance hiérarchiquement trop éloignée de l'application d'octroyer ces autorisations. En effet, une personne étrangère à l'office responsable de l'application ne connaît ni le service concerné, ni les personnes qui collaborent avec celui-ci. Elle devra exiger un dossier complet pour être à même d'apprécier si tel fonctionnaire cantonal peut être autorisé à accéder à l'application. Nommer une instance concédante au niveau du département impliquerait une charge de travail supplémentaire importante pour la préparation des demandes d'autorisation sans obtenir en contrepartie la garantie que l'instance concédante décide en connaissance de cause. D'autre part, une telle solution ne serait pas suffisamment souple pour que les mutations courantes (changements de fonction, démissions, absences prolongées) puissent être traitées rapidement.

Par contre, le Conseil fédéral estime qu'une solution devrait être trouvée au sein des offices responsables des applications. S'il appartient en principe au maître du fichier de décider qui peut être raccordé à une application, la décision de raccorder un utilisateur déterminé pourrait être examinée par le conseiller à la protection des données de l'office ou par toute autre personne n'étant pas directement concernée par l'application. Conformément aux règles approuvées par les autorités politiques cantonales (cf. recommandation 3.4), ces personnes devraient être également chargées de contrôler régulièrement que les raccordements installés correspondent aux autorisations accordées.

Avis du Conseil fédéral:

Le Conseil fédéral charge les départements d'adopter une réglementation des compétences pour l'octroi des autorisations d'accès „on line„ à leurs propres applications informatiques.

3.7 Contrôle du respect des normes de sécurité

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

Diverses dispositions légales fixent déjà que le droit fédéral sur la protection des données s'applique lorsque les cantons traitent des données personnelles en exécution du droit fédéral. Cela est le cas pour les cantons qui ne disposent pas de dispositions cantonales de protection des données (art. 37, al. 1 LPD) et pour les traitements de données exécutés en vertu de la LMSI (art. 16, al. 3 LMSI).La loi sur les offices centraux[7] stipule d'autre part que l'accès des cantons au systèmes de traitement des données est lié à la prise de mesures de protection et de sécurité (art. 12, al. 1). Cette dernière disposition donne implicitement la compétence aux offices centraux de contrôler les mesures prises par les autorités cantonales qui participent au système de traitement des données. Pour les autres traitements de données, le Conseil fédéral estime que la compétence de contrôler que les utilisateurs cantonaux et communaux respectent les mesures de sécurité ordonnées par l'organe responsable de l'application devrait figurer dans un premier temps dans l'ordonnance réglant le traitement des données personnelles de chaque application. Il convient de préciser qu'en raison de la charge de travail engendrée par ces contrôles, il ne pourra s'agir que de contrôles ponctuels et qu'il serait illusoire de prévoir des contrôles systématiques.

Le principe même de tels contrôles devrait cependant être discuté préalablement au sein de la CCDJP. Selon l'art. 37, al. 2, LPD, les cantons doivent désigner un organe chargé de veiller au respect de la protection des données. Les contrôles des mesures de sécurité informatiques pourraient par exemple être exécutés par ces organes désignés par les cantons sur mandat de l'organe fédéral responsable de l'application qui déterminerait lui-même les points à contrôler. Les organes cantonaux de contrôle pourraient se faire accompagner, si nécessaire, par des spécialistes fédéraux de la sécurité informatique. Leurs rapports seraient adressés conjointement au canton concerné et au responsable fédéral de l'application. Une modification de l'art. 37 LPD permettrait d'ancrer plus précisément de tels contrôles au niveau de la loi.

Avis du Conseil fédéral:

Le Conseil fédéral approuve le principe de cette recommandation et charge le DFJP de proposer des solutions pour sa réalisation.

[7] Loi fédérale du 7 octobre 1994 sur les offices centraux de police criminelle de la Confédération (RS **172.213.71**).

3.8 Normes pour les demandes d'autorisation

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

Il faut tout d'abord relever qu'une telle recommandation ne devrait pas s'appliquer au seul domaine de la police, mais à tous les secteurs administratifs. En effet, jusqu'ici les responsables de chaque application informatique ayant des liaisons „on line„ ont défini leur propre procédure pour les demandes d'autorisation relatives à de nouveaux utilisateurs. Le Conseil fédéral est d'accord d'examiner s'il y a lieu d'harmoniser les procédures dans ce domaine.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation et charge le DFJP de préparer des normes réglant la procédure des autorisations de liaisons «on line».

3.9 Contrôle de la fréquence d'utilisation

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

Techniquement rien ne s'oppose à ce que la fréquence d'utilisation des liaisons «on line» soit déterminée au moyen de contrôles réguliers. En effet, toutes les applications informatiques dans le domaine de la police disposent d'une fonction de journalisation conformément à l'art. 10 de l'OLPD. En pratique cela signifie que le système journalise chaque accès à une banque de données en enregistrant l'auteur, la date, l'heure et le libellé de la question. Pour des raisons de protection des données, ces procès-verbaux de journalisation ne sont pour l'instant accessibles qu'aux seuls organes ou personnes chargées de vérifier l'application des dispositions de protection des données personnelles et ils ne sont utilisés qu'à cette fin (art. 10, al. 2, OLPD). Une modification de cette disposition permettrait d'utiliser les données contenues dans les procès-verbaux de journalisation aux fins demandées par la CdG-CE, mais elle impliquerait un contrôle de la quantité des recherches effectuées par chaque utilisateur. Le Conseil fédéral consultera le PFPD pour déterminer comment procéder pour connaître la fréquence d'utilisation des liaisons «on line» sans exercer une surveillance exagérée de l'activité des utilisateurs.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation conformément aux considérations qui précèdent.

3.10 Collaborateurs du Centre de calcul du DFJP. Contrôle de sécurité

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

La LMSI prévoit à l'art. 19, al. 1, let. e, que des contrôles de sécurité peuvent être effectués à l'égard d'agents de la Confédération qui ont régulièrement accès à des données personnelles sensibles, dont la révélation pourrait porter gravement atteinte aux droits individuels des personnes concernées. Sur la base de cette disposition, il serait possible de soumettre les collaboratrices et collaborateurs du centre de calcul du DFJP à des contrôles de sécurité. L'art. 19, al. 2, LMSI autorise également les cantons à assujettir leurs agents à des contrôles de sécurité lorsqu'ils coopèrent directement à des tâches visant au maintien de la sûreté intérieure.

Le 20 janvier 1999, le Conseil fédéral a adopté une ordonnance relative aux contrôles de sécurité relatifs aux personnes[8] basée sur les art. 19, 21 et 30 de la LMSI. Par contre la liste des fonctions exigeant un contrôle n'a pas encore été arrêtée par le Conseil fédéral; elle devrait l'être au milieu de l'année. Le projet mentionne explicitement les collaboratrices et collaborateurs du Centre de calcul DFJP. Les contrôles demandés par votre recommandation seront exécutés dès que la liste des fonctions aura été approuvée.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation.

3.11 Emplacement du Centre de calcul du DFJP

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

La CdG-CE et le rapport d'expert rendent attentif aux problèmes de sécurité posés par le site du centre de calcul du DFJP. Ce problème est connu du DFJP qui a demandé en 1995 à des consultants spécialistes en matière de sécurité d'établir une liste des risques inhérents au site de Zollikofen. Le rapport indique clairement qu'il n'est pratiquement pas possible d'obtenir le niveau de sécurité souhaitable à cet emplacement. Les instances chargées de la sécurité physique des bâtiments, ainsi que l'expert qui a rédigé le rapport commandé par la CdG-CE, ont été informés des conclusions des consultants mandatés par le DFJP.

Dans le cadre du projet NOVE-IT[9], la proposition d'installer les ordinateurs du centre de calcul du DFJP dans les locaux informatiques du DDPS tout en garantissant une séparation totale entre les équipements informatiques des deux départements a été approuvée par le Conseil fédéral. Les équipements du DFJP y seront exploités par un groupe d'exploitation placé sous la responsabilité du DFJP. La date du déménagement n'a pas encore été fixée; le transfert devrait se faire par étapes en tenant compte du programme de renouvellement des équipements informatiques du DFJP. Le Centre de calcul du DFJP sera installé dans un lieu plus approprié dès que le programme de renouvellement des équipements informatiques du DFJP permettra de réaliser ce déménagement sans mettre en danger l'exploitation des systèmes existants et sans engendrer des coûts exorbitants.

8 Ordonnance du 20 janvier 1999 sur les contrôles de sécurité relatifs aux personnes (OCSP, RS **120.4**)
9 Réorganisation de l'informatique dans l'administration fédérale.

Avis du Conseil fédéral:

Le Conseil fédéral adopte la recommandation.

3.12 Fusion de KOMBV-KTV et DFJP-WAN

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

Le réseau KOMBV-KTV[10] est basé sur le protocole TCP/IP[11] qui relie entre eux tous les réseaux cantonaux et qui permet d'accéder à des applications cantonales ainsi qu'à des applications de l'administration fédérale (connexion de chacun avec chacun). Il est possible d'établir des liaisons ouvertes reliant directement chaque partenaire au sein des cantons (y compris au sein des hautes écoles); sous certaines conditions cela est également possible avec des réseaux externes.

Le DFJP-WAN[12] (ATM-Backbone) consitue un système de communication en forme d'étoile qui relie le CC DFJP à ses 26 partenaires. Les communications transitant par ce système ont lieu exclusivement entre les autorités cantonales concernées et le CC DFJP; elles ne relient jamais les partenaires entre eux ou avec des réseaux externes comme Internet. Le DFJP-WAN peut donc être considéré comme un ensemble de réseaux individuels fermés basés sur le protocole TCP/IP. Il permet d'accorder aux autorités de justice et police des cantons un accès sélectif aux applications informatiques du DFJP.

L'infrastructure de télécommunication KOMBV3 (réseau ATM de Swisscom) que l'OFI met en place depuis 1996 est utilisée par le DFJP-WAN comme support de communication à longue distance. Une migration vers KOMBV3 tenant compte de critères économiques et de disponibilité est progressivement en cours (fusion physique). Pour des raisons d'exploitation et de sécurité, les informations de police et celles relevant de la protection de l'Etat y sont cependant diffusées au sein du DFJP-WAN (qui est basé sur le support de communication KOMBV3) par le biais de sous-réseaux fermés, séparés logiquement les uns des autres. Cette conception des réseaux logiquement indépendants, mise en application par le DFJP, est également utilisée par de grandes organisations dont les tâches sont comparables à celles du DFJP. Le BKA (Bundeskriminalamt) exploite un réseau de police logiquement indépendant s'étendant à l'ensemble du pays. La Grande-Bretagne exploite le PNN (Police National Network) et aux Etats-Unis le FBI dispose du CJIS WAN (Criminal Justice Information System Wide Area Network) et du NLETS (National Law Enforcement Telecommunications System).

Le DFJP a commandé une expertise relative à la fusion des réseaux DFJP-WAN et KOMBV-KTV. Le Conseil fédéral doit encore examiner les résultats de cette étude qui met en évidence les avantages de la formation de sous-réseaux logiques du point de vue de la sécurité informatique. Il se prononcera définitivement sur l'opportunité

10 Communication entre l'administration fédérale et le réseau d'interconnexion cantonale (Kommunikation der Bundesverwaltung – Kantonverbund).
11 Protocole de contrôle des transmissions/protocole Internet (TCPIP, Transmission Control Protocol/Internet Protocol).
12 Réseau étendu du DFJP (WAN, Wide-Area-Network).

d'opérer une fusion de KOMBV-KTV et de DFJP-WAN lorsqu'il aura analysé les résultats de cette expertise.

Avis du Conseil fédéral:

Le Conseil fédéral accepte la recommandation.

4 Rapport d'expert du 30 juillet 1998

Le Conseil fédéral ne souhaite pas se prononcer sur chaque recommandation du rapport d'expert car la plupart d'entre elles sont pertinentes. Les recommandations les plus importantes ont d'ailleurs été adoptées par la CdG-CE. Certains points méritent cependant d'être soulevés.

4.1 Principes régissant les accès «on line»

Les principes régissant les accès «on line» constituent un excellent résumé des différents points à prendre en considération avant de mettre en place de telles liaisons. Les récapitulations de l'expert mandaté par la CdG-CE permettent de disposer de listes de contrôle très utiles.

4.2 Raccordement du centre de calcul aux applications dont il assure l'exploitation.

L'expert relève que pour des raisons d'exploitation et de maintenance 26 raccordements ont été mis en place entre le centre de calcul DFJP (CC DFJP) et une application. Il estime qu'aucune base juridique ne justifie ces raccordements et que leur nombre est exagéré. Il recommande au DFJP de créer une base légale suffisante pour l'accès des collaborateurs du CC DFJP à cette application.

Dans ce cas, le nombre de raccordements motivés par des raisons d'exploitation est effectivement élevé et a fait l'objet d'un contrôle interne. Le Conseil fédéral constate que les accès utilisés par les exploitants d'applications informatiques à des fins de maintenance et d'exploitation n'ont pas été traités de façon analogue dans toutes les ordonnances réglant les traitements de données personnelles. Bien que de tels accès «on line» existent pratiquement pour chaque application, ils y sont parfois mentionnées explicitement (p. ex. ordonnances DOSIS, ISOK et FAMP) alors que dans les autres cas le Conseil fédéral a estimé que la base légale de l'application couvre implicitement ce type de liaisons. En effet, ces accès sont inhérents à l'exploitation des systèmes et ils n'interviennent que pour examiner des erreurs de fonctionnement sur mandat de l'organe responsable de l'application.

Le Conseil fédéral consultera le Préposé fédéral à la protection des données afin de déterminer la manière la plus appropriée de régler le problème des accès «on line» accordés au centre de calcul à des fins de maintenance.