

06.046

**Message  
concernant la loi fédérale sur les systèmes d'information  
de police de la Confédération**

du 24 mai 2006

---

Messieurs les Présidents,  
Mesdames et Messieurs,

Par la présente, nous soumettons à votre approbation un projet de loi fédérale sur les systèmes d'information de police de la Confédération.

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames et Messieurs, l'assurance de notre haute considération.

24 mai 2006

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Moritz Leuenberger  
La chancelière de la Confédération, Annemarie Huber-Hotz

---

## Condensé

*Les objectifs de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP) sont les suivants:*

- 1. rassembler dans une même loi et actualiser les fondements légaux des systèmes de police existants, à savoir RIPOL (recherches informatisées de police), IPAS (données relatives aux personnes ayant fait l'objet d'un traitement signalétique ou d'une communication Interpol) et JANUS (données de la Police judiciaire fédérale traitées dans le cadre de procédures d'enquêtes ou d'investigations préliminaires en tant qu'Offices centraux de police criminelle), afin d'augmenter la transparence de ces systèmes, de les harmoniser dans une large mesure et d'obtenir des effets de synergie et de rationalisation;*
- 2. créer une base légale formelle pour l'index national de police; cet index est une sorte de répertoire qui rassemble les noms des personnes enregistrées dans diverses bases de données de police et permet ainsi aux autorités compétentes de déterminer rapidement, par une interrogation automatisée, si une personne est connue d'une autorité cantonale ou fédérale de police et quels sont les services disposant des données correspondantes;*
- 3. intégrer les nouveaux flux d'informations policières résultant de Schengen et d'Europol dans les systèmes existants;*
- 4. procéder à des modifications ponctuelles d'autres textes légaux afin de refléter les modifications de compétences intervenues au sein du Département fédéral de justice et police (DFJP) au cours des dernières années.*

*A l'exception de l'index national de police, qui est une sorte de répertoire des bases de données existantes, la LSIP ne crée pas de nouvelles bases de données de police. Au contraire, elle rassemble les systèmes d'information existants dans un seul acte de loi et crée un ensemble cohérent pour toutes les bases de données de police.*

## Table des matières

<b>Condensé</b>	<b>4820</b>
<b>1 Partie générale</b>	<b>4822</b>
1.1 Point de la situation	4822
1.2 Grandes lignes du projet de loi	4823
1.3 Résultats de la phase préliminaire	4824
1.3.1 Travaux préparatoires sur le plan fédéral	4824
1.3.2 Procédure de consultation	4825
1.3.3 Principales modifications par rapport à l'avant-projet	4826
<b>2 Partie spéciale</b>	<b>4826</b>
2.1 Introduction	4826
2.2 Commentaire	4827
2.2.1 Section 1: Dispositions générales	4827
2.2.2 Section 2: Réseau de systèmes d'information de police (art. 9 à 14)	4831
2.2.3 Section 3: Autres systèmes d'information de police	4835
2.2.4 Section 4: Dispositions finales	4840
2.3 Modification du droit en vigueur	4840
2.3.1 Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (art. 15)	4840
2.3.2 Loi fédérale du 21 mars 1981 sur l'entraide pénale internationale (nouvel art. 11a)	4841
2.3.3 Code pénal suisse	4843
2.3.4 Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération	4843
2.3.5 Loi fédérale du 10 octobre 1997 concernant la lutte contre le blanchiment d'argent dans le secteur financier	4843
<b>3 Conséquences</b>	<b>4844</b>
3.1 Conséquences pour la Confédération	4844
3.2 Conséquences pour les cantons et les communes	4845
3.3 Autres conséquences	4845
<b>4 Programme de la législation</b>	<b>4845</b>
<b>5 Bases juridiques</b>	<b>4846</b>
5.1 Constitutionnalité	4846
5.2 Rapports avec le droit européen	4846
5.3 Délégation de compétences législatives	4847
5.4 Forme de l'acte à adopter	4847
<b>Loi fédérale sur les systèmes d'information de police de la Confédération (Projet)</b>	<b>4849</b>

# Message

## 1 Partie générale

### 1.1 Point de la situation

L'Office fédéral de la police (ci-après fedpol) assume la responsabilité de divers systèmes d'information:

1. système de recherche informatisée de police ou RIPOL, art. 351<sup>bis</sup> du code pénal suisse (CP)<sup>1</sup>;
2. système automatisé d'identification des empreintes digitales ou AFIS, art. 351<sup>septies</sup> CP;
3. système d'information fondé sur les profils d'ADN, art. 10 ss de la loi fédérale du 20 juin 2003 sur les profils d'ADN<sup>2</sup>;
4. système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police ou IPAS, art. 351<sup>octies</sup> CP;
5. système informatisé des Offices centraux de police criminelle ou JANUS, art. 11 de la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC)<sup>3</sup>;
6. système d'information du Bureau de communication en matière de blanchiment d'argent ou GEWA, art. 35 de la loi fédérale du 10 octobre 1997 sur le blanchiment d'argent (LBA)<sup>4</sup>;
7. système de traitement des données relatives à la protection de l'Etat ou ISIS, art. 15 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)<sup>5</sup>;
8. système d'information en matière de documents d'identité ou ISA, art. 11 de la loi fédérale du 22 juin 2001 sur les documents d'identité (LDI)<sup>6</sup>.

Ces systèmes en partie à vocation policière ont connu d'importants développements depuis leur introduction à partir du début des années 1990. Pendant cette même période, la structure et les compétences de l'Office fédéral de la police ont subi de nombreux changements suite notamment au projet de restructuration du domaine policier de la Confédération («StruPol»). C'est ainsi que l'ancienne Police fédérale, rattachée au Ministère public de la Confédération, a été intégrée à l'Office fédéral de la police (aujourd'hui: fedpol), tandis que les secteurs du casier judiciaire fédéral, de l'entraide judiciaire internationale en matière pénale et de l'assistance aux Suisses de l'étranger ont été transférés à l'Office fédéral de la justice. D'autre part, suite à l'entrée en vigueur le 1<sup>er</sup> janvier 2002 de l'art. 340<sup>bis</sup> du code pénal, la Confédération assume de nouvelles compétences de poursuite pénale et fedpol s'est vu doté d'une Police judiciaire fédérale.

1 RS 311.0

2 RS 363

3 RS 360

4 RS 955.0

5 RS 120

6 RS 143.1

Enfin, avec l'entrée en vigueur au 1<sup>er</sup> mars 2006 de l'Accord entre la Confédération suisse et l'Office européen de police (Europol)<sup>7</sup> et l'acceptation des accords d'association de la Suisse à Schengen et Dublin<sup>8</sup>, la coopération policière avec les pays européens se trouve notablement renforcée. Il s'ensuit un flux plus important d'échanges d'informations policières qui doivent pouvoir être traitées dans les bases de données existantes ou dans de nouveaux systèmes.

## 1.2 Grandes lignes du projet de loi

Les développements des bases de données de police existantes, les modifications survenues au sein de fedpol et la mise sur pied d'un index national de police sont autant d'éléments qui ont amené le Conseil fédéral à estimer nécessaire l'élaboration d'un projet de loi sur les systèmes d'information de police de la Confédération (LSIP). Les objectifs de cette loi sont les suivants:

1. rassembler et actualiser dans une même loi les fondements légaux des systèmes de police existants, à savoir RIPOL, IPAS et JANUS, afin d'augmenter la transparence de ces systèmes, de les harmoniser dans une grande mesure et d'obtenir des effets de synergie et de rationalisation;
2. créer une base légale formelle pour l'index national de police;
3. intégrer les nouveaux flux d'informations policières résultant de Schengen et d'Europol dans les systèmes existants;
4. procéder à des modifications ponctuelles d'autres textes légaux afin de refléter les modifications de compétences au sein du DFJP.

Au sujet de l'objectif 1 ci-dessus, l'intégration dans la LSIP de plusieurs des systèmes placés sous la responsabilité de fedpol et mentionnés au ch. 1.1, a été écartée pour les raisons exposées ci-après:

- La base de données GEWA n'est pas à proprement parler un système de police. C'est un outil du Bureau de communication en matière de blanchiment d'argent, autorité administrative qui décide si les annonces des intermédiaires financiers doivent être transmises aux autorités de poursuite pénale. L'activité de cet autorité et son outil de travail doivent continuer d'être réelles dans la LBA<sup>9</sup>.

<sup>7</sup> RS 0.360.268.2

<sup>8</sup> Accord du 26.10.2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (RS ...); accord du ... entre la Confédération suisse et le Royaume du Danemark portant sur la création de droits et d'obligations entre ces Etats dans le domaine de la coopération Schengen (RS ...); accord du ... entre la Confédération suisse, la République d'Islande et le Royaume de Norvège sur la mise en œuvre, l'application et le développement de l'acquis de Schengen et sur les critères et les mécanismes permettant de déterminer l'Etat responsable de l'examen d'une demande d'asile introduite en Suisse, en Islande ou en Norvège (RS ...).

<sup>9</sup> RS 955.0

- ISIS est utilisé par les autorités chargées du maintien de la sûreté intérieure (tâches de protection de l’Etat, service de renseignements intérieurs) et son orientation préventive justifie une séparation nette avec les systèmes de police définis dans le présent projet, qui sont plus axés sur la répression.
- Le système d’information fondé sur les profils d’ADN est réglé de manière détaillée dans la loi fédérale du 20 juin 2003 sur les profils d’ADN<sup>10</sup>, acceptée par le parlement en 2003. Il ne paraît pas adéquat d’intégrer dans le présent projet les dispositions relatives au système d’information, de manière à ne pas tronquer une loi récemment votée de près de la moitié de sa substance.
- Quant à AFIS, il contient les images des empreintes digitales relevées tant lors de procédures d’enquête que dans le cadre de la législation sur les étrangers. Il apparaît opportun de ne régler dans la LSIP que le traitement des données personnelles liées aux empreintes relevées dans un contexte criminel<sup>11</sup>. Cela correspond à la situation actuelle, où les données dans le contexte criminel sont traitées dans IPAS et les données relatives aux étrangers le sont dans le système informatisé central sur la migration (SYMIC).
- ISA, système de gestion des documents d’identité, ne poursuit pas des objectifs de police, mais vise à permettre la gestion des passeports et cartes d’identité et à éviter leur usage abusif. Il sort ainsi du contexte du projet.

Dans le cadre de l’objectif 4 ci-dessus, une modification ponctuelle des bases légales du système d’information ISIS est proposée<sup>12</sup>. Par ailleurs, une base légale nouvelle est prévue pour un système d’information dans le domaine de l’entraide judiciaire en matière pénale<sup>13</sup>. Enfin, l’on propose un changement de la LBA<sup>14</sup>.

## **1.3 Résultats de la phase préliminaire**

### **1.3.1 Travaux préparatoires sur le plan fédéral**

Depuis la fin 1999, une organisation de projet commune du Département fédéral de justice et police (DFJP) et de la Conférence des directrices et directeurs cantonaux de justice et police (CCDJP) a procédé à un examen global du système de sûreté intérieure de la Suisse (projet USIS). C’est dans ce cadre que le DFJP et la CCDJP ont attribué un mandat visant à la création d’un index national de police. Cet index doit permettre aux autorités policières suisses de savoir si l’une d’entre elles traite des données sur une personne déterminée. Ce système a non seulement l’avantage d’accélérer les démarches d’entraide judiciaire et administrative, mais encore celui de permettre aux diverses autorités policières suisses de bénéficier du même niveau d’informations.

Partant de la nécessité de créer une base légale formelle pour l’index de police, et constatant le manque de cohérence entre les diverses bases légales régissant les bases de données policières, le DFJP a proposé d’élaborer une loi unique pour les

<sup>10</sup> RS 363

<sup>11</sup> A ce sujet, voir l’art. 14 du projet.

<sup>12</sup> Cf. ch. 2.3.1 ci-dessous.

<sup>13</sup> Cf. ch. 2.3.2 ci-dessous.

<sup>14</sup> Cf. ch. 2.3.5 ci-dessous.

systèmes d'information de police de la Confédération, y compris l'index de police. L'avant-projet élaboré par l'administration a été mis en consultation au cours du premier semestre 2005.

### 1.3.2 Procédure de consultation

Le projet de loi a été dans l'ensemble accueilli positivement, même si certains principes et points de détail ont fait l'objet de critiques parfois importantes. L'ensemble des autorités et organisations ayant répondu à la consultation a approuvé le projet dans ses principes. Certains cantons ont émis des réserves quant à leur participation à l'index national de police, dans la mesure où les coûts ne sont pas encore définis avec suffisamment de clarté et où il n'est pas encore acquis que tous les cantons participeront effectivement à l'index.

La nécessité de légiférer dans le domaine des bases de données de police n'a pas été remise en cause, pas plus que la création d'un réseau de systèmes d'information de police, la mise sur pied d'un index national de police ainsi que l'utilisation du RIPOL pour prévenir l'enlèvement international d'enfants. En fait, à l'exception de l'extension du système du droit indirect aux renseignements dans le cadre de procédures d'enquête ouvertes par le Ministère public de la Confédération (projet de modification de la loi fédérale du 15 juin 1934 sur la procédure pénale, PPF<sup>15</sup>), aucune des options fondamentales du projet de loi n'a rencontré une opposition nette ou le rejet par une majorité des cantons, des partis politiques et des organisations intéressées.

La quasi-totalité des organismes ayant répondu dans le cadre de la consultation s'est prononcée en détail sur le projet de créer un index national de police. Cet index est le seul système véritablement nouveau proposé dans le projet de LSIP. En ce qui concerne les cantons, qui sont touchés au premier chef, on constate d'une part un soutien au projet, mais aussi une réelle préoccupation quant aux répercussions financières et techniques, ainsi qu'aux conséquences sur les recherches de police si l'ensemble des cantons n'adhérait pas à l'index. On peut également relever le souci de certains cantons d'harmoniser leurs systèmes informatiques et de permettre un accès simplifié aux informations au niveau national afin de se préparer à l'espace Schengen. Certains participants à la consultation ont en outre exprimé le vœu que le système de la LSIP soit bien compatible avec nos engagements en vertu des accords bilatéraux avec l'Union européenne. Du point de vue des partis politiques, l'index rencontre un net soutien, à la condition que tous les cantons y participent.

Considérant que l'art. 14, al. 2 à 4, de la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC)<sup>16</sup> est repris à l'art. 8 LSIP, le principe dit du «droit d'accès indirect» est maintenu pour le droit aux renseignements des particuliers dans le système «infractions fédérales» de la PJF, système correspondant à la base de donnée JANUS actuelle. Lorsqu'un particulier exerce son droit aux renseignements pour ce système, il reçoit du Préposé fédéral à la protection des données et à la transparence (FPDPT) une réponse au libellé toujours identique selon laquelle aucune donnée le concernant n'a été traitée illégalement, ou que le FPDPT a adressé à l'autorité compétente la recommandation de

<sup>15</sup> RS 312.0

<sup>16</sup> RS 360

remédier à une erreur commise dans le traitement des données. Le droit d'accès indirect représente un compromis entre les intérêts de la poursuite pénale et la protection des droits fondamentaux des individus. Il a été conçu dans le cadre des débats parlementaires relatifs à la LOC et à la LMSI. Une majorité de cantons et tous les partis ayant répondu à la consultation, dont les quatre partis gouvernementaux, ne sont pas opposés au droit d'accès indirect tel qu'il existe aujourd'hui. Il en va différemment du projet d'étendre ce mode de droit d'accès aux procédures d'enquête ouvertes par le Ministère public de la Confédération, que 6 cantons ont expressément rejeté, alors que seuls 3 cantons soutiennent de manière générale le droit indirect aux renseignements tel que proposé dans l'avant-projet.

### **1.3.3 Principales modifications par rapport à l'avant-projet**

Les modifications principales sont les suivantes:

- renoncement à modifier la loi fédérale sur la procédure pénale (PPF)<sup>17</sup> en ce qui concerne le droit aux renseignements des particuliers pour les données traitées par la police judiciaire;
- intégration des échanges d'information résultant de Schengen et d'Europol dans les bases de données de police existantes;
- reprise de l'article du CP traitant de la partie nationale du système d'information Schengen (N-SIS);
- possibilité pour la Confédération de fixer des critères de saisie des données cantonales dans l'index national de police (catalogue de délits, par exemple).

Au demeurant, la structure générale du projet n'a subi aucune modification majeure et les principes généraux de traitement des données demeurent les mêmes.

## **2 Partie spéciale**

### **2.1 Introduction**

Comme évoqué au ch. 1.2, la LSIP régleme le l'utilisation des systèmes de police de la Confédération. Ces systèmes sont le réseau de systèmes d'information de police, le système de recherches informatisées de personnes et d'objets, la partie nationale du système d'information Schengen (N-SIS), le système interne de gestion des affaires et des documents de fedpol et l'index national de police. Hormis l'index de police et le N-SIS, ces systèmes d'information existent déjà depuis plusieurs années et disposent d'une base légale formelle. Sous réserve de l'index, la LSIP n'introduit dès lors pas à proprement parler de nouvelles bases de données, mais actualise uniquement les bases légales existantes. En ce qui concerne le N-SIS, la base légale formelle acceptée par le peuple en votation populaire du 5 juin 2005<sup>18</sup> a simplement été transférée dans la LSIP.

<sup>17</sup> RS 312.0

<sup>18</sup> FF 2004 6709 ss (l'art. sur le N-SIS y figure comme art. 351<sup>decies</sup> CP)



Pour chaque système d'information, sont déterminés dans la loi le but du traitement des données et le type de données, les principes du traitement des données, les autorités habilitées à accéder à ces données et le droit des particuliers de savoir si des informations sont traitées à leur sujet. D'autres éléments de détail seront réglés dans des ordonnances d'application<sup>19</sup>.

## **2.2                      Commentaire**

### **2.2.1                  Section 1: Dispositions générales**

#### *Art. 1                  Objet*

Cet article décrit l'objet de la loi, à savoir régler les fondements des systèmes d'information de police énumérés à l'art. 2.

#### *Art. 2                  Champ d'application*

Cet article énumère les systèmes d'information traités par le projet de loi. L'énumération est exhaustive.

#### *Art. 3                  Principes*

Les utilisateurs principaux des systèmes d'information de police sont les autorités de poursuite pénale, de police et de maintien de la sûreté intérieure. Les systèmes d'information ont pour but d'assister ces autorités dans l'accomplissement des tâches qui leur sont attribuées par la loi (al. 1). En ce qui concerne les autorités de maintien de la sûreté intérieure, il s'agit de rappeler que leur ressource principale est le système ISIS, prévu par la LMSI<sup>20</sup>. Cela ne doit toutefois pas les empêcher de consulter ponctuellement les systèmes d'information de police prévus par la LSIP lorsqu'elles en ont besoin pour accomplir leurs tâches légales.

L'al. 2 énonce de manière générale le fait que les autorités de police sont habilitées à traiter des données sensibles et des profils de la personnalité dans les systèmes d'information de police. La présente disposition vise à satisfaire l'exigence de l'art. 17, al. 2, de la loi fédérale du 12 juin 1992 sur la protection des données (LPD)<sup>21</sup> qui prévoit que de telles données ne peuvent être traitées que si une loi au sens formel le prévoit expressément. Il ne s'agit toutefois pas ici d'une autorisation générale de traiter des données sensibles; ces données ne pourront être traitées dans un système particulier que si l'accomplissement des tâches légales l'exige et que cela correspond aux buts et aux dispositions spécifiques du système. Les autorisations d'accès des diverses autorités aux différents systèmes d'information de police sont d'ailleurs fixées de manière détaillée dans les sections 2 et 3 du projet.

<sup>19</sup> Cf. ch. 2.2.4 et 5.3 ci-dessous

<sup>20</sup> RS 120

<sup>21</sup> RS 235.1

*Art. 4*            Traitement de données dans le cadre de la coopération policière internationale

Cet article a pour objet de montrer plus clairement que le travail de police dépend également et de plus en plus de la collaboration avec l'étranger. Les autorités de police de la Confédération sont déjà habilitées à échanger des informations avec l'étranger<sup>22</sup>. L'art. 4 du projet vise à renforcer les dispositions existantes et à autoriser expressément la Confédération à traiter les données afférentes à la collaboration internationale dans les systèmes d'information de police. Il prévoit par ailleurs la possibilité d'un accès en ligne d'autorités étrangères ou d'organisations internationales aux systèmes d'information suisses, pour autant qu'une base légale expresse existe. Ce principe général réaffirme une possibilité déjà existante<sup>23</sup> et permet d'envisager de nouveaux accès à l'avenir.

A l'heure actuelle, une lutte efficace contre la criminalité ne peut plus s'envisager sans une coopération internationale renforcée, au besoin par le biais d'échanges d'informations automatisés. L'art. 4 anticipe dès lors l'évolution probable du travail de police, qui tend de plus en plus à une intensification de la collaboration avec l'étranger, notamment dans la lutte contre la criminalité transfrontalière. Le projet de LSIP intègre déjà les modalités du traitement des données issues de l'échange d'informations dans le cadre de Schengen et d'Europol, mais vise également à laisser la porte ouverte à d'autres formes de coopération prévues par un accord international.

*Art. 5*            Traitement de données à des fins de contrôle et de maintenance

Les autorisations de consulter les informations, ou accès en ligne, varient d'un système à l'autre, en fonction des besoins et des tâches légales des autorités concernées. L'art. 5 fixe cependant de manière générale le droit des organes internes de contrôle et des personnes chargées de la maintenance informatique d'accéder aux systèmes d'information de police, leur permettant ainsi d'effectuer correctement leur travail. Cette disposition a été insérée dans la partie générale afin d'éviter une répétition aux articles concernant chaque système d'information.

*Art. 6*            Conservation, effacement, archivage et destruction des données

Cet article rappelle un des principes de la protection des données, selon lequel les données ne doivent être conservées qu'aussi longtemps que le but du traitement l'exige. Des durées maximales de conservation sont par ailleurs prévues. Elles diffèrent pour chaque système d'information et sont réglées dans des dispositions spéciales, au niveau d'une ordonnance d'application (cf. art. 19, let. d). L'art. 6 prévoit en sus que la conservation des données doit être réglée selon un procédé bien défini:

<sup>22</sup> Cf. par exemple art. 2, let. a, b, d et e, LOC, RS **360**, et art. 4 à 8 de l'accord entre la Confédération suisse, la République d'Autriche et la Principauté du Liechtenstein concernant la coopération transfrontalière des autorités compétentes en matière de sécurité et de douane, RS **0.360.163.1**.

<sup>23</sup> Cf. par exemple art. 351<sup>bis</sup> al. 3 let. e CP (possibilité pour les organes d'Interpol de consulter en ligne des données du RIPOL)

- Pour les systèmes d’information de police appliquant le procédé de l’al. 1, let. a, chaque donnée a un délai de conservation individuel à l’issue duquel un effacement a lieu, indépendamment d’éventuels liens avec d’autres informations (procédé «statique»).
- Selon l’al. 1, let. b, (procédé «dynamique» ou historique), toute donnée a également un délai de conservation maximal fixe. Toutefois, si une nouvelle information liée à la donnée initiale est inscrite dans le système, un lien entre les deux peut être effectué, créant un bloc de données dont la durée de conservation globale est prolongée.

Lorsqu’on applique le système dynamique ou historique, une appréciation générale des données doit en outre être effectuée à intervalles réguliers (al. 2). Cette appréciation effectuée par un service spécialisé de fedpol<sup>24</sup> permet d’évaluer chaque bloc de données et de détruire ou de rendre anonymes des données qui respectent certes le délai maximal de conservation, mais sont devenues inutiles au regard de la finalité du traitement de l’information.

L’al. 4 reflète les principes de la loi fédérale du 26 juin 1998 sur l’archivage<sup>25</sup>.

#### *Art. 7* Droit aux renseignements pour les particuliers

L’al. 1 pose le principe général qui découle de l’art. 8 LPD, à savoir que toute personne est autorisée à demander au maître du fichier si des informations la concernant sont traitées dans un système d’information de police. De manière générale, fedpol est désigné comme interlocuteur pour tous les systèmes d’information de police. Le reste de l’article et l’art. 8 sont consacrés aux différentes modalités applicables selon le système visé.

L’al. 2 prévoit que fedpol transmet les demandes de droit d’accès au Ministère public de la Confédération pour ce qui concerne le système contenant les données relatives à des procédures d’enquête de police judiciaire de la Confédération (art. 10), soumis aux règles de la procédure pénale fédérale<sup>26</sup>. Les demandes concernant le système contenant les données traitées par la Police judiciaire fédérale en dehors d’une procédure pénale (infractions fédérales; cf. art. 11) sont quant à elles transmises au Préposé fédéral à la protection des données et à la transparence. Elles sont traitées conformément à l’art. 8 du projet. Les demandes concernant les données des cantons selon l’art. 13 du projet de loi doivent être adressées directement à ceux-ci et sont traitées conformément au droit cantonal.

L’al. 4 concerne les données traitées dans les systèmes coopération policière internationale et intercantonale (art. 12), identification (art. 14), recherches informatisées de police (art. 15), N-SIS (art. 16), dans l’index national de police (art. 17) et dans le système de gestion de fedpol (art. 18). Le droit d’accès s’effectue conformément à la LPD. Fedpol statue sur la demande après avoir consulté l’autorité source de l’information. La LPD est applicable, ce qui inclut les motifs de refus prévus à l’art. 9 de cette loi. Dans tous les cas, le secret de l’enquête pénale doit être garanti.

<sup>24</sup> Cf. p.ex. art. 14 de l’ordonnance JANUS (RS **360.2**) pour le système JANUS actuel.

<sup>25</sup> RS **152.1**

<sup>26</sup> Art. 102<sup>bis</sup> PPF

Cet article régit les demandes relatives aux traitements de données dans le système visé à l'art. 11 (système infractions fédérales). Il reprend l'art. 14 al. 2 à 4 LOC actuellement en vigueur et maintient ainsi le régime dit du «droit d'accès indirect». Selon ce procédé, la personne qui demande si des données sont traitées à son sujet reçoit du Préposé fédéral à la protection des données et à la transparence (PF PDT) une réponse toujours identique selon laquelle une vérification a été opérée par ses soins et qu'aucune donnée n'a été traitée illégalement ou qu'une recommandation a été adressée au service compétent en vue de remédier à une erreur commise dans le traitement des données. La personne intéressée n'est ainsi pas en mesure de savoir si des données sont effectivement traitées à son sujet ou non. Elle dispose en revanche du droit de saisir le Tribunal administratif fédéral, qui vérifiera à son tour le travail du PF PDT.

Pour le PF PDT, ce régime n'est pas satisfaisant dans la mesure où il ne correspond pas à un vrai droit d'accès. En particulier, le PF PDT, qui exerce le droit d'accès par représentation, ne peut pas juger si d'éventuelles informations sont exactes, ce qui prive la personne concernée de son droit de rectification. Il souhaiterait dès lors remplacer le régime actuel par un droit d'accès direct.

Les arguments du PF PDT peuvent être réfutés comme suit: en instituant un droit d'accès direct pour le système d'information de la Police judiciaire fédérale, le secret des enquêtes ne serait plus garanti et le travail de police pourrait ainsi être menacé. Avec le droit d'accès indirect, également applicable aux traitements de données dans le domaine du renseignement intérieur, le législateur a voulu éviter que les acteurs de la grande criminalité puissent savoir si la PJF est en train de procéder à une récolte d'informations permettant éventuellement de découvrir des organisations criminelles secrètes. En remplaçant le droit d'accès indirect par un droit aux renseignements direct, on permettrait aux milieux criminels d'accéder à une telle information. En effet, il est possible de refuser une demande de renseignements directe, mais un tel refus doit être motivé. Or le simple fait de refuser l'information peut indiquer au requérant qu'un traitement de données à son sujet est en cours, ce que le législateur a voulu éviter.

Au demeurant, le droit d'accès est limité au système «infractions fédérales» de la PJF, qui sert notamment à la détection des organisations criminelles et à la lutte contre les infractions qu'elles commettent<sup>27</sup>. Dès qu'une procédure pénale est ouverte contre une personne ayant fait l'objet d'un traitement de données par la PJF, le droit direct aux renseignements s'applique. Le droit d'accès indirect prévu par la LSIP est donc conforme à la proportionnalité, ne serait-ce qu'en raison de son champ d'application limité.

Le Conseil fédéral considère donc que la réglementation actuelle représente un bon compromis entre les intérêts de la protection des données et ceux de la police; c'est pourquoi il souhaite la reprendre telle quelle dans la LSIP. Cette réglementation est par ailleurs similaire à la solution adoptée par d'autres pays européens<sup>28</sup>.

<sup>27</sup> A ce sujet, voir le commentaire de l'art. 11

<sup>28</sup> Par exemple la France, qui prévoit un contrôle indirect par la Commission nationale de l'informatique et des libertés (C.N.I.L.) pour certaines bases de données.

Hormis le système de droit indirect aux renseignements, prévu par le présent article, la LPD<sup>29</sup> est applicable aux systèmes d'information de police, lorsque la LSIP ou la PPF<sup>30</sup> ne prévoient pas de dispositions spécifiques. On peut par exemple songer aux motifs de refus d'une demande de renseignements (art 9 LPD) ou à la possibilité pour les autorités fédérales de communiquer des données personnelles dans un cas d'espèce (art. 19 LPD).

## **2.2.2 Section 2: Réseau de systèmes d'information de police**

Les art. 9 à 14 constituent le cœur de la LSIP et définissent le réseau de systèmes d'information de police, outil principal de la Police judiciaire fédérale pour lutter contre la criminalité.

L'idée directrice de ce réseau consiste à réunir toutes les informations de police dans un système unique tout en distinguant différentes catégories de données. Chaque catégorie est soumise à un régime distinct et les autorités habilitées à accéder à ces catégories ne sont pas les mêmes. Le réseau recouvre les données actuellement traitées dans les systèmes JANUS et IPAS conformément aux art. 11 LOC et 351<sup>octies</sup> CP<sup>31</sup>. Le rapprochement entre ces deux systèmes figure à l'art. 9, al. 2, du projet: une seule interrogation permet de savoir si une personne figure dans un ou plusieurs systèmes d'information selon les art. 10 à 14 (procédures d'enquête, infractions fédérales, coopération policière internationale et intercantonale, enquêtes cantonales et identification), dans la mesure où la personne effectuant l'interrogation dispose des droits d'accès correspondants.

### *Art. 10*            Système d'appui aux enquêtes de police judiciaire de la Confédération

L'art. 10 concerne les données relatives aux enquêtes de police judiciaire de la Confédération. Après l'ouverture d'une procédure par le Ministère public de la Confédération, les actes de la Police judiciaire fédérale (PJF), rattachée à fedpol, sont régis par la PPF<sup>32</sup>, en particulier les art. 100 ss. Le système d'information prévu à l'art. 10 LSIP est destiné à recevoir toutes les données traitées par la PJF pendant cette phase procédurale. L'accès à ces informations est réservé aux autorités menant la procédure, à savoir la PJF et le Ministère public de la Confédération. Pour chaque procédure, l'accès peut également être restreint selon décision du Ministère public de la Confédération (art. 10, al. 5). Le Service d'analyse et de prévention de fedpol est également habilité à traiter des données dans le système pour des tâches particulières définies dans la loi.

### *Art. 11*            Système infractions fédérales

Le système institué par l'art. 11 doit servir d'outil à la PJF pour ses investigations préliminaires. Il s'agit là du traitement d'informations en dehors d'une procédure qui

<sup>29</sup> RS 235.1

<sup>30</sup> RS 312.0

<sup>31</sup> RS 311.0

<sup>32</sup> RS 312.0

est prévu par la LOC et les traités internationaux relatifs à la coopération policière<sup>33</sup> en ce qui concerne les infractions soumises à la juridiction fédérale<sup>34</sup> et les domaines d'activité des Offices centraux de police criminelle de la Confédération.

Le système infractions fédérales prévu par cet article correspond au système JANUS actuel, exploité par la PJF. L'art. 11 LSIP reprend dès lors l'art. 11 de la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC)<sup>35</sup>, qui est abrogé dans le présent projet. Les données contenues dans ce système sont récoltées par la PJF en sa qualité d'office central de police criminelle de la Confédération au sens de l'art. 1 de l'ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police<sup>36</sup>.

Les missions des offices centraux de police criminelle et la façon dont ils sont autorisés à obtenir les informations qui sont ensuite stockées dans le système infractions fédérales sont décrites aux art. 2, 3, 7 et 11 LOC. Dans le domaine de la lutte contre le crime organisé, selon l'art. 7, al. 1 et 2 de la LOC, les offices centraux ont pour mission de démasquer les organisations criminelles au sens de l'art. 260<sup>ter</sup> du Code pénal<sup>37</sup>, de découvrir les infractions économiques transnationales et, notamment, de combattre les délits que commettent les organisations criminelles.

Les activités de détection précoce des formes les plus graves de la criminalité justifient la possibilité pour les offices centraux de traiter des données à l'insu des personnes concernées et notamment le régime très particulier du droit d'accès indirect<sup>38</sup>. C'est également pour cette raison qu'il est expressément prévu à l'al. 4 que toutes les données de ce système n'apparaissent pas forcément dans l'index national de police<sup>39</sup>. Selon l'art. 17, al. 4, LSIP, le Conseil fédéral est en outre habilité à supprimer complètement l'accès de certaines autorités aux données de l'index répertoriant les données du système infractions fédérales.

Les accès en ligne au système infractions fédérales sont réglés à l'al. 5. Les autorités y figurant ne sont autorisées à accéder au système que dans la mesure où l'exige l'accomplissement de leurs tâches légales. En vertu de l'art. 19, let. c LSIP, le Conseil fédéral est habilité à régler par voie d'ordonnance la portée des autorisations d'accès, à savoir leur ampleur.

L'al. 6 de l'art. 11 prévoit, lorsque des intérêts importants liés à la poursuite pénale l'exigent, que les données peuvent être récoltées à l'insu de la personne concernée. Cette compétence est accordée à la PJF en tant qu'office central de police criminelle, conformément à l'art. 3 LOC, en relation avec l'art. 14, al. 1, LOC. Si la PJF a effectivement recueilli des données à l'insu de la personne concernée, celle-ci doit être informée dès que le motif de maintien du secret a disparu et dans la mesure où d'autres motifs légaux ne s'opposent pas à une communication. Cette disposition reprend le texte de l'actuel art. 14, al. 1, LOC, avec les précisions suivantes:

- L'art. 11, al. 6, LSIP, prévoit expressément que l'information a lieu dans la mesure où les données ont été recueillies *par la PJF* à l'insu de la personne concernée. L'actuel art. 14 al. 1 LOC, en relation avec l'art. 3 LOC, permettait

<sup>33</sup> Cf. également les considérations relatives à l'art. 4

<sup>34</sup> Art. 340 et 340<sup>bis</sup> CP

<sup>35</sup> RS 360

<sup>36</sup> RS 360.1

<sup>37</sup> RS 311.0

<sup>38</sup> Cf. art. 8 LSIP et son commentaire

<sup>39</sup> Cf. également le commentaire de l'art. 17 LSIP, 5<sup>ème</sup> paragraphe

de se dispenser d'une telle précision. La genèse de ces dispositions permet d'affirmer que le Parlement voulait limiter l'information ultérieure des personnes concernées aux traitements de données effectués *par les offices centraux*: en effet, l'art. 14 al. 1 LOC était, dans le projet du Conseil fédéral, initialement un article distinct dans la première partie du texte (dispositions générales), qui réglait également les modes d'acquisition des informations par les offices centraux<sup>40</sup>. Ce n'est que lors de la phase des débats parlementaires que cet article a été déplacé à la section 4 et fusionné au reste de l'art. 14 LOC<sup>41</sup>. Etant donné que le projet de LSIP reprend l'art. 14 al. 1 LOC, il paraît approprié de mentionner expressément qu'il s'applique aux traitements de données *de la PJF*. Le Préposé fédéral à la protection des données et à la transparence (PF PDT) s'oppose à cette interprétation et est d'avis que l'obligation de la PJF d'informer les personnes concernées doit également s'appliquer lorsque les données ont été récoltées par d'autres autorités. L'avis du PF PDT n'est pas réfuté que par la genèse de la LOC, mais également par le principe d'attribution des compétences qui pose que seule l'autorité qui a procédé à la récolte des informations à l'insu de la personne concernée peut être responsable de l'information ultérieure de celle-ci. En effet, seule cette autorité, qui connaît l'ensemble de la procédure, est en mesure de déterminer si les intérêts de poursuite pénale justifiant un traitement de données secret ont entretemps disparu. Si l'autorité qui a récolté les données est cantonale ou étrangère, il devient évident que l'information ultérieure ne saurait être réglée dans la LOC.

- Les let. a à c de l'art. 11, al. 6, contiennent quelques précisions quant à la possibilité de renoncer à l'information ultérieure ou de la différer. Ces critères correspondent à la pratique actuelle de la PJF et ne sont pas remis en question par le PF PDT.

#### *Art. 12*            Système de traitement des données relatives à la coopération policière internationale et intercantonale

Le système prévu à l'art. 12 doit permettre à la PJF de traiter toutes les données qu'elle reçoit d'autorités suisses ou étrangères mais qui ne concernent pas des infractions soumises à la juridiction fédérale ou relevant des compétences d'Office central de police criminelle. Par exemple, en tant que Bureau central national Interpol, la PJF peut être requise par un canton de transmettre à l'étranger des données concernant une personne soupçonnée d'avoir commis des lésions corporelles graves. La PJF, en tant que premier point contact pour les autorités étrangères de police, est également susceptible de recevoir des informations relatives à des vols de voiture. Ce ne sont pas là des délits soumis à la juridiction fédérale, mais il est important de disposer d'un système permettant de répertorier les données pertinentes en matière de police et généralement transmises à des tiers. Ce système doit également permet-

<sup>40</sup> Il s'agissait de l'art. 35<sup>duodecies</sup>, al. 2, CP (Recherche d'informations [par l'office central de lutte contre le crime organisé]), cf. FF 1994 I 1125

<sup>41</sup> Cf. proposition de la Commission des affaires juridiques du Conseil des Etats, BO CE 1994 II 725. Le texte original du Conseil fédéral y est repris sans modification et n'a pas été commenté ou discuté par le parlement lors de la suite des débats.

tre de traiter les données relatives à la coordination d'enquêtes intercantionales ou internationales<sup>42</sup> pour des délits non soumis à la juridiction fédérale.

Aujourd'hui, le système IPAS remplit cette fonction dans une certaine mesure. En vertu de l'art. 351<sup>octies</sup>, al. 3, let. e, CP<sup>43</sup>, toutes les données traitées dans le cadre d'Interpol peuvent y être saisies, indépendamment du délit concret. Or, depuis l'entrée en vigueur de l'art. 351<sup>octies</sup> CP, les canaux de transmission internationale d'informations policières se sont multipliés<sup>44</sup>. Il s'agit donc de prévoir un système permettant de saisir ce genre d'informations quel que soit le système de transmission choisi. En vertu de l'al. 5, le système permet de distinguer le type de canal de transmission pour chaque information, ce qui contribue à une bonne gestion des différentes informations et permet d'observer les règles en partie différentes applicables à leur traitement. Cette réglementation se retrouve aux art. 11, al. 3, et 18, al. 4.

*Art. 13*                    Système d'appui aux enquêtes des cantons dans leur domaine de compétence en matière de poursuite pénale

L'art. 13 prévoit un système mis à la disposition des cantons pour leurs propres affaires de police. Il s'agit d'un service de la Confédération qui permet aux cantons d'utiliser un système informatique développé au niveau fédéral. Ce service n'est pas nouveau: le système JANUS connaît déjà cette solution<sup>45</sup>. Au cas où une même affaire relève parallèlement de la compétence fédérale et de la compétence d'un ou de plusieurs cantons, le système de l'art. 13 permet par ailleurs de faciliter l'échange d'informations entre autorités et ainsi de mieux coordonner les procédures. Les cantons demeurent bien évidemment libres d'utiliser leurs propres systèmes informatiques pour traiter les données relatives à leur domaine exclusif de compétences. Les données traitées dans le système de l'art. 13 sont soumises au droit cantonal, qui réglera par exemple les personnes autorisées à consulter ces données, y compris les autorités fédérales, le droit des particuliers aux renseignements pour les données traitées à leur sujet, ainsi que la durée de conservation des données. Le projet rappelle cependant l'obligation pour les cantons d'édicter des dispositions de protection des données en la matière et d'instituer un organe de contrôle, conformément aux principes prévus par la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel<sup>46</sup>, qui s'applique également aux cantons.

*Art. 14*                    Système d'information pour l'identification de personnes dans le cadre de poursuites pénales et de recherche de personnes disparues

L'art. 14 est consacré au système d'identification de personnes dans le domaine de la poursuite pénale et de la recherche des personnes disparues. Cet article évoque en fait trois systèmes distincts:

<sup>42</sup> Tâche des Offices centraux de police criminelle selon l'art. 2 let. b LOC

<sup>43</sup> RS 311.0

<sup>44</sup> Schengen, Europol, accords bilatéraux de coopération policière conclus avec tous les pays voisins et plusieurs autres pays.

<sup>45</sup> Cf. art. 12 LOC et art. 7, let. b, de l'ordonnance sur le système informatisé de la Police judiciaire fédérale (ordonnance JANUS, RS 360.2).

<sup>46</sup> RS 0.235.1



1. le système contenant les profils d'ADN; ce système est régi par la loi fédérale du 20 juin 2003 sur les profils d'ADN<sup>47</sup>, à laquelle la LSIP ne fait que renvoyer (al. 2);
2. le système contenant les autres données signalétiques, principalement les empreintes digitales (actuellement le système AFIS<sup>48</sup>); il est régi par l'art. 351<sup>septies</sup> CP<sup>49</sup>;
3. le système contenant les données personnelles correspondant aux données signalétiques et aux profils d'ADN (ces données sont actuellement traitées dans le système IPAS, cf. art. 351<sup>octies</sup>, al. 3, let. c. CP); ce système fait l'objet de la réglementation de l'art. 14.

Ces trois systèmes sont exploités séparément pour des raisons de sécurité et de protection des données, ce d'autant plus que le système AFIS contient des empreintes digitales relevées tant dans le cadre d'enquêtes policières que dans le cadre de la législation sur les étrangers. Seul fedpol est habilité à effectuer le lien entre les données personnelles et les données signalétiques. Ce lien est réalisé au moyen du numéro de contrôle de processus. L'art. 14 LSIP n'introduit pas de nouveautés matérielles, mais expose de manière plus systématique l'architecture informatique actuelle en matière de systèmes d'identification. Les images d'empreintes et de traces, les photos et les codes numériques correspondant aux profils d'ADN sont stockés dans des bases de données spécialisées. Les noms des personnes qui s'y rapportent et les circonstances du relevé signalétique figurent dans le système selon l'art. 14 LSIP. Ce système correspond à la catégorie «AFIS-ADN» du système principal IPAS<sup>50</sup>. En conséquence, un accès en ligne est prévu comme aujourd'hui pour la PJF et l'Office fédéral de la justice pour ce qui concerne l'entraide internationale en matière pénale<sup>51</sup>.

### 2.2.3 Section 3: Autres systèmes d'information de police

*Art. 15*            Système de recherches informatisées de police

Cet article reprend pour l'essentiel le contenu de l'actuel article 351<sup>bis</sup> CP (RIPOL<sup>52</sup>). Une précision a été apportée s'agissant des buts pour lesquels les autorités sont habilitées à saisir des données dans le RIPOL ou à les consulter. Chaque autorité ne peut en effet accéder au système que pour un ou plusieurs buts bien déterminés, mais pas systématiquement pour tous les buts mentionnés à l'al. 1. Font exception à ce principe fedpol et les polices cantonales, qui sont également chargés d'introduire des données pour le compte d'autres autorités. Fedpol et les polices cantonales peuvent donc être amenés à saisir des données pour l'ensemble des tâches légales prévues à l'al. 1.

Une autre nouveauté mérite une mention spéciale. Il est proposé d'utiliser le RIPOL pour permettre la prévention de l'enlèvement international d'enfants (al. 1, let. h). Il

<sup>47</sup> RS 363

<sup>48</sup> Cf. art. 7 à 11 de l'ordonnance sur le traitement des données signalétiques, RS 361.3.

<sup>49</sup> Dont une modification est proposée dans le cadre du présent projet, cf. ch. 2.3.3.

<sup>50</sup> Art. 5, al. 1, let. a, de l'ordonnance IPAS, RS 361.2.

<sup>51</sup> Cf. art. 9 et 10 ainsi que l'annexe 2 de l'ordonnance IPAS.

<sup>52</sup> Ce système est exploité avec succès depuis environ dix ans.

faut en effet savoir que ce type d'enlèvement, aux conséquences graves, se produit relativement fréquemment en Suisse<sup>53</sup>. Actuellement, seules les personnes ayant déjà été enlevées peuvent être inscrites dans le RIPOL. Or ce système est l'outil principal des autorités chargées des contrôles aux frontières. Ainsi, le signalement dans le RIPOL d'un enfant menacé d'enlèvement et/ou des personnes susceptibles de commettre un tel enlèvement permettra certainement d'éviter bon nombre de cas. La menace d'un enlèvement doit toutefois paraître suffisamment grave pour justifier une inscription préventive dans le RIPOL. C'est pourquoi l'inscription n'est possible que si une autorité judiciaire ou tutélaire l'a ordonnée. Il est par ailleurs prévu de fixer un délai de conservation court (en principe 1 année) pour ce type de données dans l'ordonnance d'application. La brièveté du délai vise à éviter que des informations à but préventif ne demeurent trop longtemps dans le RIPOL, et à assurer que la menace d'enlèvement soit réévaluée à intervalles réguliers par l'autorité judiciaire ou tutélaire concernée.

Toujours concernant l'al. 1, une nouvelle lettre (let. i) mentionne la possibilité d'utiliser le RIPOL aux fins de surveillance discrète ou de contrôle ciblé de personnes et de véhicules en vue d'une poursuite pénale ou pour prévenir les risques pour la sécurité publique. Il ne s'agit pas véritablement d'une nouveauté, car la surveillance discrète est déjà prévue dans l'ordonnance RIPOL<sup>54</sup>. Cette mention ne saurait par ailleurs fonder de nouvelles compétences pour les autorités qui inscrivent des recherches. En effet, la licéité d'une mesure ordonnée par une autorité demeure régie par les codes de procédure pénale applicables ou d'autres actes législatifs. Il s'agit plutôt ici d'augmenter la transparence et d'inclure un objectif déjà prévu dans la législation applicable à la partie nationale du Système d'information Schengen<sup>55</sup>.

A l'al. 4, un accès est nouvellement prévu pour l'autorité chargée d'effectuer des contrôles de sécurité selon la LMSI, pour le seco et les autorités cantonales et communales compétentes dans les domaines de la migration et de l'emploi, pour les autorités d'établissement des documents d'identité (let. f à h). Ces accès sont déjà prévus par l'art. 3, al. 3, de l'ordonnance sur le système de recherches informatisées de police<sup>56</sup>. Il s'agit des «autres autorités judiciaires et administratives» de l'art. 351<sup>bis</sup>, al. 3, let. h, CP, la loi permettant au Conseil fédéral de désigner par voie d'ordonnance de nouvelles autorités habilitées à consulter des données, autorités qui n'existaient pas ou qui existaient sous une autre désignation lors de la rédaction de la loi. Par analogie, il est prévu d'accorder à l'avenir un accès à la Commission fédérale des maisons de jeu, cette nouvelle autorité ayant des fonctions de poursuite pénale en partie similaires à celles de l'Administration fédérale des douanes qui bénéficie déjà d'un accès<sup>57</sup>. Le Préposé fédéral à la protection des données et à la transparence doute de la nécessité pour la Commission d'avoir accès au système pour accomplir ses tâches légales. Au vu des fonctions de poursuite pénale de la Commission, le Conseil fédéral estime que cet accès répond au principe de la proportionnalité et propose dès lors son maintien.

<sup>53</sup> Environ une centaine de cas par année.

<sup>54</sup> Art. 10, al. 2, let. b de l'ordonnance, RS **172.213.61**.

<sup>55</sup> Cf. art. 16, al. 2, let. f, du projet.

<sup>56</sup> Ordonnance RIPOL, RS **172.213.61**.

<sup>57</sup> Cf. art. 57 de la loi fédérale du 18 décembre 1998 sur les jeux de hasard et les maisons de jeu, RS **935.52**, qui prévoit que la Commission poursuit les infractions pénales, conformément à la loi fédérale sur le droit pénal administratif.

Avec l'al. 5, l'interface actuellement en place, qui permet aux utilisateurs RIPOL d'effectuer une interrogation simultanée dans les systèmes SYMIC<sup>58</sup>, ISA<sup>59</sup>, MOFIS<sup>60</sup>, FABER<sup>61</sup>, PAGIRUS<sup>62</sup> et INFOSTAR<sup>63</sup>, reçoit une base légale formelle. Cette possibilité n'est toutefois ouverte qu'aux personnes qui disposent effectivement d'un droit d'accès aux bases de données correspondantes. Il s'agit donc d'une solution technique qui ne change strictement rien aux données que les utilisateurs pourraient obtenir en interrogeant séparément les cinq systèmes correspondants. Seule l'interrogation s'effectue de manière centralisée. Cette solution pourra également être étendue à la consultation du système d'information Schengen (SIS) lors de la mise en application de l'accord d'association<sup>64</sup>.

#### *Art. 16*            Partie nationale du Système d'information Schengen

Le présent article a été repris du projet de modification de l'art. 351<sup>decies</sup> du code pénal accepté par le peuple suisse lors de la votation du 5 juin 2005 sur les accords bilatéraux d'association à Schengen et à Dublin<sup>65</sup>. Il a fait l'objet de modifications purement formelles pour qu'il soit en adéquation avec le reste du projet de loi. La compétence attribuée au Conseil fédéral en vertu de l'al. 7 sera exercée au travers de l'adoption d'une ou de plusieurs ordonnances d'exécution. Cette compétence est prévue pour les autres systèmes d'information de police à l'art. 19 du projet.

#### *Art. 17*            Index national de police

Comme indiqué au ch. 2.1, l'index national de police est le seul système d'information véritablement nouveau de ce projet de loi. La mise sur pied de ce système répond aux vœux du Conseil fédéral et de la CCDJP. Il permettra de faciliter et d'optimiser le travail des autorités de police de toute la Suisse. A l'heure actuelle, aucune autorité cantonale ne dispose d'informations en ligne sur le travail des polices voisines. Lorsqu'elle recherche des renseignements sur un individu, elle doit présenter une demande aux 25 autres cantons ainsi qu'à fedpol pour obtenir un résultat, ce qui est lent et fastidieux. L'index de police a pour but d'accélérer ce processus d'entraide administrative. Une interrogation permettra de savoir si une personne est connue de la police, que ce soit auprès d'un canton, de fedpol ou même de l'étranger (données relatives aux échanges d'informations de police effectués dans le cadre d'Interpol, par exemple). Le résultat de l'interrogation est limité à l'identité de la personne, à l'autorité responsable, à la date et au motif de l'inscription, ainsi qu'au système d'information de provenance des données (art. 17, al. 3). Pour obtenir de plus amples renseignements, une demande à l'autorité compétente est indispensable. Lors de cette demande, la nature des renseignements fournis dépendra des circonstances d'espèce et des conditions de l'entraide judiciaire et administrative.

58    Système informatisé central sur la migration.

59    Système d'information sur les documents d'identité des ressortissants suisses.

60    Registre automatisé des véhicules et des détenteurs de véhicules.

61    Registre des autorisations de conduire.

62    Système de gestion de personnes, de dossiers et d'affaires dans le domaine de l'entraide internationale en matière pénale.

63    Banque de données centrale de l'état civil.

64    Cf. également le commentaire de l'art. 16.

65    Pour le texte de la modification, voir FF 2004 6709.

Le Préposé fédéral à la protection des données et à la transparence estime qu'il n'est pas question d'indiquer ni le motif de l'inscription ni le système dont proviennent les données, faute de quoi il ne s'agit plus d'un index de police. Or le motif de l'inscription apparaît exclusivement pour les personnes ayant fait l'objet d'un signalement (prise des empreintes digitales et/ou établissement d'un profil d'ADN) par une autorité de police. Il s'agit donc de personnes contre lesquelles il existe des soupçons fondés de commission d'une infraction et qui ont été rendues attentives aux conséquences du traitement par la police de leurs données signalétiques. En ce qui concerne le système source, une telle indication peut à nouveau préciser le résultat de la consultation de l'index et permet d'éviter des demandes de renseignement supplémentaires. Le projet prévoit dès lors le maintien de la possibilité de connaître le motif et le système source lors de la consultation de l'index de police.

L'index rassemble l'identité des personnes traitées dans:

1. le réseau de systèmes d'information de police;
2. le système de recherches informatisées de police;
3. les systèmes d'information de police des 26 cantons.

Ce nouvel outil permettra certainement d'améliorer l'efficacité de la lutte contre une criminalité de plus en plus complexe et mobile géographiquement. Il est prévu de le réaliser en étroite collaboration avec les cantons, qui devraient également fournir certaines prestations dans ce contexte (cf. ch. 3.2).

La possibilité de restreindre l'accès prévue à l'al. 5 permet au Conseil fédéral de limiter les données visibles par certaines autorités. Il serait envisageable de limiter leur accès aux données de personnes impliquées dans une procédure et, notamment, de ne pas faire apparaître les personnes figurant dans le système de la PJF selon l'art. 11 (système infractions fédérales). Cette solution permet de faciliter l'entraide administrative avec des autorités relativement éloignées du travail de police, telles que l'Office fédéral de la justice ou les autorités de la justice militaire, tout en ne les laissant pas accéder à des données qui ne les concernent pas.

L'introduction de l'index permet de renoncer à l'index IPAS prévu par le droit actuel (art. 351<sup>octies</sup>, al. 2, CP) et de remplacer certains accès limités d'autorités fédérales à plusieurs systèmes d'information, notamment les accès actuels du Bureau de communication en matière de blanchiment d'argent et du Service d'analyse et de prévention<sup>66</sup>. Si l'index devait ne pas être réalisé, ces accès limités devraient alors être introduits dans les bases légales des systèmes d'information correspondants. Au demeurant, le cercle d'utilisateurs de l'index a été fixé de telle sorte que seules les autorités assumant une fonction de police ou de poursuite pénale et celles habilitées à obtenir des informations des systèmes d'information de police existants en vertu du droit en vigueur aujourd'hui bénéficient d'un accès.

L'al. 8 prévoit que les autorités cantonales décident librement du raccordement à l'index et des données qui sont répertoriées dans celui-ci. Il s'agit ici de la possibilité de choisir quelles personnes font partie de l'index. Ce choix est toutefois limité par le type de données autorisées selon l'al. 3. Il n'est donc pas possible pour un canton de transmettre à l'index des données autres que celles qui sont définies dans le catalogue de l'al. 3.

<sup>66</sup> Cf. également art. 10, al. 3, de l'ordonnance JANUS (RS 360.2).

L'index de police doit faciliter l'accès à toutes les informations ayant trait aux activités criminelles d'une personne. Ce faisant, il pourrait également diminuer l'ampleur des recherches qui s'imposent lorsque l'on souhaite déterminer si une personne est en détention et le cas échéant localiser le lieu où elle se trouve. En effet, si une personne se trouve en prison, elle a certainement fait l'objet de recherches de police qui devraient logiquement être répertoriées dans l'index national de police. Dans ce sens, les informations supplémentaires qu'apporte cet outil pourraient permettre de répondre en partie à la recommandation n° 4 du rapport du 16 novembre 2005 de la Délégation des commissions de gestion<sup>67</sup> et aux souhaits exprimés dans la motion Burkhalter 05.3773, «Banque de données centralisée répertoriant les personnes en détention».

#### *Art. 18*            Système de gestion des affaires et des documents de fedpol

Ce système se distingue du réseau de systèmes d'information de police selon les art. 10 à 14. L'usage en est réservé exclusivement au personnel de fedpol et les données correspondantes ne sont pas intégrées dans l'index national de police. Les activités de fedpol ne se limitent en effet pas aux tâches de police, mais incluent des tâches de police administrative telles que la recherche de personnes disparues ou les tâches de coordination en matière de documents d'identité et de légitimation<sup>68</sup>.

Cette diversité justifie un système de gestion interne des affaires et des documents relevant de la compétence de fedpol. Ce système permet d'enregistrer et de répertorier tous les documents relatifs aux activités de fedpol ainsi que les communications entrantes et sortantes de toute sorte et, au besoin, de les relier à d'autres systèmes d'information en fonction de leur nature. Ici à nouveau, il ne s'agit pas de créer une nouvelle base de données, mais d'actualiser l'architecture interne. Un tel système trouve actuellement sa base légale à l'art. 351<sup>octies</sup> CP (al. 1, let. b à e; al. 3 et 4).

Comme pour les autres systèmes d'information, la possibilité de distinguer les communications transmises par les canaux Interpol, Europol ou Schengen a été prévue (al. 4). Cette méthode permet de faciliter le triage de l'information et la gestion des différentes règles de droit qui peuvent s'y appliquer.

L'al. 5 permet un stockage de données relatives aux affaires des services compétents pour les documents d'identité et la recherche de personnes disparues. Il s'agit ici du domaine de la «police administrative relevant de la compétence de l'office [fédéral de la police]» visé à l'art. 351<sup>octies</sup>, al. 3, let. d, CP.

L'accès de l'Office fédéral de la justice (al. 6) vise à permettre aux personnes compétentes d'accéder aux informations leur permettant de vérifier que les conditions d'un mandat d'arrêt international ou d'une autre mesure d'entraide judiciaire internationale en matière pénale sont remplies. Pour les mêmes raisons, un accès similaire est accordé à l'Office fédéral de la justice aux systèmes visés aux art. 11 et 12 LSIP.

<sup>67</sup> «Le dispositif de sécurité de la Suisse et le cas Mohamed Achraf – appréciation résumée sous l'angle de la haute surveillance parlementaire».

<sup>68</sup> Art. 11, al. 2 et 3, de l'ordonnance sur l'organisation du Département fédéral de justice et police, RS 172.213.1.

## 2.2.4 Section 4: Dispositions finales

### Art. 19 Dispositions d'exécution

L'art. 19 délègue au Conseil fédéral la compétence d'édicter des dispositions qui, pour chaque système d'information de police, définiront:

- a. la responsabilité du traitement des données;
- b. le genre de données saisies;
- c. l'ampleur des autorisations d'accès au moyen d'une procédure d'appel;
- d. la procédure d'effacement et la durée de conservation des données;
- e. la collaboration avec les cantons;
- f. la communication de données des systèmes d'information de police aux tiers dans un cas d'espèce;
- g. la sécurité des données.

Ces dispositions prendront la forme d'une ou de plusieurs ordonnances d'application. La LSIP définit le principe, l'existence, le but de traitement et les utilisateurs des systèmes d'information de police. Il paraît toutefois adéquat de laisser au Conseil fédéral le soin de régler les autres aspects dans des dispositions réglementaires de niveau inférieur à une loi fédérale. Ces autres aspects sont en effet d'un niveau de détail plus grand et peuvent subir des modifications plus fréquentes (p.ex. création de nouvelles autorités, nouvelles modalités de participation financière des cantons, nouveaux procédés techniques). La délégation au Conseil fédéral permet de répondre à ces nouvelles situations avec la flexibilité nécessaire tout en demeurant dans le cadre net fixé par la loi.

## 2.3 Modification du droit en vigueur

### 2.3.1 Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (art. 15)

Cette modification reflète les modifications de structure intervenues au DFJP. L'art. 15, al. 4, actuel de la LMSI<sup>69</sup> prévoit que les données de la police judiciaire et les données recueillies en dehors d'une enquête de police judiciaire sont traitées séparément dans le système ISIS. Cette disposition correspond à l'art. 11, al. 3, LOC<sup>70</sup> et a été rédigée à l'époque où la Police fédérale dépendait du Ministère public et était la police judiciaire de la Confédération au sens de la loi fédérale sur la procédure pénale.

A l'heure actuelle, les activités de l'ancienne Police fédérale ont été transférées au Service d'analyse et de prévention d'une part et à la Police judiciaire fédérale d'autre part. Ces deux unités font partie de fedpol. La première se consacre aux activités préventives liées à la protection de l'Etat et prévues par la LMSI. Elle ne participe pas aux enquêtes de police judiciaire. Suite à cette réorganisation, et sous réserve de l'art. 15, al. 6, LMSI, les données de police judiciaire n'ont plus leur

<sup>69</sup> RS 120

<sup>70</sup> RS 360

place dans le système ISIS et le passage correspondant de l'art. 15, al. 4, LMSI doit être supprimé.

L'art. 15, al. 6, LMSI actuellement en vigueur autorise fedpol à traiter dans ISIS des données issues de procédures d'enquête à des fins préventives. Or, comme expliqué ci-avant, le Service d'analyse et de prévention ne participe plus aux procédures d'enquête. Il paraît dès lors justifié de reformuler l'al. 6 de sorte que la Police judiciaire fédérale, chargée des enquêtes, transmette au Service d'analyse de prévention des données issues de procédures qui permettent d'assurer le maintien de la sûreté intérieure (prévention au sens de l'art. 2 LMSI), et que le Service d'analyse de prévention soit habilité à traiter ces données dans son propre système d'information. L'exigence selon laquelle les données ne peuvent être transmises qu'une fois la procédure close a été abandonnée afin de permettre une plus grande souplesse. En effet, c'est le critère de l'importance de l'information au regard du maintien de la sécurité intérieure ou extérieure qui doit prévaloir plutôt que celui de l'état d'avancement de la procédure. Cela s'impose d'autant plus que le Service d'analyse et de prévention est complètement exclu des procédures d'enquête depuis qu'il n'est plus rattaché au Ministère public de la Confédération. En revanche, la condition de l'information simultanée de l'autorité pénale compétente est maintenue.

### **2.3.2                   Loi fédérale du 21 mars 1981 sur l'entraide pénale internationale (nouvel art. 11a)**

#### *1. But (al. 1)*

Le nouvel art. 11a de la loi fédérale du 20 mars 1981 sur l'entraide pénale internationale (EIMP)<sup>71</sup> prévoit que l'Office fédéral de la justice (OFJ) exploite le nouveau système de gestion de personnes, de dossiers et d'affaires. L'al. 1 évoque le caractère particulièrement sensible des données que contient le système ainsi que les buts du traitement de ces données. Cette base de données est destinée à intégrer toutes les formes de coopération prévues par l'EIMP.

La let. a prévoit que le nouveau système permet à ses utilisateurs de constater si l'OFJ traite des données au sujet d'une personne déterminée. Cette disposition ne permet pas l'accès au contenu des dossiers sur des personnes ou des affaires, ni à celui des entrées électroniques de personnes. La possibilité de traiter des données relatives aux contenus résulte en revanche du but figurant à la let. b. Le type de données relatives au contenu de dossiers de personnes et d'affaires et d'entrées électroniques de personnes est toutefois limité à des domaines bien déterminés (cf. al. 2). Les buts évoqués aux let. c à e visent à permettre une gestion et une exploitation uniformes, efficaces et fiables des dossiers concernant des personnes ou des affaires.

#### *2. Contenu (al. 2)*

Il découle du but du nouveau système de gestion de personnes, de dossiers et d'affaires que ce système contient l'identité des personnes dont l'OFJ traite les données. Si ces données n'étaient pas accessibles, le système ne permettrait en effet

<sup>71</sup> RS 351.1

pas de savoir si l'OFJ traite des données au sujet d'une personne déterminée. L'accès aux données d'identité évoquées à l'al. 2, let. a, n'est possible que par la recherche d'une personne déterminée, ce qui implique que l'utilisateur connaisse un nom ou des indications concrètes relatives à un cas (par exemple le numéro d'un dossier particulier). Le système peut également être interrogé à l'aide d'autres critères d'identité tels que prénom, profession, domicile et numéro d'immatriculation de véhicule.

L'al. 2, let. b, évoque toutes les informations indispensables à la gestion et à l'exploitation de données relatives à des personnes ou à des affaires ainsi que des dossiers personnel et d'affaires, par exemple autorité requérante, autorité cantonale d'exécution, phase procédurale.

L'al. 2, let. c, a pour but de permettre la gestion électronique de dossiers (pas de support papier). Les parties essentielles de toutes les communications parvenant à l'OFJ ou émanant de celui-ci sur support papier sont scannées et rattachées aux documents électroniques, aux courriers électroniques ou aux communications électroniques d'Interpol concernant la même affaire, puis enregistrées et classées.

### *3. Accès au moyen d'une procédure d'appel (al. 3)*

Cet alinéa est la base légale permettant à certaines autorités de savoir par le biais d'une procédure d'appel (en ligne) si l'OFJ traite des données au sujet d'une personne déterminée. Cette possibilité d'interrogation permet de réduire au minimum nécessaire les contacts directs entre autorités, qui impliquent une lourde charge administrative. Le seul critère de recherche admis pour ce type d'interrogation est celui du nom. D'autres critères limitatifs pourront être introduits. Le résultat de l'interrogation sera limité aux données énumérées à l'al. 2, let. a et b.

### *4. Délégation (al. 4)*

En vertu du principe de la proportionnalité, le traitement doit être limité aux données dont les utilisateurs ont absolument besoin pour accomplir leurs tâches légales (let. a). Il s'agit en l'espèce des données relatives aux personnes et aux affaires décrites à l'al. 2, let. a et b. Une autre catégorie de données dont le catalogue devra être établi dans l'ordonnance est celle des données des autorités judiciaires participant à la procédure d'entraide judiciaire. Il s'agit des données de l'Etat requérant (demande d'entraide judiciaire avec les données administratives telles qu'expéditeur, date de réception, etc.) ainsi que celles des autorités d'exécution (destinataire de la demande d'entraide judiciaire transmise par l'OFJ, étapes procédurales telles que décisions incidentes, etc.). La dernière catégorie de données se rapporte aux types de délit fondant la demande d'entraide (genre de délit, données concernant la commission du délit, lieu, etc.).

La let. b donne au Conseil fédéral le mandat de régler de manière appropriée la durée de conservation et l'archivage dans l'ordonnance.

La let. c prévoit que les services de l'OFJ autorisés à traiter des données dans le système doivent être mentionnés dans l'ordonnance. Les possibilités de traitement devront également être limitées dans leur étendue en fonction des différents services. Enfin, il est prévu que dans un cas d'espèce, l'OFJ pourra communiquer des données à d'autres autorités que celles mentionnées à l'al. 3.



### 2.3.3 Code pénal suisse

Le projet abroge l'art. 351<sup>bis</sup> CP (système RIPOL). Le contenu de cet article est repris à l'art. 15 LSIP (cf. commentaire de cet article).

L'art. 351<sup>septies</sup> CP (collaboration à des fins d'identification de personnes) intègre un nouvel al. 2<sup>bis</sup>. Cet alinéa vise à rendre plus transparent le fait que l'art. 351<sup>septies</sup> ne règle que les données signalétiques proprement dites, à l'exclusion des profils d'ADN et des données personnelles liées aux données signalétiques (identité, motif de l'inscription, etc.). Cette modification constitue un parallèle à la réglementation de l'art. 14 LSIP. Les empreintes digitales peuvent également être relevées dans le domaine des étrangers. Les données personnelles y relatives sont quant à elles traitées dans le système informatisé central sur la migration<sup>72</sup>.

L'art. 351<sup>octies</sup> CP (système IPAS) est abrogé; sa teneur est reprise pour l'essentiel aux art. 10 à 14 LSIP (ch. 2.2.2), et certains de ses éléments sont repris dans le système de gestion de fedpol (art. 18 LSIP) et l'index national de police (art. 17 LSIP). Le domaine de l'entraide judiciaire internationale en matière pénale est réglé au nouvel art. 11a de la loi fédérale du 20 mars 1981 sur l'entraide pénale internationale (ch. 2.3.2)

### 2.3.4 Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération

Les art. 11, 12 et 14 LOC<sup>73</sup> sont suppléés par les art. 10 à 14 LSIP (ch. 2.2.2).

### 2.3.5 Loi fédérale du 10 octobre 1997 concernant la lutte contre le blanchiment d'argent dans le secteur financier

L'art. 17 al. 4, let. e, du projet prévoit que le bureau de communication en matière de blanchiment d'argent (ci-après le bureau) dispose d'un accès à l'index national de police. Il s'agit ici, en parallèle et en complément à cette disposition, de créer dans la LBA<sup>74</sup> une base légale formelle pour l'accès du bureau aux divers systèmes d'information de la Confédération.

A l'heure actuelle, pour accomplir ses tâches légales, le bureau a accès aux banques de données RIPOL, AUPER<sup>75</sup>, IPAS, JANUS et VOSTRA. La base légale de ces accès se trouve à l'art. 5 de l'ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent<sup>76</sup>. Le rapport d'activité du bureau présenté au Conseil fédéral en 2002 a démontré que cette base légale n'est pas

<sup>72</sup> SYMIC; cf. loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines de l'étranger et de l'asile, FF **2003** 4032.

<sup>73</sup> RS **360**

<sup>74</sup> RS **955.0**

<sup>75</sup> Ce système est remplacé par le système d'information central sur la migration (SYMIC, cf. FF **2002** 4367) et le système de gestion de personnes, de dossiers et d'affaires dans le domaine de l'entraide judiciaire internationale en matière pénale (PAGIRUS, cf. ch. 2.3.2 du présent message).

<sup>76</sup> RS **955.23**

suffisante et qu'une loi au sens formel est nécessaire. Par décision du 9 avril 2002, le Département fédéral de justice et police a été chargé d'élaborer un projet de loi en conséquence. Le projet d'art. 35<sup>bis</sup> LBA résulte de ce mandat.

La recommandation 26 du Groupe d'action financière sur la lutte contre le blanchiment de capitaux (GAFI) préconise que le service de communication national dispose d'un accès direct ou indirect aux informations dont il a besoin pour accomplir ses tâches. Un accès aux bases de données fédérales est indispensable pour le travail du bureau et ce point n'est pas controversé. Le seul problème réside dans le fait que ledit accès n'est jusqu'ici prévu que par une ordonnance.

Seul l'accès au système de traitement des données relatives à la protection de l'Etat (ISIS) est nouveau dans le présent projet. Cet accès est contesté par le Préposé fédéral à la protection des données et à la transparence. Or l'accès du bureau à ISIS est d'une grande importance pour le bureau dans le cadre de ses activités légales d'analyse, particulièrement en ce qui concerne le financement du terrorisme<sup>77</sup>. L'accès à AUPER est remplacé par un accès aux systèmes qui lui succèdent, à savoir SYMIC et PAGIRUS, tandis que l'accès à JANUS, IPAS et RIPOL est remplacé par un accès à l'index national de police, qui englobe l'identité des personnes traitées dans ces trois systèmes.

La «personne» mentionnée à l'al. 1 peut être aussi bien une personne physique qu'une personne morale. L'accès du bureau à des informations plus étendues se détermine d'après les dispositions spéciales de chaque système d'information (al. 2).

### **3 Conséquences**

#### **3.1 Conséquences pour la Confédération**

Il s'agit de rappeler ici qu'à l'exception de l'index national de police et du N-SIS, la LSIP ne crée pas de nouveaux systèmes d'information, mais les regroupe et les catégorise selon de nouveaux principes. Les coûts financiers et en personnel découlant de ces aménagements peuvent être pris en charge dans le cadre de la planification financière ordinaire du DFJP.

En revanche, l'index national de police est une application entièrement nouvelle. Son développement devrait occasionner des coûts d'environ 2 millions de francs. Les coûts annuels d'exploitation sont estimés à 100 000 francs par année.

D'autre part, la mise en place de l'index national de police augmentera notablement la rapidité et l'efficacité des recherches de police. Cela permettra de gagner du temps et de l'argent.

Les conséquences financières et en personnel découlant du raccordement au Système d'information Schengen ont déjà été présentées dans le cadre du message du Conseil fédéral relatif à l'approbation des accords bilatéraux entre la Suisse et l'Union européenne, y compris les actes législatifs relatifs à la transposition des accords («accords bilatéraux II»)<sup>78</sup>.

<sup>77</sup> Conformément à l'art. 1, al. 1, let. a de l'ordonnance sur le Bureau de communication en matière de blanchiment d'argent (RS 955.23), le Bureau est chargé d'assister les autorités de poursuite pénale dans la répression du blanchiment d'argent, de la criminalité organisée et du financement du terrorisme.

<sup>78</sup> FF 2004 5593 ss; cf. ch. 3.6.1.

## **3.2 Conséquences pour les cantons et les communes**

C'est l'introduction de l'index national de police qui comporte des conséquences notables pour les cantons. En effet, le développement de l'index proprement dit est à la charge de la Confédération, mais chaque canton devrait, à ses frais, rendre son propre système de police compatible avec l'index national de façon à permettre un transfert de données, en principe par voie d'interface. Les coûts correspondants (finances et personnel) varieront d'un canton à l'autre et ne peuvent être exposés ici. En raison de la possibilité d'intégrer l'index dans le réseau informatique de police existant, les frais ne devraient toutefois pas dépasser quelques dizaines de milliers de francs par canton.

Il s'agira également pour les cantons d'adapter le cas échéant le droit cantonal applicable à leurs systèmes d'information de police afin de permettre un transfert d'une partie de ces données vers un système fédéral. Au cours de la procédure de consultation, aucun canton n'a indiqué une impossibilité absolue de procéder à de telles adaptations. L'un d'entre eux a par ailleurs indiqué que l'article correspondant de la LSIP, l'art. 17, pouvait constituer la base légale à cet effet.

Au vu de la compétence originaire des cantons en matière de police, la Confédération ne peut imposer de telles mesures aux cantons. La participation de tous les cantons à l'index de police devra donc s'effectuer sur une base volontaire. Le projet reflète le caractère volontaire du raccordement à l'art. 17, al. 8. Il est prévu que les cantons qui acceptent le raccordement s'engagent à respecter les standards informatiques décrétés par la Confédération à cet égard et à appliquer les critères qu'elle fixe pour le type d'infractions à inclure (délits d'une certaine gravité).

Les conséquences positives de l'index et d'une certaine harmonisation des autres systèmes d'information de police figurent au ch. 3.1 et valent tout aussi bien pour la Confédération que pour les cantons.

## **3.3 Autres conséquences**

L'objectif général du projet est de mettre à jour le cadre juridique qui régit l'utilisation des bases de données de police. La clarification des structures et la création d'une base légale pour l'index de police contribueront à améliorer l'efficacité de la poursuite pénale. Cette plus grande efficacité pourrait se traduire à son tour par de nouveaux succès dans la lutte contre la criminalité, ce qui aura naturellement des conséquences positives sur la sécurité du pays et, indirectement, sur l'économie suisse.

## **4 Programme de la législation**

Le projet n'est pas mentionné expressément dans le rapport sur le Programme de la législation 2003 à 2007<sup>79</sup>. Il rejoint cependant l'objectif 9 (Garantir la sécurité: optimiser la coopération internationale, la prévention et les structures internes en matière de justice et police) dans la mesure où l'actualisation des bases légales

<sup>79</sup> FF 2004 1035

concernant les systèmes d'information de police permet une plus grande transparence dans ce domaine, ainsi que la flexibilité requise pour les autorités de police. La création de l'index national de police permet en outre de renforcer la collaboration avec les cantons. Le projet de LSIP figure par ailleurs parmi les objectifs 2006 du Conseil fédéral. Enfin, avec la LSIP, une partie du champ d'application du projet de loi fédérale sur la police<sup>80</sup> est déjà couverte.

## **5 Bases juridiques**

### **5.1 Constitutionnalité**

La LSIP donne un cadre aux réglementations existantes, concernant, par exemple, le système automatisé de recherches de police ainsi que la collaboration avec Interpol; elle prévoit en outre la création d'un index national de police. Ce faisant, la Confédération accomplit une tâche que les cantons seuls ne sont pas en mesure d'accomplir entièrement<sup>81</sup>. La LSIP se fonde ainsi sur l'art. 57, al. 2, de la Constitution, qui attribue à la Confédération la compétence de coordonner ses efforts avec les cantons en matière de sécurité intérieure et sur la compétence de l'Assemblée fédérale de traiter les objets qui relèvent de la compétence de la Confédération et qui ne ressortissent pas à une autre autorité fédérale (art. 173, al. 2, Cst).

### **5.2 Rapports avec le droit européen**

Le présent projet tient compte des exigences de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE n° 108), dont la Suisse est signataire<sup>82</sup>. Il respecte également les prescriptions du Protocole additionnel à cette Convention concernant les autorités de contrôle et les flux transfrontaliers de données. Ce protocole additionnel a été accepté par les Chambres dans le cadre de la révision de la LPD<sup>83</sup>. Le projet a par ailleurs été conçu de manière à satisfaire aux exigences des art. 8 et 13 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)<sup>84</sup>. Il tient en outre compte des principes énoncés dans la recommandation R 87 (15) du Comité des Ministres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

<sup>80</sup> Voir la liste des objets parlementaires, FF **2004** 1089.

<sup>81</sup> Comparer le message du Conseil fédéral concernant la modification du code pénal suisse (création d'un office central de lutte contre le crime organisé), FF **1994** I 1125.

<sup>82</sup> RS **0.235.1**

<sup>83</sup> FF **2003** 1915 ss

<sup>84</sup> RS **0.101**

### **5.3**

#### **Délégation de compétences législatives**

Le projet prévoit, à son article 19, de déléguer au Conseil fédéral la compétence de déterminer pour chaque système d'information de police plusieurs éléments significatifs (cf. ch. 2.2.4). Cette compétence s'exercera sous la forme d'une ou plusieurs ordonnances d'application.

### **5.4**

#### **Forme de l'acte à adopter**

Le présent projet est conçu sous la forme d'une loi fédérale. En effet, les dispositions fondamentales relatives, en particulier, à la restriction des droits constitutionnels ainsi qu'à l'organisation et à la procédure des autorités fédérales doivent être édictées sous la forme d'une loi fédérale (art. 163, al. 1, et 164, al. 1, let. b et g, Cst.).

