

# **Lutter plus efficacement contre le terrorisme et le crime organisé**

## **Rapport du Conseil fédéral donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats (05.3006)**

du 9 juin 2006

---

Messieurs les Présidents,  
Mesdames et Messieurs,

En réponse au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats intitulé «Lutter plus efficacement contre le terrorisme et le crime organisé», nous vous soumettons le présent rapport.

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

9 juin 2006

Au nom du Conseil fédéral suisse:

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

---

## Condensé

*Le présent rapport répond au postulat 05.3006 «Lutter plus efficacement contre le terrorisme et le crime organisé» déposé par la Commission de la politique de sécurité du Conseil des Etats le 21 février 2005, qui demande au Conseil fédéral d'examiner les modifications à apporter à la législation pour lutter plus efficacement contre le terrorisme et le crime organisé. Il aborde les neuf questions soulevées par le postulat, les dispositions pénales applicables en matière de lutte contre le terrorisme et le crime organisé ainsi que les normes fédérales qui règlent la collaboration entre les autorités de poursuite pénale et le service de renseignement intérieur.*

*Le rapport expose tout d'abord les normes pénales et les règles de procédure applicables aux organisations criminelles de type mafieux ou terroriste en Suisse. Il se penche en outre sur un phénomène nouveau auquel la Suisse n'a pas échappé: l'émergence de petits groupes ou de cellules qui approuvent les actes de violence de nature politico-idéologique commis dans le monde et se disent prêts à perpétrer eux-mêmes de tels actes. Comme ces groupuscules ne montrent pas de signes suffisamment clairs pour être interprétés comme des actes préparatoires au sens de l'art. 260<sup>bis</sup> CP avant une longue période et ne se cloisonnent pas de façon aussi hermétique que les syndicats mafieux visés à l'art. 260<sup>er</sup> CP, la poursuite pénale de ce phénomène s'avère très difficile. Le Conseil fédéral juge néanmoins prématuré de prendre dès maintenant des mesures législatives concrètes pour réprimer ce phénomène, d'autant que l'on ne dispose encore d'aucune jurisprudence en la matière et que les Chambres fédérales avaient renoncé, en 2002, à introduire une disposition générale sur le terrorisme. Par ailleurs, le Conseil fédéral estime judicieux d'attendre les résultats des débats parlementaires sur la révision partielle de la LMSI qui est en cours.*

*Le rapport examine ensuite les compétences préventives et répressives dont dispose la Confédération dans la lutte contre ces actes de violence. Dans l'exercice de ces compétences, les autorités fédérales de poursuite pénale sont tenues de collaborer étroitement avec le service de renseignement intérieur. Cette collaboration s'inscrit dans un cadre très réglementé qui, sur le plan juridique se révèle certes adéquat mais peut poser des problèmes d'application pour les autorités de police. Il s'agit de compenser ce défaut en promouvant la formation et le perfectionnement professionnel, en incitant les autorités à utiliser au mieux les canaux d'information, et en les encourageant à échanger les informations et à unir leurs efforts dans la conduite des opérations.*

*Au-delà d'une collaboration optimale entre les autorités compétentes dans le pays, l'efficacité de la lutte contre les actes de violence criminelle de nature terroriste ou mafieuse suppose une étroite collaboration avec les autorités étrangères, d'autant que les infractions constatées en Suisse sont souvent en relation avec des actes commis à l'étranger. La coopération internationale repose sur l'entraide administrative et judiciaire au niveau des services de renseignement et des autorités de poursuite pénale. L'entraide est régie en partie par le droit national et en partie par*

---

*des traités bilatéraux ou multilatéraux. Pour le Conseil fédéral, aucune intervention législative ne s'impose actuellement sur ce plan.*

*La pratique suisse et étrangère montre que fréquemment, faute de preuves matérielles suffisantes, la lutte contre le terrorisme et le crime organisé ne parvient à ses fins qu'avec l'aide de témoignages. Mais un témoin menacé n'accepte de déposer ou de maintenir sa déposition qu'en échange d'une protection adéquate. Les droits protecteurs institués par le régime juridique suisse actuel et ceux qui sont prévus par le P-CPP constituent un volet important de la protection des témoins. Ces mesures dites procédurales sont toutefois insuffisantes lorsque l'auteur connaît le témoin ou peut remonter jusqu'à son identité. Pour prévenir les actes d'intimidation ou de représailles, il est nécessaire de garantir une protection appropriée en dehors des actes de procédure à proprement parler et applicables après le procès aussi. Faute de normes juridiques spécifiques sur la protection extraprocédurale des témoins, aucune mesure du genre n'est actuellement mise en œuvre. Fort de ce constat, le Conseil fédéral charge le DFJP d'élaborer des propositions pour créer dans le droit fédéral les conditions permettant de mettre en place des programmes de protection des témoins introduisant des mesures extraprocédurales.*

*Ensuite, le rapport examine si les résultats de l'exploration radio menée à l'étranger par le DDPS (CGE) ne pourraient être utilisés au profit du MPC lorsque l'entraide judiciaire internationale atteint ses limites. Pour que le MPC puisse directement mandater la CGE au DDPS, il faudrait créer une base juridique spéciale dans une loi dont le Conseil fédéral ne voit cependant pas l'utilité dans l'immédiat d'autant plus que le droit actuel autorise la transmission au MPC d'informations recueillies fortuitement dans le cadre de l'exploration radio. En l'espèce, le Conseil fédéral voit des possibilités d'augmenter l'efficacité en renforçant la collaboration entre les autorités chargées du renseignement. Il estime également qu'il faut poursuivre les examens techniques entamés en vue d'une utilisation des ressources de la CGE au profit du renseignement intérieur, afin de garantir une surveillance des télécommunications efficace dans un domaine marqué par une évolution technologique fulgurante.*

*Le cryptage, complet ou partiel, des communications par téléphone satellite et d'autres formes de télécommunications (p.ex. téléphonie Internet) rend le travail de surveillance et d'exploration plus difficile. Le Conseil fédéral n'envisage aucune mesure législative dans ce domaine (obligation de consigner les clés de chiffrement utilisées ou les procédures de chiffrement appliquées) dans la mesure où elles ne constitueraient un moyen ni approprié ni judicieux pour faciliter les tâches de surveillance et d'exploration. En revanche, il plaide également en faveur d'une utilisation du décryptage au profit des autorités de poursuite pénale. Ici encore, une collaboration technique accrue entre les instances suisses concernées générerait des gains d'efficacité.*

*Au sujet de la durée de conservation des données téléphoniques, le Conseil fédéral partage l'avis des auteurs du postulat selon lequel le délai de six mois prévus par le droit actuel est trop court, en particulier dans les procédures pénales de longue durée. Vu les difficultés rencontrées dans la pratique pour recueillir des éléments de preuve et l'évolution du droit en Europe, le Conseil fédéral considère qu'il est*

---

*nécessaire d'augmenter la durée de conservation des données de communication. L'augmentation de six mois proposée dans le postulat lui paraît raisonnable. Néanmoins, il ne se prononcera sur la suite à donner à ce dossier que lorsque sera disponible le rapport relatif à la révision de la LSCPT qu'il a mandaté le 29 mars 2006 pour clarifier les questions juridiques en suspens liées à la surveillance des télécommunications dans le cadre de la poursuite pénale.*

*Enfin, le rapport examine quatre autres problématiques abordées par le postulat. Le Conseil fédéral ne voit aucune nécessité de légiférer pour le moment sur les interventions préventives et sur la prolongation de la durée de conservation des profils d'ADN. Quant à la surveillance préventive et à la prolongation de la détention en cas de risque de récidive, elles font déjà l'objet de révisions législatives dans des projets en cours (LMSI et P-CPP).*

## Table des matières

<b>Condensé</b>	<b>5422</b>
<b>Table des abréviations</b>	<b>5428</b>
<b>1 Structure et organisation des travaux</b>	<b>5430</b>
<b>2 Lutte contre le terrorisme et le crime organisé</b>	<b>5430</b>
2.1 Contexte	5430
2.2 Etat des lieux	5430
2.2.1 Poursuite des organisations criminelles	5430
2.2.2 Poursuite des organisations criminelles de type mafieux	5431
2.2.3 Poursuite des organisations criminelles de type terroriste	5431
2.2.4 Poursuite des infractions principales de terrorisme	5432
2.2.5 Actes préparatoires délictueux	5432
2.2.6 Poursuite des cellules terroristes	5432
2.2.7 Compétence de la Confédération et des cantons en matière de poursuite pénale	5433
2.3 Appréciation	5433
2.3.1 Poursuite des organisations criminelles	5433
2.3.2 Poursuite des cellules terroristes	5434
2.3.3 Etendue des compétences de poursuite pénale de la Confédération	5434
2.4 Mesures	5435
<b>3 Coopération entre les organes de poursuite pénale et le service de renseignement intérieur</b>	<b>5435</b>
3.1 Contexte	5435
3.2 Etat des lieux	5436
3.2.1 Organisation des forces de police au sein du DFJP	5436
3.2.2 Le SAP, service de renseignement intérieur de la Suisse, et ses tâches	5436
3.2.3 Les autorités fédérales de poursuite pénale et leurs tâches	5437
3.2.4 Délimitation des tâches entre le service de renseignement intérieur et les autorités de poursuite pénale	5437
3.2.5 Coopération entre les autorités fédérales de poursuite pénale de la Confédération et le SAP	5439
3.3 Appréciation	5441
3.4 Mesures	5442
<b>4 Coopération internationale</b>	<b>5442</b>
4.1 Contexte	5442
4.2 Etat des lieux	5442
4.2.1 Entraide judiciaire	5442
4.2.2 Coopération policière	5444
4.2.3 Coopération entre les services de renseignement	5446
4.3 Appréciation	5447
4.4 Mesures	5448

<b>5 Protection extraprocédurale des témoins</b>	<b>5448</b>
5.1 Contexte	5448
5.1.1 Mesures de protection des témoins	5448
5.1.2 Délimitation de la réglementation relative aux témoins «de la Couronne»	5449
5.2 Etat des lieux	5450
5.2.1 Protection extraprocédurale des témoins en Suisse	5450
5.2.2 Importance des mesures extraprocédurales dans la lutte contre le terrorisme et le crime organisé	5452
5.3 Appréciation	5453
5.4 Mesures	5454
5.4.1 Possibilités de protection extraprocédurale des témoins	5454
5.4.2 Propositions pour la Suisse	5455
<b>6 Recours à l'exploration radio et à la surveillance des télécommunications</b>	<b>5456</b>
6.1 Contexte	5456
6.2 Etat des lieux	5457
6.2.1 Recherche d'informations à l'étranger par les autorités fédérales de poursuite pénale	5457
6.2.2 Recherche d'informations à l'étranger par les services de renseignement	5457
6.2.3 Communication des découvertes fortuites	5458
6.3 Appréciation	5458
6.4 Mesures	5459
6.4.1 Renforcement de la collaboration	5459
6.4.2 Evaluation d'une utilisation des moyens de l'exploration radio en Suisse	5459
<b>7 Décryptage des communications</b>	<b>5460</b>
7.1 Contexte	5460
7.2 Etat des lieux	5460
7.2.1 Système de consignation des clés et interdiction de chiffrement à l'aide de clés non consignées	5461
7.2.2 Interdiction des appareils de chiffrement dont l'algorithme n'a pas été consigné	5461
7.2.3 Tour d'horizon international	5461
7.3 Appréciation	5462
7.4 Mesures	5463
7.4.1 Utilisation des systèmes de décryptage au profit des autorités de poursuite pénale	5463
7.4.2 Collaboration technique entre les autorités nationales concernées	5463
<b>8 Augmentation de la durée de conservation des données de télécommunication</b>	<b>5463</b>
8.1 Contexte	5463
8.2 Etat des lieux	5464
8.2.1 Bases légales	5464

8.2.2 Situation et tendances en Europe	5464
8.2.3 Pratique de la surveillance rétroactive	5465
8.2.4 Question de l'insuffisance de la durée actuelle de conservation	5465
8.3 Appréciation	5466
8.4 Mesures	5467
<b>9 Autres points abordés par le postulat</b>	<b>5468</b>
9.1 Interventions préventives	5468
9.2 Surveillance préventive	5469
9.3 Risque de récidive	5469
9.4 Prolongation de la durée de conservation des profils d'ADN	5469

## Table des abréviations

ATF	Arrêt du Tribunal fédéral
BO	Bulletin officiel
CE	Conseil des Etats
CEDH	Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101)
CGE	Division de la conduite de la guerre électronique (DDPS) et les autres services de l'administration fédérale chargés de la conduite de la guerre électronique
CN	Conseil national
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
CPM	Code pénal militaire du 13 juin 1927 (RS 321.0)
CPS	Commission de la politique de sécurité
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS 101)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFJP	Département fédéral de justice et police
EIMP	Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (RS 351.1)
EuGRZ	Europäische Grundrechte-Zeitschrift
Europol	Office européen de police
fedpol	Office fédéral de la police
FF	Feuille fédérale
Interpol	Organisation Internationale de Police Criminelle
LAAM	Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (RS 510.10)
LAVI	Loi fédérale du 4 octobre 1991 sur l'aide aux victimes d'infractions (RS 312.5)
LCPI	Loi fédérale du 22 juin 2001 sur la coopération avec la Cour pénale internationale (RS 351.6)
LFIS	Loi fédérale du 20 juin 2003 sur l'investigation secrète (RS 312.8)
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (RS 120)
LOC	Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (RS 360)

Loi sur les profils d'ADN	Loi fédérale du 20 juin 2003 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (RS 363)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1)
LSCPT	Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
LTC	Loi du 30 avril 1997 sur les télécommunications (RS 784.1)
MPC	Ministère public de la Confédération
MROS	Bureau de communication en matière de blanchiment d'argent
OCGE	Ordonnance du 15 octobre 2003 sur la conduite de la guerre électronique (RS 510.292)
ODM	Office fédéral des migrations
OMSI	Ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (RS 120.2)
ONU	Organisation des Nations Unies
OOO	Ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police (RS 360.1)
OSCP	Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (RS 780.11)
OSF	Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale (RS 120.72)
P-CPP	Projet de code de procédure pénale suisse (FF 2006 1373)
PJF	Police judiciaire fédérale (DFJP)
PPF	Loi fédérale du 15 juin 1934 sur la procédure pénale (RS 312.0)
RPS	Revue Pénale Suisse
RS	Recueil systématique du droit fédéral suisse (et des accords internationaux)
SAP	Service d'analyse et de prévention (DFJP)
SFS	Service fédéral de sécurité (DFJP)
SRS	Service de renseignement stratégique (DDPS)
STS	Service des tâches spéciales (Secrétariat général du DETEC)
TEJUS	Traité du 25 mai 1973 entre la Confédération Suisse et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale (RS 0.351.933.6)
TF	Tribunal fédéral
UE	Union européenne

# Rapport

## 1 Structure et organisation des travaux

Le présent rapport, qui a été préparé par le DFJP avec le concours de représentants du MPC, du DETEC et du DDPS, répond au postulat 05.3006 «Lutter plus efficacement contre le terrorisme et le crime organisé» déposé par la Commission de la politique de sécurité du Conseil des Etats, le 21 février 2005, et transmis par le Conseil des Etats au Conseil fédéral, le 15 juin 2005.

Le postulat demande au Conseil fédéral d'examiner dans un délai d'une année la façon dont la législation peut être adaptée dans plusieurs domaines afin de permettre de lutter plus efficacement contre le terrorisme et le crime organisé. Il demande en particulier de faire le tour des neuf questions suivantes: l'utilisation des moyens affectés à la conduite de la guerre électronique pour la surveillance des communications sur le territoire national, la coopération internationale, le décryptage des communications par téléphone satellite, la prolongation de la durée de conservation des données téléphoniques, l'autorisation de la surveillance préventive, l'autorisation des interventions préventives, le risque de récidive, la banque de données ADN et la protection des témoins.

## 2 Lutte contre le terrorisme et le crime organisé

### 2.1 Contexte

Avant de répondre à la question de savoir si et dans quelle mesure il est nécessaire de légiférer en vue d'optimiser la lutte contre le terrorisme et le crime organisé, il faut présenter l'arsenal juridique à disposition. Il y a donc lieu tout d'abord d'examiner comment le droit pénal et la procédure pénale traitent actuellement ces deux phénomènes criminels. Il s'agira ensuite de se pencher sur la question de savoir si et dans quelle mesure ces instruments sont suffisants pour obtenir l'efficacité visée par les auteurs du postulat.

### 2.2 Etat des lieux

#### 2.2.1 Poursuite des organisations criminelles

Quiconque participe ou apporte son soutien à une organisation criminelle risque la réclusion pour cinq ans au plus ou l'emprisonnement en vertu de l'art. 260<sup>ter</sup> CP<sup>1</sup>. Par rapport aux critères du droit pénal, cette norme pénale implique une extension de la répression en amont: quiconque encourage de manière générale les activités d'une organisation criminelle est punissable, sans qu'une relation avec un acte délictueux concret (précis) de l'organisation ne soit nécessaire. Soutenir un groupe, c'est lui apporter toute contribution décisive aboutissant au renforcement de l'organisation<sup>2</sup>.

<sup>1</sup> En vigueur depuis le 1<sup>er</sup> août 1994.

<sup>2</sup> Hans Baumgartner, in: Strafgesetzbuch II, Commentaire bâlois, Bâle 2003, note 12 ad art. 260<sup>ter</sup>.

Cette contribution pourrait consister par exemple à fournir une partie de l'infrastructure logistique.

Une «organisation criminelle» est définie par le droit pénal comme un groupe de personnes dont l'existence est tenue secrète, dont les structures hiérarchisées sont conçues pour durer et dont le but est de commettre des actes de violence criminelle ou de s'enrichir par des moyens criminels.

### **2.2.2 Poursuite des organisations criminelles de type mafieux**

L'art. 260<sup>ter</sup> CP a été conçu dans l'optique de la répression des organisations criminelles comme la mafia italienne, dont la motivation première est l'argent. Ce type de syndicat criminel agit à travers des entreprises, pratique un cloisonnement hermétique vis-à-vis de l'extérieur, recourt à des méthodes d'intimidation et cherche à exercer son influence sur la politique, l'appareil d'Etat et l'économie<sup>3</sup>.

### **2.2.3 Poursuite des organisations criminelles de type terroriste**

Le champ d'application de l'art. 260<sup>ter</sup> CP s'étend aussi aux organisations criminelles qui poursuivent des objectifs politico-idéologiques. En criminologie, on qualifie de «terrorisme» la menace d'actes violents émanant d'organisations criminelles dont les motivations sont d'ordre politico-idéologique.

Il n'existe pas encore de définition juridique internationalement reconnue du terrorisme, d'autant que la distinction avec les luttes de libération ou le terrorisme d'Etat n'est pas claire. La norme pénale sanctionnant le financement du terrorisme (art. 260<sup>quinquies</sup> CP) définit l'acte terroriste comme un «acte de violence criminelle visant à intimider une population ou à contraindre un Etat ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte». Si l'on s'en tient à la jurisprudence du TF sur le terrorisme, les «Brigate rosse» italiennes, l'organisation basque ETA, l'Armée de libération du Kosovo ou le réseau international Al-Qaïda sont des organisations criminelles au sens de l'art. 260<sup>ter</sup>, ch. 1, CP<sup>4</sup>.

Les organisations terroristes peuvent aussi mener des activités économiques pour financer les actes de violence criminelle qu'elles veulent mettre à exécution.

<sup>3</sup> H. Baumgartner, in: Strafgesetzbuch II, Commentaire bâlois, Bâle 2003, note 6 ad art. 260<sup>ter</sup>; message du Conseil fédéral concernant la modification du code pénal suisse et du code pénal militaire (punissabilité de l'organisation criminelle), FF 1993 III 269, 272 s. avec renvois; ATF 131 II 235 ss.

<sup>4</sup> ATF 1A.50/2005 consid. 2.6, avec renvoi aux ATF 128 II 355 consid. 2.2, p. 361, et ATF 125 II 569 consid. 5c à 5d, p. 574 s.; ATF 131 II 235 ss.

## 2.2.4 Poursuite des infractions principales de terrorisme

Hormis la disposition précédemment mentionnée visant le financement du terrorisme, le code pénal<sup>5</sup> ne contient pas d'autre norme qui réprime explicitement le terrorisme. En revanche, il renferme une foule de dispositions qui permettent de poursuivre les actes terroristes perpétrés contre des personnes ou des équipements (infractions contre la vie et l'intégrité corporelle<sup>6</sup>, infractions contre la liberté<sup>7</sup>, infractions créant un danger collectif<sup>8</sup> et autres crimes ou délits<sup>9</sup>). Sont également punissables la tentative, l'instigation et la complicité intervenant dans le cadre de ces actes. Il est possible de tenir compte d'un caractère particulièrement répréhensible, par exemple de mobiles terroristes, dans la fixation de la peine<sup>10</sup>. Ces éléments constitutifs de l'infraction ressortissent pour la plupart à la juridiction cantonale.

## 2.2.5 Actes préparatoires délictueux

S'agissant par ailleurs de la poursuite pénale d'infractions particulièrement graves<sup>11</sup> qui sont typiquement commises dans le cadre d'actes terroristes, le législateur a fixé le seuil de répression avant le stade de la tentative en introduisant la notion d'acte préparatoire délictueux à l'art. 260<sup>bis</sup> CP. Selon cette disposition, se rend coupable d'acte préparatoire délictueux celui qui, suivant un plan, prend des dispositions concrètes d'ordre technique ou organisationnel, dont la nature et l'ampleur indiquent qu'il s'apprête à passer à l'exécution de l'une des infractions graves susmentionnées<sup>12</sup>. En l'occurrence, les dispositions prises doivent être des actes suffisamment concrets<sup>13</sup>. La complicité et l'instigation à commettre des actes préparatoires délictueux sont également punissables.

## 2.2.6 Poursuite des cellules terroristes

Les autorités judiciaires suisses sont de plus en plus confrontées à l'émergence de petits groupes, ou cellules, qui cautionnent des actes de violence de nature politico-idéologique commis dans le monde et manifestent leur volonté de contribuer à l'instauration du règne de la violence, même au péril de leur vie, jusque dans les pays d'Europe occidentale.

<sup>5</sup> La législation pénale accessoire réprime également les infractions principales de terrorisme (p.ex. art. 34 de la loi fédérale du 13 décembre 1996 sur le matériel de guerre (RS 514.51).

<sup>6</sup> Art. 111 ss CP (p.ex. assassinat, lésions corporelles graves, mise en danger de la vie).

<sup>7</sup> Art. 180 ss CP (p.ex. séquestration et enlèvement, prise d'otage, contrainte).

<sup>8</sup> Art. 221 ss CP (p.ex. explosion; emploi avec dessein délictueux d'explosifs et de gaz toxiques; fabriquer, dissimuler et transporter de telles substances).

<sup>9</sup> Infractions contre la paix publique (art. 258 ss CP) ou contre l'Etat (art. 265 ss CP).

<sup>10</sup> Art. 63 CP

<sup>11</sup> Meurtre, assassinat, lésions corporelles graves, brigandage, séquestration et enlèvement, prise d'otage, incendie intentionnel, génocide.

<sup>12</sup> Il existe un plan lorsque plusieurs actes liés convergent vers un objectif commun.

<sup>13</sup> De simples conjectures ne suffisent pas à constituer un acte répréhensible, BO CE 1981, p. 284; H. Baumgartner, in: Strafgesetzbuch II, Commentaire bâlois, Bâle 2003, notes 4 ss. ad art. 260<sup>bis</sup>.

Il existe des informations de nature policière selon lesquelles certaines cellules présentes en Suisse, sans être directement affiliées à une organisation, ont de vagues relations avec des membres d'organisations terroristes qui relèvent de la grande criminalité et qui vivent à l'étranger. Les membres de ces cellules, qui se préparent mentalement à l'exécution d'actes de violence, peuvent se rencontrer pendant des mois, voire des années, sans prendre aucune mesure de cloisonnement. Dans certains cas, ils vont jusqu'à diffuser publiquement leurs messages politiques haineux en se cachant derrière la liberté d'expression et en évitant délibérément de lancer des appels explicites à commettre des actes de violence criminelle<sup>14</sup>. Jusqu'au moment où ces cellules terroristes commettent des actes préparatoires délictueux, le droit procédural ne confère aux instances de poursuite pénale que des pouvoirs de contrôle et des ressources limités pour combattre leur travail de sape.

## **2.2.7 Compétence de la Confédération et des cantons en matière de poursuite pénale**

La loi fédérale instituant de nouvelles compétences de procédure en faveur de la Confédération dans les domaines de crime organisé et de la criminalité économique, qui est entrée en vigueur, le 1<sup>er</sup> janvier 2002, dans le cadre du «Projet d'efficacité», a notamment introduit le nouvel art. 340<sup>bis</sup> CP. A l'al. 1 de cette norme de compétence, le législateur soumet à la juridiction fédérale les infractions définies dans le contexte de la lutte contre le crime organisé, en particulier celles qui sont le fait des organisations criminelles visées à l'art. 260<sup>ter</sup> CP. La juridiction fédérale s'applique si les infractions visées par l'art. 260<sup>ter</sup> CP et les actes punissables émanant d'une organisation criminelle ont été commis pour une part prépondérante à l'étranger, ou dans plusieurs cantons sans qu'il y ait de prédominance évidente dans l'un d'entre eux.

En revanche, la compétence de poursuivre les actes préparatoires délictueux visés à l'art. 260<sup>bis</sup> CP relève en principe des cantons; les autorités fédérales sont néanmoins compétentes si les actes sont dirigés contre la Confédération<sup>15</sup>.

## **2.3 Appréciation**

### **2.3.1 Poursuite des organisations criminelles**

Comme cela a déjà été mentionné, l'art. 260<sup>ter</sup> CP a été conçu dans l'optique de la lutte contre des organisations criminelles du type de la mafia italienne, caractérisées par une stricte loi du silence et par des structures hiérarchiques établies pour durer. Les organes de poursuite judiciaire sont certes confrontés à certaines difficultés pour apporter la preuve de ces critères. Mais la jurisprudence sur cette disposition du code pénal n'étant pas encore suffisamment développée, il paraît encore trop tôt pour en déduire une nécessité générale de légiférer, ce d'autant que l'art. 260<sup>ter</sup> CP implique déjà dans sa version actuelle une extension de la criminalisation en amont.

<sup>14</sup> Il faut examiner dans ce cas la possibilité d'appliquer l'art. 259 CP: provocation publique au crime ou à la violence (juridiction cantonale).

<sup>15</sup> Art. 340, ch. 1, al. 7, CP

### 2.3.2 Poursuite des cellules terroristes

Il est plus difficile d'évaluer l'arsenal pénal relatif aux groupes de personnes qui répondent à notre définition de cellule terroriste, qui ne prennent pas (encore) des dispositions suffisamment concrètes pour qu'elles puissent être considérées comme des actes préparatoires au sens de l'art. 260<sup>bis</sup> CP, et qui ne pratiquent pas un cloisonnement aussi hermétique que les syndicats mafieux visés à l'art. 260<sup>ter</sup> CP. La poursuite pénale de ce phénomène en Suisse reste très difficile.

Un laisser-faire vis-à-vis de cellules terroristes portées à perpétrer les actes de violence criminelle les plus graves constituerait un risque pour la sûreté nationale que le Conseil fédéral ne peut prendre à la légère. Néanmoins, pour des raisons de proportionnalité et de pertinence pénale et considérant que la jurisprudence sur ce sujet est encore peu développée<sup>16</sup>, il ne doit pas conclure trop vite à l'existence d'une lacune dans le droit pénal.

Dans la perspective d'un éventuel élargissement de la notion pénale du regroupement de personnes de nature terroriste, le Conseil fédéral doit aussi tenir compte du fait que, lors des débats de 2002 sur la ratification des deux conventions de l'ONU pour la répression du financement du terrorisme et la répression des attentats à l'explosif<sup>17</sup>, les Chambres fédérales se sont limitées à adopter une norme pénale sur le financement du terrorisme<sup>18</sup> et se sont abstenues de créer un crime de terrorisme<sup>19</sup>. A l'époque, le Parlement avait considéré qu'une telle norme pénale ne s'imposait pas. Qui plus est, les conventions internationales en question ne l'exigeaient pas. De plus, il n'était convaincu ni par la définition du terrorisme qui lui était proposée ni par l'urgence de l'introduire dans notre droit.

Enfin, le Conseil fédéral n'entend pas introduire des mesures concrètes de poursuite pénale en matière de terrorisme avant d'être fixé sur la volonté du législateur de mettre en œuvre des mesures supplémentaires pour lutter à titre préventif contre le terrorisme par le service de renseignement intérieur. A ce sujet, une révision partielle de la LMSI est actuellement en préparation (projet LMSI II). Le message devrait être présenté au cours du second semestre 2006.

### 2.3.3 Etendue des compétences de poursuite pénale de la Confédération

Lorsque des actes de violence criminelle supposés mafieux ou terroristes ne remplissent que partiellement les critères définis par la loi et précisés par la jurisprudence pour qu'ils puissent être considérés comme le fruit d'une organisation criminelle, ou lorsque l'existence de ces critères ne peut être prouvée, les cantons sont en principe compétents pour instruire et juger les faits. Comme cela a déjà été expliqué, la même

<sup>16</sup> La question de savoir si cette situation découle d'un arsenal légal inadéquat ou d'un nombre relativement faible de cas pratiques méritant sanction est controversée.

<sup>17</sup> Message relatif aux Conventions internationales pour la répression du financement du terrorisme et pour la répression des attentats terroristes à l'explosif, FF 2002 5014 ss.

<sup>18</sup> Art. 260<sup>quinquies</sup> CP. Avant d'adopter définitivement cette norme, le Parlement avait ajouté diverses restrictions (voir al. 2 à 4); juridiction fédérale conformément à l'art. 340<sup>bis</sup> CP.

<sup>19</sup> Art. 260<sup>quinquies</sup> du projet qui prévoyait de punir l'acte de violence criminelle visant à intimider une population ou à contraindre un Etat ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque.

règle s'applique en matière de poursuite et de jugement des actes préparatoires délictueux visant l'exécution d'infractions graves, si ces dernières ne visent pas directement des institutions ou des autorités fédérales. Pour le MPC, cette situation est problématique, car bien souvent les cantons n'ont pas les infrastructures requises pour enquêter sur l'existence de relations et de structures de type mafieux ou terroriste, surtout dans un contexte de criminalité internationale. Le Conseil fédéral prend ces préoccupations au sérieux, mais il ne peut se contenter d'admettre simplement qu'une réglementation s'impose. Pour émettre une telle hypothèse, un examen approfondi devrait être fait avec le concours, entre autres, des autorités judiciaires cantonales.

## **2.4 Mesures**

Le Conseil fédéral juge prématuré de prendre dès maintenant des mesures législatives concrètes pour réprimer les nouveaux phénomènes liés au terrorisme. Il vaut mieux, à ses yeux, attendre les résultats des procédures en suspens et des jugements en attente, et les résultats des débats parlementaires sur la révision de la LMSI II qui est en cours avant de se prononcer sur la nécessité de légiférer.

## **3 Coopération entre les organes de poursuite pénale et le service de renseignement intérieur**

### **3.1 Contexte**

La lutte contre les organisations criminelles de type terroriste ou mafieux suppose toute une série de dangers à combattre et toute une série de compétences fédérales en matière de poursuite, qui nécessitent le concours de plusieurs organes policiers et judiciaires de la Confédération. Dans le présent chapitre, il s'agit de se pencher d'une part sur les différences entre les tâches préventives et répressives confiées à ces organes fédéraux et, d'autre part, sur l'exhaustivité et l'efficacité du cadre légal sur lequel s'appuie la collaboration entre les autorités fédérales de poursuite pénale et le service de renseignement intérieur, en mettant en avant les particularités et les limites juridiques de cette collaboration ainsi que les difficultés d'exécution qui ont récemment donné lieu à plusieurs interventions parlementaires<sup>20</sup>. La question de la collaboration entre le renseignement intérieur et le renseignement stratégique ne sera pas abordée puisqu'elle a déjà été amplement traitée dans d'autres rapports<sup>21</sup>. Il en sera de même de la collaboration entre les autorités de poursuite pénale et le Service de renseignement stratégique de la Confédération. Relevons néanmoins que cette collaboration n'intervient pas systématiquement, mais s'opère de manière ponctuelle et dans le cadre des règles de l'entraide administrative ordinaire.

<sup>20</sup> Motion CPS-CN 05.3001: Création de bases légales complètes pour les services de renseignement; Motion Schlüter 05.3637: Fusion des services de renseignement du DDPS et du DFJP.

<sup>21</sup> Décision du Conseil fédéral du 22 juin 2005 et travaux consécutifs.

## **3.2 Etat des lieux**

### **3.2.1 Organisation des forces de police au sein du DFJP**

En vue de l'extension, présentée dans le ch. 2, de la juridiction pénale de la Confédération aux affaires de criminalité organisée de type terroriste ou mafieux, le Conseil fédéral avait regroupé l'ancienne Police fédérale et le Service de sécurité de l'administration fédérale, le 1<sup>er</sup> septembre 1999, en les transférant du MPC à fedpol<sup>22</sup>. En réunissant tous les services de police du DFJP dans cet office, le Conseil fédéral faisait un pas en direction des cantons qui souhaitaient un interlocuteur unique au niveau fédéral pour toutes les questions liées à la police. Il donnait également suite à une exigence formulée après l'affaire des fiches, qui demandait que la fonction de procureur général de la Confédération, en tant qu'accusateur public, soit séparée de celle de premier responsable de l'ancienne Police fédérale, qui exerçait alors non seulement la fonction de police judiciaire mais également celle de service de renseignement intérieur, ce qui l'amenait à accomplir des tâches de nature préventive<sup>23</sup>.

Ainsi, le 1<sup>er</sup> janvier 2001, à l'issue du projet de restructuration du domaine policier de la Confédération (StruPol), les tâches de police préventive et de police judiciaire ont été séparées sur le plan organisationnel au sein de fedpol: la division «Offices centraux de police criminelle» et la «Police fédérale» ont été remplacées par les nouvelles divisions principales PJJ et SAP. La première a la fonction de police judiciaire et exerce à ce titre les tâches de poursuite pénale, tandis que la seconde se concentre sur la prévention par le renseignement. Les compétences de fedpol ont également été étendues à la protection des autorités, des institutions, des informations et des immeubles placés sous la responsabilité de la Confédération ainsi que des personnes, des immeubles et des biens qui doivent être protégés en vertu du droit international. Ces tâches sont prises en charge par la division SFS.

### **3.2.2 Le SAP, service de renseignement intérieur de la Suisse, et ses tâches**

Le SAP est le service de renseignement intérieur de la Suisse et ses tâches sont définies dans la LMSI et les ordonnances afférentes. Sa fonction consiste à fournir aux organes politiques dirigeants de la Confédération, mais aussi des cantons, des informations sur les menaces qui pèsent sur la sûreté intérieure, afin que des mesures préventives puissent être prises en temps utile. Les menaces en question sont des événements exceptionnels touchant à la sûreté de l'Etat et qui concernent la Suisse dans son ensemble. Afin d'identifier ces risques pour les fondements de la démocratie et de l'Etat de droit, de même que pour les libertés fondamentales de la population suisse, le SAP est tenu à une observation continue de la situation ainsi qu'à des appréciations périodiques de la menace. Etant donné que la LMSI lie les mesures préventives, généralement secrètes, ainsi que les interventions qui s'y rapportent à la prévention des risques pour la sûreté de l'Etat, les activités du renseignement poursuivent un objectif exclusivement préventif.

<sup>22</sup> A cette époque l'Office fédéral de la police s'abrégait OFP.

<sup>23</sup> Evénements survenus au DFJP – Rapport de la commission d'enquête parlementaire du 22 novembre 1989, FF 1990 I 593, chap. VII, ch. 1 (801 ss.)

### **3.2.3 Les autorités fédérales de poursuite pénale et leurs tâches**

Les organes fédéraux de poursuite pénale sont le MPC et la PJJ, lesquels mènent les enquêtes de police judiciaire qui relèvent de la juridiction fédérale. Le procureur général de la Confédération dirige les investigations de la PJJ et soutient l'accusation par-devant les tribunaux de la Confédération<sup>24</sup>. La fonction de répression pénale attribuée à ces instances judiciaires fédérales consiste à élucider une présomption concrète d'infraction. La poursuite pénale est donc une activité qui vise des infractions concrètes, qui n'intervient que lorsque les soupçons sont suffisamment étayés et qui se termine formellement soit par une ordonnance de non-lieu et par une libération, soit par une condamnation<sup>25</sup>. Les tâches du MPC et de la PJJ découlent du CP, de la PPF et de la LOC.

### **3.2.4 Délimitation des tâches entre le service de renseignement intérieur et les autorités de poursuite pénale**

#### *a. Délimitation quant à la finalité de la recherche d'informations*

La recherche d'informations du SAP vise à détecter précocement les dangers ou les troubles de nature à compromettre la sécurité. S'il en découvre, les autorités compétentes de la Confédération et des cantons prennent les mesures policières ou administratives qui s'imposent pour les réprimer ou les éliminer. S'il existe des soupçons selon lesquels des actes délictueux pourraient être à l'origine de ces dangers, les autorités de poursuite pénale sont activées<sup>26</sup>. La recherche d'informations vise à clarifier la présomption d'infraction et la question de la faute individuelle qui lui est liée pour pouvoir confier le cas aux organes judiciaires.

#### *b. Délimitation quant aux moyens de la recherche d'informations*

A la suite des investigations préliminaires, les autorités de poursuite pénale peuvent, si nécessaire, recourir aux mesures de contrainte prévues par la procédure pénale. En revanche, le législateur de 1997 a explicitement interdit au service de renseignement intérieur de recourir à des mesures de contrainte et à l'observation de faits dans des locaux privés, comme cela est possible dans une procédure pénale<sup>27</sup>. La question de savoir si, et si oui dans quelle mesure cette interdiction doit être maintenue – vu la menace que représentent aujourd'hui les associations et les cellules terroristes – est traitée dans le cadre de la révision partielle de la LMSI conduite au sein du DFJP (projet LMSI II). Par conséquent il n'y a pas lieu d'approfondir la problématique des moyens de la recherche d'informations dans le cadre du présent rapport.

<sup>24</sup> Art. 15 PPF

<sup>25</sup> A l'échelle nationale, une procédure pénale peut également se terminer par un retrait en faveur de l'étranger et par l'exécution de l'entraide judiciaire.

<sup>26</sup> Cf. art. 2, al. 3, et art. 17, al. 1, LMSI

<sup>27</sup> Art. 14, al. 3, LMSI

*c. Délimitation quant aux compétences de détection précoce de la grande criminalité de nature terroriste ou mafieuse*

Les menaces traditionnelles pour la sûreté de l'Etat et le terrorisme se caractérisent, outre par le recours à la violence contre la société et l'Etat, par des motivations politico-idéologiques. Le législateur a voulu faire figurer le terrorisme au premier rang des menaces pour la sûreté de l'Etat à l'art. 2, al. 1, LMSI plaçant ainsi cette forme de criminalité au cœur des activités de détection précoce et de prévention qui incombent au renseignement intérieur, autrement dit au SAP.

Les syndicats de type mafieux, qui poursuivent un but d'enrichissement et de reconnaissance sociale, ne peuvent être considérés comme une menace pour la sûreté de l'Etat dans la mesure où le chaos ou la destruction de l'ordre public visé par les terroristes représenterait plutôt un obstacle à leurs entreprises, leur objectif n'étant pas l'anéantissement mais l'instrumentalisation de l'économie, de la société et de leur prochain. Cela ne signifie pas que la détection précoce des phénomènes liés à la grande criminalité doit être laissée au hasard. Etant donné que les activités à but lucratif des organisations mafieuses se déroulent nécessairement dans un contexte commercial, le législateur suisse a jugé que leur détection devait faire partie de la sphère de compétences de la police judiciaire. Cette réglementation inscrite dans la LOC est judicieuse puisque la PJF est également chargée de démasquer et de poursuivre les affaires internationales de blanchiment de capitaux, de corruption, de trafic de stupéfiants et de criminalité économique. Or ces catégories d'infractions, surtout lorsqu'elles sont perpétrées à large échelle et par-delà les frontières, sont typiques de l'activité des syndicats mafieux.

La détection précoce s'inscrit dans la fonction d'*office central de police criminelle* de la PJF. Selon les art. 7, 8 et 11 LOC, c'est à elle qu'il incombe de «*découvrir*» et de «*combattre*» les phénomènes complexes et transfrontaliers liés à la grande criminalité lorsque, conformément à l'art. 340<sup>bis</sup> CP, ils relèvent de la juridiction fédérale. Pour accomplir ces tâches, la PJF doit exploiter un système informatisé dans lequel sont notamment traitées des informations devant permettre de démasquer des organisations criminelles de type mafieux, leur sphère d'influence, leurs membres, leurs protégés et leurs protecteurs.

*d. Délimitation quant aux tâches de police judiciaire*

Il ne faut pas confondre la recherche d'informations dans le cadre de la détection précoce avec l'instruction d'une infraction et la poursuite de son auteur. Dans le domaine de la grande criminalité, complexe et transfrontalière, les enquêtes et les poursuites pénales ne peuvent souvent être ouvertes qu'après une analyse des premiers indices recueillis dans le cadre de la détection précoce. Sur cette base, la PJF parvient à établir des liens avec les milieux de la mafia ou du terrorisme avec un degré de vraisemblance suffisamment élevé, de façon à pouvoir limiter les présomptions de culpabilité à un cercle raisonnablement restreint de suspects.

Après la phase de recherche des informations, et pour autant que la juridiction fédérale soit établie, l'instruction des infractions à connotation mafieuse ou terroriste ainsi que la poursuite de leurs auteurs incombent exclusivement à la PJF.

### 3.2.5 **Coopération entre les autorités fédérales de poursuite pénale de la Confédération et le SAP**

#### *a. Nécessité d'un échange d'informations rapide et régulier en raison de la superposition partielle des sphères de compétences*

Si les compétences en matière de lutte contre les syndicats mafieux, d'une part, et contre la menace pour la sûreté de l'Etat que représente le terrorisme, d'autre part, sont clairement délimitées dans la loi, dans la réalité il peut se produire des situations où les motivations pécuniaires et politico-idéologiques sont enchevêtrées au point de nécessiter une démarche parallèle du SAP et de la PJF. Le législateur a aussi prévu de tels cas de figure en obligeant chacune des deux divisions principales de fedpol à partager les informations en sa possession avec l'autre, et sans délai, lorsque celles-ci relèvent de la sphère de compétences de l'autre.

#### *b. Transmissions d'informations par le SAP à la PJF et au MPC*

Lorsque le SAP entre en possession d'informations concernant des organisations mafieuses, il est tenu de les transmettre aux organes de poursuite pénale de la Confédération ou des cantons<sup>28</sup>. Par ailleurs, la finalité préventive de la fonction de protection de l'Etat n'exclut aucunement que des informations acquises dans le cadre du renseignement soient transmises à des autorités de poursuite pénale suisses si cela peut permettre d'ouvrir une enquête sur des infractions concrètes. Le législateur a également prévu cette situation en obligeant le SAP à transmettre spontanément toute information relevant du droit pénal aux autorités suisses de poursuite pénale<sup>29</sup>. Dès que, dans le cadre de la recherche de renseignements, le SAP entre en possession d'indices pouvant éventuellement servir à démasquer ou à élucider des infractions, il les transmet aux organes de poursuite pénale compétents en Suisse (Confédération ou canton selon les cas), que les motivations à l'origine des infractions présumées soient de nature politico-idéologique, pécuniaire ou autre. Si les indices transmis sont suffisamment concrets, l'organe de poursuite pénale compétent pourra procéder directement à l'ouverture formelle de la procédure, et en cas contraire, il les utilisera pour corroborer, vérifier, motiver ou restreindre ses présomptions dans le cadre de recherches préliminaires.

Dans ses ordonnances, le Conseil fédéral a amplement concrétisé et précisé les obligations d'informer qui incombent au SAP<sup>30</sup>. Pour harmoniser l'exécution du droit réglementaire, le directeur de fedpol a édicté une directive qui établit entre autres les critères régissant la transmission d'informations dans le domaine de la lutte contre le terrorisme et la criminalité organisée<sup>31</sup>. Dans une autre directive, il a prescrit la tenue régulière de rapports opérationnels au niveau de la direction de fedpol et à tous les échelons hiérarchiques des divisions principales SAP et PJF<sup>32</sup>.

<sup>28</sup> Art. 2, al. 3, LMSI

<sup>29</sup> Art. 17, al. 1, LMSI; voir également l'obligation de collaborer prévue à l'art. 4 LOC.

<sup>30</sup> Art. 4 OOC et art. 18, al. 1, OMSI

<sup>31</sup> Weisung des Direktors BAP vom 22.12.2000 betreffend die Abgrenzung der Zuständigkeiten der Hauptabteilung DAP im Bereich der präventivpolizeilichen und analytischen Tätigkeiten und der Hauptabteilung BKP im Bereich der gerichtspolizeilichen Tätigkeiten (en version allemande uniquement).

<sup>32</sup> Weisung des Direktors Fedpol über die Zusammenarbeit zum Informationsabgleich zwischen der BKP und dem DAP vom 22. Februar 2006 (en version allemande uniquement).

### *c. Transmissions d'informations par la PJF et le MPC au SAP*

Le législateur a prévu une obligation réciproque pour la PJF et le MPC en matière de transmission d'informations au SAP<sup>33</sup>. Tous deux sont tenus de communiquer spontanément des renseignements au SAP lorsqu'ils décèlent des menaces concrètes pour la sûreté intérieure ou extérieure<sup>34</sup>.

Le Conseil fédéral a également concrétisé et précisé ces obligations dans ses ordonnances<sup>35</sup>. Ici aussi, les directives émises par le directeur de fedpol sont garanties d'une application uniforme du droit par la PJF<sup>36</sup>. S'agissant de l'obligation du MPC d'informer le service de renseignement intérieur, fedpol et le MPC ont conclu une convention le 30 août 2004 afin de régler dans le détail les compétences individuelles ainsi que les modalités d'application des règles d'exécution. Le procureur général de la Confédération a émis une directive complémentaire sur cette base<sup>37</sup>. Au-delà de l'échange d'informations opérationnelles, le MPC doit communiquer spontanément et sans délai au SAP les jugements et ordonnances de non-lieu qui touchent au champ d'application de la LMSI.

### *d. Echange d'informations en ligne*

Lorsque l'entraide administrative nécessite la transmission quotidienne de nombreuses informations, l'économie de gestion commande la mise en place d'un processus de consultation en ligne pour les données fréquemment demandées. Le SAP et le MPC disposent aujourd'hui déjà d'un accès simplifié à leurs systèmes réciproques, grâce auquel ils peuvent vérifier si des données concernant une personne sont en traitement dans le système consulté. Dans la loi fédérale sur les systèmes d'information de police de la Confédération, le Conseil fédéral envisage la création d'un index national de police destiné à accélérer et à simplifier l'entraide administrative en matière de police.

### *e. Garanties de procédure dans l'entraide administrative*

L'échange de données personnelles entre le service de renseignement intérieur et les autorités de poursuite pénale relève de l'entraide administrative. Mais comme l'on touche ici à des droits fondamentaux, la procédure doit reposer sur des principes légaux qui mettent en rapport les intérêts de l'Etat dans la lutte contre certains risques et la protection des individus visés. Dans ce contexte, la transmission d'informations suppose toujours un lien concret avec un cas particulier; elle doit être indispensable et permettre à l'autorité requérante de remplir ses tâches légales; enfin, elle doit servir les objectifs d'intérêt public poursuivis sans empiéter de façon disproportionnée sur la sphère d'intérêts juridiquement protégée des personnes directement ou indirectement concernées.

<sup>33</sup> Art. 13, al. 1, let. a, LMSI

<sup>34</sup> Art. 13, al. 2, LMSI

<sup>35</sup> Art. 8, al. 1 et 2, OMSI et art. 5, al. 2, let. a et b, OOC

<sup>36</sup> Voir notes 31 et 32 ci-dessus

<sup>37</sup> Directive du 1<sup>er</sup> juillet 2005 concernant la transmission au Service d'analyse et de prévention (SAP) d'informations provenant d'enquêtes de police judiciaire.

Pour que ces principes de protection soient réellement appliqués lors de l'échange de données personnelles entre le service de renseignement intérieur et les autorités de poursuite pénale, il faut que certaines exigences de procédure soient remplies: la demande d'entraide administrative doit être suffisamment motivée et d'importants processus de travail doivent être établis par écrit et par voie électronique dans le cadre de l'échange des données personnelles<sup>38</sup>. Ainsi les intéressés ont la garantie de pouvoir obtenir les informations les concernant qui ont été échangées dans le cadre de l'entraide administrative, au moment où leur demande de consultation fondée sur le droit de la protection des données est exécutée.

Outre la protection des données et les formalités que cela comporte sur le plan de la procédure, le service de renseignement intérieur et les autorités de poursuite pénale doivent prendre en considération certains intérêts publics prépondérants qui peuvent conduire à une limitation voire à une exclusion pure et simple de l'entraide et soumettre la transmission des données à des tiers à certaines restrictions. Lorsqu'il transmet des informations relevant du renseignement, le SAP doit ainsi veiller à la sauvegarde des intérêts prépondérants<sup>39</sup> mais aussi à la protection des sources. Le but de la protection des sources est le maintien du secret sur les informations qui permettraient de remonter jusqu'à l'origine des informations recueillies par les services de renseignement. La protection des sources est toujours garantie dans les rapports avec l'étranger<sup>40</sup> tandis que le besoin de protection des sources internes doit être pondéré dans chaque cas en fonction de la nécessité de l'entraide administrative ou judiciaire. Le directeur de fedpol a défini ce processus dans une directive<sup>41</sup>.

La PJF et le MPC peuvent aussi refuser ou restreindre la transmission d'informations ou encore l'assortir de charges. Ils y sont tenus lorsque les intérêts légitimes d'une personne l'exigent<sup>42</sup> ou lorsque la procédure en cours le commande, par exemple parce que le secret de l'instruction doit encore être sauvegardé.

### 3.3 Appréciation

Pour lutter efficacement contre le terrorisme et les organisations criminelles de type mafieux, il est essentiel que les autorités fédérales de poursuite pénale travaillent en intelligence avec le service de renseignement intérieur. Leur collaboration s'appuie sur un dispositif normatif dense, composé de lois fédérales, d'ordonnances et de directives. D'un point de vue strictement juridique, le Conseil fédéral considère que cette législation spéciale est amplement suffisante. Il constate toutefois que la mise en œuvre de ce dispositif au jour le jour atteint ses limites. Les employés des services de police de la Confédération doivent ainsi consulter fréquemment un grand nombre d'actes relevant du droit spécial afin de vérifier, pour chaque cas particulier, les conditions et les restrictions à la coopération policière. Cette systématique particulière du droit fédéral est due à l'évolution historique, mais elle ne doit pas occulter le fait que la pesée des intérêts inhérente à l'entraide administrative va de pair avec un certain pouvoir d'appréciation de la part de l'employé de police. Le droit positif

<sup>38</sup> Art. 4, al. 4, OOC et art. 18, al. 1, OMSI

<sup>39</sup> Art. 18, al. 5, OMSI

<sup>40</sup> Art. 17, al. 7, LMSI et art. 20a OMSI

<sup>41</sup> Weisung des Direktors Fedpol vom 1. Februar 2006 über die Handhabung des Quellschutzes durch den DAP (en version allemande uniquement).

<sup>42</sup> Art. 102<sup>quater</sup>, al. 2, en relation avec l'art. 27, al. 2, PPF; art. 7, al. 2, OOC

peut alléger l'exercice de ce pouvoir, mais certainement pas le remplacer. Il peut aussi faciliter l'interprétation et l'appréciation de l'échange d'informations policières, mais seulement de façon restreinte. En fin de compte, l'aptitude à fixer des priorités dans le traitement et la transmission d'informations qui se révéleront ensuite essentielle sur le plan de la politique de sécurité ou de la tactique de la procédure pénale dépend de l'expérience individuelle des employés des services de police. Cela étant, le Conseil fédéral ne voit aucune nécessité urgente de prendre des mesures législatives dans ce domaine.

### **3.4 Mesures**

Compte tenu de l'ancrage dans le droit spécial du droit de la police au niveau fédéral, le Conseil fédéral attache une grande importance à la formation et au perfectionnement professionnel des employés des organes de police de la Confédération. Les enseignements doivent porter sur le droit positif, mais aussi sur la conception de l'entraide administrative et sur les liens entre prévention et répression. Des cycles de formation continue peuvent être organisés à l'interne ou être suivis dans le cadre de l'offre d'établissements spécialisés tels que l'Institut suisse de police ou l'Institut de lutte contre la criminalité économique.

Une autre mesure concrète que le Conseil fédéral considère comme une mission permanente est la promotion de la capacité de tous les organes de sécurité de la Confédération à utiliser au mieux les canaux d'information existants, à encourager l'échange d'informations et à mener à terme des opérations de concert. C'est surtout une question de culture: dans un contexte dynamique caractérisé par le renouvellement rapide des systèmes de coopération tels que Interpol, Europol et Schengen-Dublin, les cultures d'entreprise doivent se consolider, se renforcer, mais également s'ouvrir.

## **4 Coopération internationale**

### **4.1 Contexte**

Le postulat aborde la question de la coopération internationale, réglée notamment par l'EIMP, en demandant notamment dans quelle mesure la procédure peut être simplifiée. L'EIMP est *un* pilier de la coopération internationale en matière de lutte contre le terrorisme et le crime organisé, mais pas le seul. C'est pourquoi il s'agit de faire le point de la situation sur la réglementation actuelle de l'entraide judiciaire et sur la coopération internationale entre les services de police et entre les services de renseignement.

### **4.2 Etat des lieux**

#### **4.2.1 Entraide judiciaire**

Le postulat invite le Conseil fédéral à examiner «si, et comment, au-delà de la révision actuellement en cours, [l'EIMP] peut être adaptée de façon à prévoir une procédure simplifiée permettant une coopération immédiate avec les autorités étrangères».

S'agissant tout d'abord de la simplification de la procédure, il faut relever que l'EIMP, qui est la base légale du droit national sur laquelle s'appuie la coopération avec l'étranger en matière pénale, prévoit aujourd'hui déjà une «extradition simplifiée» (art. 54) et une «exécution simplifiée» dans le cadre de la «petite entraide» (art. 80c). Sous certaines conditions, la Suisse peut ainsi faire l'économie d'une procédure formelle pour extraire une personne poursuivie ou pour livrer des moyens de preuve à des autorités de poursuite pénale étrangères. Hormis ces deux cas, le Conseil fédéral n'identifie pas d'autre domaine d'application pour une «procédure simplifiée». A partir du moment où la Suisse requiert l'entraide judiciaire d'un Etat tiers, le recours à des procédures simplifiées nécessite le concours d'autorités étrangères. Dans ce contexte, la marge de manœuvre législative de la Suisse est toutefois très étroite.

Le postulat demande aussi que l'on examine la possibilité de créer, dans le cadre de l'EIMP, des bases légales permettant une coopération immédiate entre les autorités de poursuite pénale suisses et étrangères. Les Etats signataires de la Convention européenne d'entraide judiciaire en matière pénale ont déjà réglé cette question à l'art. 4 du Deuxième Protocole additionnel à la Convention<sup>43</sup> (entré en vigueur le 1<sup>er</sup> février 2005 pour la Suisse). Ce protocole additionnel révisé certaines dispositions de la Convention, de sorte que les «autorités compétentes» et les ministères de la Justice peuvent à présent correspondre directement, sous certaines conditions. De son côté, la Suisse a établi des modalités d'entraide directe avec ses voisins par le biais d'accords bilatéraux<sup>44</sup>. Par contre, la voie des autorités centrales, autrement dit du ministère de la Justice, reste la règle dans les relations avec les Etats non européens. Certains éléments externes, tels que les différences dans l'organisation des autorités compétentes, et d'autres facteurs de nature politique peuvent retarder la procédure dans le pays étranger, et rien ne permet de penser que de tels cas de figure pourront être évités dans le futur. En pareille situation, les instances suisses requérant l'entraide judiciaire ne peuvent que compter sur une intervention personnelle des autorités compétentes en Suisse ou de leurs représentations diplomatiques sur place.

D'une manière générale, la simplicité de la procédure est une condition essentielle à la célérité de l'entraide judiciaire internationale. La Suisse n'a toutefois aucune influence sur les modalités de la procédure à l'étranger. Dans son propre ordre juridique, elle a créé des conditions permettant un déroulement rapide de la procédure lors de la révision partielle de l'EIMP de 1996<sup>45</sup>. L'efficacité de l'entraide judiciaire de la Suisse à l'égard d'autres Etats dépend enfin des voies de recours. Lors de la session d'été 2005, dans le cadre de la révision totale de l'organisation judiciaire fédérale, le Parlement a modifié les voies de recours dans la procédure d'entraide judiciaire en créant une deuxième instance de recours<sup>46</sup>.

<sup>43</sup> RS **0.351.12**

<sup>44</sup> Il s'agit d'accords en vue de compléter la Convention européenne d'entraide judiciaire en matière pénale. Pour un exemple de correspondance directe entre les autorités judiciaires de deux Etats, voir l'art. VIII de l'accord conclu avec l'Allemagne (RS **0.351.913.61**). Il en existe aussi avec l'Autriche (RS **0.351.916.32**), la France (RS **0.351.934.92**) et l'Italie (RS **0.351.945.41**).

<sup>45</sup> Voir message du Conseil fédéral: FF **1995** III 1 ss.

<sup>46</sup> La loi sur le Tribunal fédéral (LTF; FF **2005** 3829) adoptée le 17 juin 2005 permettra de recourir devant le TPF dans le cadre des procédures d'entraide judiciaire internationale et d'extradition, voire devant le TF dans les «cas particulièrement importants» (art. 84 LTF).

La Suisse est par ailleurs intégrée dans un vaste réseau de traités multilatéraux (a) et bilatéraux (b) d'entraide judiciaire en matière pénale.

#### *a. Traités multilatéraux*

S'agissant d'abord des traités multilatéraux régissant l'entraide judiciaire, qui ont été signés sous l'égide de l'ONU et du Conseil de l'Europe, la Suisse a ratifié tous les instruments qui lui étaient ouverts à la signature ou a initié la procédure de ratification. Il convient de citer notamment les conventions de l'ONU et du Conseil de l'Europe sur le terrorisme, qui élargissent le champ de la coopération<sup>47</sup>. Déjà mentionné précédemment, le Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale ouvre quant à lui la porte à de nouvelles techniques d'investigation et d'enquête dans la procédure pénale<sup>48</sup> (audition des témoins et des prévenus par vidéoconférence, observation transfrontalière, livraison surveillée, enquêtes discrètes, équipes communes d'enquête).

#### *b. Traités bilatéraux*

La Suisse a conclu des traités bilatéraux sur l'entraide judiciaire avec de nombreux pays. Il faut toutefois que certaines conditions minimales soient garanties en matière de respect du droit international et des principes de l'Etat de droit. La Suisse renonce donc à conclure de tels traités avec des pays où les droits de l'homme ne bénéficient pas de garanties suffisantes. Le droit suisse sur l'entraide judiciaire (art. 2 EIMP) n'admet une coopération en matière pénale que si l'Etat étranger respecte les principes de procédure énoncés dans la CEDH et dans le Pacte international relatif aux droits civils et politiques<sup>49</sup> (procès équitable, indépendance et impartialité des juges, droits de la défense, droit d'être entendu, etc.). C'est pour cette raison que la Suisse a jusqu'ici fait preuve de retenue dans la conclusion de tels traités. Par ailleurs, suivant sa pratique constante, la Suisse ne conclut pas de traités bilatéraux d'entraide judiciaire portant seulement sur certaines catégories de délits.

## **4.2.2                   Coopération policière**

Dans la pratique pénale, il arrive fréquemment qu'au moment où les autorités de poursuite pénale demandent l'entraide judiciaire pour un cas concret, et même longtemps avant, d'intenses échanges (d'informations) aient déjà eu lieu au niveau de la police, donc avant l'ouverture formelle d'une procédure pénale. La coopération internationale de la Suisse dans le domaine de la police s'appuie sur trois axes: la coopération multilatérale à l'échelle du globe, à travers Interpol (a), la coopération régionale en Europe (b) et la coopération bilatérale, plus particulièrement avec les Etats voisins (c).

#### *a. Coopération mondiale*

A l'échelle mondiale, l'instrument privilégié de la Suisse en matière d'échange d'informations de police est Interpol.

<sup>47</sup> Dernier acte: le 14 septembre 2005, le président de la Confédération Samuel Schmid a signé la Convention contre le terrorisme nucléaire au siège de l'ONU à New York.

<sup>48</sup> RS 0.351.12

<sup>49</sup> RS 0.103.2

### b. Coopération régionale

A l'échelon européen, la Suisse a accès à deux nouvelles plates-formes de coopération multilatérale grâce à son association à l'accord de Schengen et à l'accord de coopération avec Europol. L'accord de Schengen permettra à la Suisse d'intensifier la coopération policière, surtout grâce au système de recherche de personnes et d'objets SIS. Une catégorie de signalements spéciale permettra notamment de mieux suivre les itinéraires et destinations des terroristes lors de leurs déplacements<sup>50</sup>. La mission d'Europol<sup>51</sup> consiste à soutenir les Etats parties dans la prévention de la grande criminalité organisée et internationale, y compris le terrorisme, et dans la lutte contre ses manifestations. Grâce à l'accord de coopération conclu avec Europol, entré en vigueur le 1<sup>er</sup> mars 2006<sup>52</sup>, la Suisse pourra échanger des informations opérationnelles avec l'Office européen de police.

### c. Coopération bilatérale

La coopération bilatérale de la Suisse en matière de police repose actuellement sur des traités conclus avec six Etats<sup>53</sup>. Six autres traités de même nature ont été signés et devraient être ratifiés sous peu<sup>54</sup>. Le champ d'application matériel de ces traités est la lutte contre la criminalité en général. Les traités de ce type sont conclus en priorité avec nos voisins directs et avec des Etats de l'Europe de l'Est et de l'Europe du Sud-Est, autrement dit avec des partenaires revêtant une certaine importance dans le cadre de la lutte contre le crime organisé<sup>55</sup>.

Le traité d'entraide judiciaire conclu avec les Etats-Unis (TEJUS) constitue un cas spécial de coopération bilatérale dans la lutte contre le terrorisme. Suite à un événement sans précédent, les attentats du 11 septembre 2001, fedpol et le MPC ont conclu, sur la base de ce traité, un *Operative Working Arrangement (OWA)* avec les Etats-Unis dont le champ d'application est très étroit puisque limité à la coopération bilatérale dans le cadre des enquêtes sur les auteurs de ces attentats (Al-Qaïda et milieux connexes). L'accord est entré en vigueur le 4 septembre 2002<sup>56</sup>. Du point de vue du MPC, il a rempli son objectif, la dernière affaire ayant été transmise à l'Office des juges d'instruction fédéraux. Sur le plan de la police judiciaire, il a permis une coopération particulièrement étroite entre les autorités de poursuite pénale des deux pays (raccourcissement des voies administratives, communication simplifiée). De plus, le travail en étroite collaboration avec les enquêteurs américains a permis aux autorités suisses de poursuite pénale de bénéficier d'un précieux transfert de connaissances et d'expériences.

<sup>50</sup> Pour plus de précisions, voir message du Conseil fédéral du 1<sup>er</sup> octobre 2004 relatif aux «accords bilatéraux II», FF **2004** 5705 ss.

<sup>51</sup> Pour plus de précisions quant à cette organisation internationale et à l'accord de coopération conclu par la Suisse, voir message du Conseil fédéral du 26 janvier 2005, FF **2005** 895 ss.

<sup>52</sup> RS **0.360.268.2**

<sup>53</sup> Allemagne, France, Italie, Principauté de Liechtenstein / Autriche (traité trilatéral), Hongrie.

<sup>54</sup> Accords avec la Slovénie (FF **2005** 967), la Lettonie et la République tchèque (FF **2005** 3765), la Roumanie (FF **2006** 2185), l'Albanie et la Macédoine (FF **2006** 2127).

<sup>55</sup> Le réseau d'accords a été élargi sur la base d'un document stratégique dont le Conseil fédéral a pris acte en janvier 2003. Une nouvelle stratégie pour la période 2006–2009 doit être soumise au Conseil fédéral en cours d'année (2006).

<sup>56</sup> Pour plus de précisions au sujet de ce traité, voir Rapport du Conseil fédéral sur les traités internationaux conclus en l'an 2002 (FF **2003** 3764); pour les débats au Conseil national relatifs à l'OWA, voir également BO 9.3.2004.

La Suisse dispose encore d'un réseau d'attachés de police dans un petit nombre de pays. Ces agents de liaison jouent un rôle très important dans la lutte contre la criminalité transfrontalière, en optimisant la coopération internationale en la matière. Leur tâche consiste à créer un réseau d'interlocuteurs de confiance et à découvrir des sources d'informations. La vérification informelle de renseignements par le truchement des attachés de police est une méthode efficace et rapide qui a fait ses preuves en apportant un soutien optimal à la Confédération et aux cantons dans le cadre de leurs procédures d'enquête.

### 4.2.3 Coopération entre les services de renseignement

La lutte contre le terrorisme doit agir en amont, très tôt, afin de déjouer les projets si possible au stade de la planification ou des préparatifs. Mais après un attentat terroriste, la qualité du renseignement joue aussi un rôle de premier plan pour une identification rapide des auteurs.

En application de la LMSI et de l'OMSI, notre service de renseignement intérieur, le SAP, est chargé des relations entre la Confédération et les autorités étrangères qui accomplissent des tâches de sécurité au sens de la LMSI (art. 8 LMSI) et il représente la Suisse dans des instances internationales (art. 6 OMSI). La lutte contre le terrorisme représente aujourd'hui la majeure partie des échanges internationaux d'informations entre services de renseignement.

Dans le détail, le SAP échange des informations sur une base permanente avec environ 90 services partenaires appartenant à divers Etats et organisations internationales (par ex. l'ONU ou l'UE)<sup>57</sup>. Le SAP représente aussi la Suisse dans quatre organismes multilatéraux informels: le «Groupe antiterroriste» (un service pour chaque Etat de l'UE ainsi que pour la Norvège et pour la Suisse), le «Club de Berne» (services de renseignement de 22 pays), la «Middle European Conference» (services de 17 pays provenant principalement du Sud-Est de l'Europe) et le «Police Working Group on Terrorism» (unités de police antiterroriste de 26 pays). La conclusion d'un accord sur les procédures de sécurité dans les échanges d'informations classifiées est prévue afin de pouvoir échanger des renseignements avec le «Centre de situation» de l'UE<sup>58</sup>.

En ce qui concerne le cercle des partenaires étrangers, cet échange de renseignements répond aux besoins actuels de la Suisse en matière de lutte contre le terrorisme et le crime organisé. Toutefois, si la coopération des services de renseignement suisses avec l'étranger ne peut être garantie en raison d'une marge de manœuvre légale trop étroite sur le plan intérieur, le flux d'informations vers la Suisse risque peu à peu de tarir. Le Conseil fédéral va proposer de nouveaux instruments d'acquisition de renseignements (comme la surveillance préventive des télécommunications) aux Chambres fédérales avec le projet de révision LMSI II.

<sup>57</sup> La stratégie de coopération internationale du SAP est définie dans un document classé confidentiel que le Conseil fédéral a approuvé en juin 2005.

<sup>58</sup> L'accord a été approuvé par le Conseil de l'UE le 24 juin 2005 et par le Conseil fédéral le 29 juin 2005. L'UE procédera, dans une prochaine étape, à l'évaluation de la pratique suisse en matière d'utilisation des informations classifiées et, si le résultat de cet examen devait s'avérer positif, l'accord devrait être signé.

## 4.3

### Appréciation

Selon le Conseil fédéral, les instruments dont disposent actuellement les autorités suisses dans le domaine de la coopération internationale, y compris leur élargissement futur, peuvent globalement être qualifiés de suffisants. Il en conclut qu'aucune nouvelle mesure législative ne s'impose.

Dans le domaine de l'*entraide judiciaire* en particulier, le Conseil fédéral ne voit aucune nécessité de réviser l'EIMP, qui remplit encore son mandat. Dans un avis relatif à deux interventions parlementaires qui demandaient une révision totale de la législation sur l'entraide pénale internationale, le Conseil fédéral avait relevé qu'une fois la nouvelle procédure de recours en place, il n'y aura «pas de raison de procéder à des modifications législatives supplémentaires s'agissant de la procédure d'entraide judiciaire»<sup>59</sup>. Sur le fond, cette conclusion concerne autant les voies de recours des personnes visées par des mesures d'entraide judiciaire que d'autres thèmes de révision. Pour le Conseil fédéral, à moyenne échéance, il faudra mettre l'accent sur l'application absolue du droit en vigueur et des traités d'entraide pénale internationale. Pour ce qui est justement des traités, la Suisse dispose d'ores et déjà d'un bon réseau, et à ce sujet le Conseil fédéral espère pouvoir bientôt compter le Protocole portant amendement à la Convention européenne pour la répression du terrorisme au nombre des traités internationaux ratifiés par la Suisse.

Le Conseil fédéral examinera individuellement toute opportunité de développement bilatéral ou multilatéral de l'entraide judiciaire. A cet égard, l'évolution du droit au sein de l'UE revêt un intérêt particulier<sup>60</sup>.

Quant à la *coopération internationale entre les services de police*, dans sa stratégie pour les années 2006–2009 le Conseil fédéral a l'intention d'élargir les bases bilatérales de la coopération policière et d'étendre son réseau d'attachés de police. Les traités bilatéraux en matière policière qui ont déjà été ratifiés, de même que l'OWA conclu avec les Etats-Unis ou le traité qui le remplacera éventuellement<sup>61</sup> illustrent les diverses possibilités qui s'offrent à deux Etats, ou plus, qui manifestent un intérêt commun pour la création de nouveaux instruments de coopération en matière de police.

La *coopération internationale entre les services de renseignement* repose en grande partie sur la confiance réciproque et les informations sont très souvent échangées sur une base donnant-donnant. Les canaux de communication avec les partenaires du renseignement les plus importants pour la Suisse font l'objet d'une utilisation intensive.

<sup>59</sup> Avis du Conseil fédéral du 14 septembre 2005 relatifs aux motions Baumann J. Alexander (04.3174) «Meilleure protection des intérêts légitimes dans la procédure d'entraide judiciaire» et Frick Bruno (04.3368) «Procédure d'entraide judiciaire. Etat des lieux».

<sup>60</sup> Eurojust pourrait devenir intéressant pour la Suisse. Cette structure a été mise en place afin de faciliter la mise en pratique d'une communication directe entre les autorités et de coordonner les enquêtes et les poursuites pénales. Plusieurs Etats membres de l'UE «ont désigné des magistrats de liaison pour travailler de manière bilatérale avec d'autres pays de l'UE et favoriser ainsi l'entraide judiciaire» (Rapport annuel 2004 d'Eurojust, p. 17). Eurojust a fait part de son intérêt pour l'ouverture de négociations avec la Suisse, en indiquant que parmi les Etats tiers, la Suisse bénéficierait d'un traitement prioritaire.

<sup>61</sup> En mars 2005 le Conseil fédéral a décidé d'examiner s'il était possible de remplacer l'OWA par un traité bilatéral qui devrait être soumis à l'approbation du Parlement. Le contenu de ce traité, eu égard au TEJUS, serait essentiellement axé sur l'intervention de groupes d'enquête communs, comme dans le Deuxième Protocole additionnel du 8 novembre 2001 à la Convention européenne d'entraide judiciaire en matière pénale.

## 4.4

## Mesures

Le Conseil fédéral ne voit pas la nécessité de prendre de nouvelles mesures dans le domaine de la coopération internationale, en particulier dans celui de l'entraide pénale. Dans la mesure où les procédures d'entraide judiciaire à l'étranger accusent des retards, les autorités suisses ne cesseront de s'investir dans le renforcement des contacts directs sur place dans le but d'assurer un déroulement rapide de ces procédures. Dans le même temps, les efforts entrepris notamment dans l'élargissement progressif du réseau de traités d'entraide judiciaire et d'accords bilatéraux de coopération policière doivent se poursuivre.

## 5

## Protection extraprocédurale des témoins

### 5.1

### Contexte

#### 5.1.1

#### Mesures de protection des témoins

La protection des personnes dont le témoignage revêt un intérêt public peut être nécessaire tant dans le cadre des poursuites pénales que dans le domaine de la protection de l'Etat. Dans le contexte de la révision LMSI II actuellement en cours, la possibilité d'introduire une «protection des informateurs» est par exemple à l'étude. Etant donné que les mesures traitées dans le projet LMSI II ne font pas l'objet du présent rapport, les considérations qui suivent se concentrent sur la protection des témoins dans la procédure pénale.

Dans la procédure pénale, la question de la protection des témoins se pose à chaque fois que les moyens de preuve autres que les déclarations de témoins font défaut<sup>62</sup>. Plus les déclarations d'une personne sont capitales, plus le risque est grand de l'influencer afin d'empêcher la vérité d'émerger. L'objectif des mesures de protection des témoins est donc double: il s'agit d'une part de protéger les personnes dont l'intégrité corporelle et la vie sont menacées du fait de leur témoignage ou de leur participation à la procédure et d'autre part de garantir la poursuite de la procédure pénale en suscitant et en entretenant la volonté de déposer. Dans ce contexte, la notion de témoin ne doit pas être restreinte à la définition qu'en donne le droit de procédure pénale, mais s'étend à toute personne pouvant fournir des informations sur les faits (p.ex. le coaccusé considéré comme «personne appelée à fournir des renseignements» dans la procédure pénale) ou devant s'exprimer durant la procédure (p.ex. comme interprète ou comme expert)<sup>63</sup>.

Les mesures de protection des témoins se subdivisent en mesures procédurales et extraprocédurales. Les mesures *procédurales* sont destinées à protéger les témoins qui interviennent durant la procédure. Elles sont régies par des dispositions spéciales du droit de procédure. Outre le droit de refuser son témoignage, ces mesures comprennent notamment le secret partiel ou intégral sur l'identité du témoin durant la

<sup>62</sup> Ce constat avait d'ailleurs été à l'origine de la révision de la procédure militaire qui a introduit des dispositions sur la protection des témoins, notamment dans le cadre des procès de criminels de guerre; voir message du 21 janvier 2003 concernant la modification de la procédure pénale militaire (Protection des témoins) FF **2003** 693 ss.

<sup>63</sup> Cette extension de la notion de témoin est également acceptée par le Comité des Ministres du Conseil de l'Europe, la Cour européenne des droits de l'homme et les tribunaux pénaux internationaux; voir ATF **125** I 127, 132, consid. 6a.

procédure. En Suisse, la procédure pénale de certains cantons ainsi que quelques lois fédérales spéciales prévoient des droits protecteurs dans la procédure, pour les témoins en général ou pour certaines catégories de témoins<sup>64</sup>. Ces droits ont été intégrés dans le P-CPP.

Les mesures *extraprocédurales* ont pour but de protéger une personne menacée en dehors des actes de procédure à proprement parler, notamment pendant et après le procès. Contrairement aux droits protecteurs procéduraux, ces mesures n'affectent pas les garanties de procédure de l'accusé (droits de la partie et droits de la défense). On citera par exemple le conseil sur la manière de se comporter, la mise à disposition d'instruments tels qu'un nouveau numéro de téléphone portable ou un système d'alarme, la protection personnelle, le logement provisoire dans un lieu sûr, le blocage des données, la mise à disposition d'une identité d'emprunt provisoire, voire le changement d'identité définitif. On désigne par «programme de protection de témoin», un ensemble de mesures de protection spécifiques convenu entre les autorités et la personne protégée.

Partant de cette définition de la protection extraprocédurale des témoins dans le contexte des poursuites pénales, le présent chapitre se propose d'examiner l'importance de cette forme de protection des témoins dans la lutte contre le terrorisme et le crime organisé et d'exposer des mesures envisageables.

## 5.1.2 Délimitation de la réglementation relative aux témoins «de la Couronne»

Il convient d'établir une distinction entre la protection des témoins et les réglementations relatives aux témoins «de la Couronne», autrement dit les témoins à charge, en usage dans les systèmes juridiques d'inspiration anglo-saxonne. Le but de ces réglementations n'est pas de protéger les témoins, mais uniquement de favoriser l'émergence de la vérité. Le principe consiste à inciter les coupables à témoigner contre leurs complices en échange de l'immunité pénale ou d'autres avantages. Les mesures de protection des témoins deviennent une composante nécessaire de la réglementation relative aux témoins à charge, voire une condition impérative lorsque, par ses déclarations, le témoin s'expose à des représailles. La mise en place d'une réglementation relative aux témoins à charge assortie d'une éventuelle suppression de peine a été envisagée dans le cadre de l'unification de la procédure pénale suisse, mais cette possibilité n'a pas été retenue en raison de certains doutes quant à sa légitimité et parce qu'elle ne semble pas répondre à un besoin réel dans notre pays<sup>65</sup>. Les motifs évoqués à l'époque sont toujours valables<sup>66</sup>. Il faut cependant relever que le droit en vigueur prévoit déjà des incitations à la coopération dans le cadre du procès: en application de l'art. 260<sup>ter</sup> CP, le juge peut atténuer la peine d'un coaccusé qui s'est efforcé d'empêcher l'organisation de poursuivre son activité

<sup>64</sup> Voir les dispositions y relatives des codes de procédure pénale des cantons de BL, BS, BE, FR, SG, ZH, de la loi vaudoise sur la police cantonale, ainsi que de la LFIS, pour les témoins par profession (RS 312.8), et de la LAVI, pour les victimes appelées à déposer (RS 312.5).

<sup>65</sup> «De 29 à l'unité», Concept d'un code de procédure pénale fédéral, Rapport de la Commission d'experts, DFJP, juin 2001, p. 56 ss.

<sup>66</sup> En Europe, l'Italie et l'Allemagne ont adopté des réglementations relatives aux témoins «de la Couronne». L'Allemagne a supprimé la sienne en 1999 car elle n'a pas produit les effets escomptés et n'a été utilisée que très rarement.

criminelle<sup>67</sup>. D'une manière générale, la jurisprudence du TF admet que la coopération d'un accusé puisse entraîner une atténuation importante de la peine.

## 5.2 Etat des lieux

### 5.2.1 Protection extraprocédurale des témoins en Suisse

#### *a. Situation juridique*

Le droit pénal ordinaire ne contient aucune norme juridique, ni sur le plan fédéral ni sur le plan cantonal, régissant spécifiquement et intégralement les conditions dans lesquelles des mesures de protection extraprocédurales, voire des programmes de protection des témoins peuvent être mis en place, ni selon quelles modalités.

C'est pourquoi les mesures de protection extraprocédurales s'appuient sur le mandat général de protection qui incombe aux cantons et oblige leur corps de police à prévenir les risques directs pour la vie et l'intégrité corporelle des citoyens. Ce principe est formulé de manière générale dans les législations cantonales sur la police, parmi les tâches du corps de police. Dans sa jurisprudence, le TF a par ailleurs établi que, en vertu de l'art. 10 Cst. et de l'art. 2 CEDH, l'obligation de témoigner avait pour corollaire une obligation positive de l'Etat d'assurer la protection des personnes qui courent un risque du fait de leur témoignage<sup>68</sup>.

La LFIS contient une règle qui vise concrètement les témoins menacés et qui permet la mise en place de mesures de protection pour les agents infiltrés, par conséquent des témoins par profession. Conformément à l'art. 9 LFIS, ces agents ont droit à la meilleure protection possible de leur vie et de leur intégrité corporelle<sup>69</sup>. La nouvelle loi sur les étrangers adoptée par les Chambres fédérales le 16 décembre 2005 crée aussi les conditions nécessaires à l'adoption de mesures de protection supplémentaires en faveur des témoins de la traite d'êtres humains puisque, pour cette catégorie de personnes, elle permet de déroger aux règles d'admission usuelles dans le cadre de la réglementation sur le séjour des étrangers.

#### *b. Situation pratique*

Faute de normes juridiques spécifiques sur la protection extraprocédurale des témoins, la Suisse ne pratique actuellement aucun programme de protection de témoins à proprement parler. Au niveau cantonal, il existe des cas où des personnes menacées ont pu se mettre à l'abri temporairement dans un autre canton, voire plus longtemps sous une nouvelle identité, grâce au concours de différents services<sup>70</sup>, mais il s'agit de cas isolés qui, sur le plan juridique, ont été réglés dans le cadre du

<sup>67</sup> Le code pénal autrichien (§ 41a) prévoit un système semblable connu comme la «petite réglementation relative aux témoins de la Couronne».

<sup>68</sup> ATF 1A.32/1999 du 13 septembre 1999, publié dans EuGRZ 2000, 451.

<sup>69</sup> Des mesures de protection ne visant pas spécifiquement les témoins sont énoncées dans l'OSF, qui prévoit que les agents de la Confédération exposés à des risques peuvent bénéficier d'une protection personnelle et d'un conseil sur des mesures architectoniques et techniques. De son côté, la LAVI (RS 312.5) prévoit une protection minimale sous forme de conseil et d'assistance pour les victimes au sens de la loi.

<sup>70</sup> Dans l'affaire de l'assassinat du maître d'école de St-Gall, la fille du condamné a par exemple reçu une nouvelle identité (voir Tagblatt du 25 avril 2001, «Eine neue Heimat und ein neuer Name»).

mandat général de protection qui incombe aux pouvoirs publics. Il serait donc abusif de parler d'institutionnalisation de la protection des témoins.

L'absence de réglementation légale spécifique à la protection extraprocédurale des témoins est la cause d'insécurité juridiques et de problèmes.

- *Attribution matérielle des tâches inexistante, notamment lacune de compétence de la P.J.F.*: les mesures de protection des témoins ont un statut particulier. Elles servent à limiter les risques, mais vont bien au-delà du mandat de police de sécurité dévolu à la police. Le domaine de tâches «protection des témoins» ne peut donc pas être attribué à la police ordinaire. Certains pays ont ainsi créé un service spécialisé dans la protection des témoins au sein de leur corps de police<sup>71</sup>. Pour créer de telles unités, il faut toutefois disposer d'une compétence légale et il faut aussi que la protection extraprocédurale des témoins soit institutionnalisée. Cette base est d'autant plus nécessaire dans le cadre de la lutte contre la grande criminalité qui incombe à la P.J.F, cette dernière n'ayant aujourd'hui aucun mandat de police de sécurité comparable à celui dont sont investis les corps de police cantonaux.
- *Incertitudes quant à la compétence territoriale*: les mesures de protection des témoins relèvent de la police et de son mandat de prévention des risques, mais elles sont aussi étroitement liées à la procédure pénale. La question de la compétence territoriale pour l'exécution des mesures de protection extraprocédurales n'est pas résolue (autorités du for judiciaire ou autorités du domicile – pas toujours clair – de la personne à protéger?).
- *Inexistence de normes de compétence contraignantes*: des dispositions légales concrètes sont nécessaires pour qu'il soit possible de prendre des mesures de protection spécifiques comme le blocage des données dans des services publics et privés ou la fabrication et l'émission de papiers d'identité d'emprunt pour les personnes menacées. A défaut de bases légales, les services publics et privés ne peuvent être ni autorisés ni obligés à collaborer. Sans un cadre institutionnel et légal, même les mesures de protection les plus rudimentaires (conseil en comportement, protection des objets et des biens, logement en lieu sûr) sont limitées a priori, faute de ressources.
- *Coordination nationale plus difficile*: pour atteindre l'objectif visé, il faut que toutes les instances impliquées procèdent de manière coordonnée et structurée. Et à plus forte raison parce que la Suisse a une structure fédéraliste et un territoire exigu. Dans ces conditions, une collaboration étroite entre les autorités fédérales, cantonales et communales de justice et de police, mais aussi avec d'autres administrations et institutions publiques (par exemple l'ODM et les offices des affaires sociales) revêt une importance capitale pour le succès des mesures de protection des témoins. Or l'absence de normes de compétences complique la collaboration entre toutes ces instances.
- *Coopération internationale plus difficile*: une coopération internationale est également nécessaire pour les cas de menace extrême où le territoire suisse est trop exigu pour garantir une protection adéquate au témoin menacé. En cas de nécessité, les personnes qui doivent être protégées pourraient être déplacées temporairement à l'étranger ou pour une plus longue durée.

<sup>71</sup> Autriche, Belgique, Allemagne.

L'absence de bases juridiques complique la coopération internationale et peut même la rendre impossible.

### **5.2.2 Importance des mesures extraprocédurales dans la lutte contre le terrorisme et le crime organisé**

Les caractéristiques principales du monde du crime organisé sont le cloisonnement de l'organisation vis-à-vis de l'extérieur et le mode d'action planifié de ses protagonistes. Les criminels qui agissent par métier connaissent les méthodes d'investigation de la police et évitent de laisser des traces telles que des déclarations compromettantes au téléphone. Dans ces conditions, les déclarations des témoins sont donc capitales, car les preuves matérielles sont souvent insuffisantes. Dans le cadre de la poursuite pénale, l'issue de la procédure dépend donc considérablement du témoignage des personnes (participant entendu comme témoin, victime appelée à déposer) qui, en raison de leur proximité avec les auteurs, sont en mesure de délivrer des informations précises sur les participants à l'action, sur la planification et le déroulement de l'action, ou encore sur la structure de l'organisation. Les organisations criminelles le savent aussi, et c'est pourquoi elles n'hésitent pas à exercer des pressions ou des repréailles. Dans certains cas, il peut donc s'avérer nécessaire d'adopter des mesures de protection des témoins et de leurs proches afin de les mettre à l'abri des pressions physiques et psychiques et de les inciter à déposer.

Un bref tour d'horizon à l'étranger montre que le développement des programmes policiers de protection des témoins est lié au renforcement de la lutte contre le crime organisé, tant aux Etats-Unis qu'en Europe. Constatant qu'il est très difficile d'apporter la preuve des délits commis par les organisations criminelles sans le concours de témoins et d'informateurs, divers pays étrangers ont adopté des mesures de protection étendues et créé des structures spécifiques qu'ils ont chargées de leur application<sup>72</sup>. Les rapports et statistiques établis annuellement, par exemple en Allemagne, confirment le bien-fondé et l'utilité de la protection des témoins dans la lutte contre la grande criminalité. De nombreux Etats de l'UE, parmi eux des pays dont la taille et la population sont comparables à celles de la Suisse, disposent aujourd'hui de programmes de protection extraprocédurale des témoins dont l'ampleur est variable<sup>73</sup>. L'an dernier, le Conseil de l'UE a en outre chargé la Commission d'élaborer un programme de protection de témoins en se basant sur les travaux préliminaires effectués par Europol<sup>74</sup>.

De par sa position géographique au cœur de l'Europe, son secteur financier bien développé et ses infrastructures ultramodernes, la Suisse attire les groupements qui gravitent autour des multinationales du crime organisé. On peut obtenir de bons résultats par l'enquête sous couverture, en infiltrant un agent, autrement dit un témoin par profession, dans l'organisation. Cette méthode d'investigation est toutefois lourde et non sans danger pour l'agent infiltré. Le recours aux témoignages des complices ou des victimes de l'organisation est donc une option qui doit être prise

<sup>72</sup> Informations sur divers pays dans l'avis de droit 05-161: Bekämpfung von Terrorismus und organisiertem Verbrechen, ISDC, Lausanne 2005; Buggisch Walter, Zeugenbedrohung und Zeugenschutz in Deutschland und den USA, Berlin 2001, 303.

<sup>73</sup> Allemagne, France, Italie, Autriche, Espagne, Belgique, Pays-Bas, République tchèque, Grande-Bretagne, Norvège, Suède.

<sup>74</sup> Communication de la Commission du 10 juin 2005.

en considération. Les cantons et la PJJ ont toutefois vécu des situations, en particulier dans les domaines du trafic d'armes et de stupéfiants, de la traite d'êtres humains et du trafic de migrants, et plus généralement du crime organisé, où des témoins potentiels, par crainte ou suite à de lourdes menaces, n'étaient prêts à déposer que contre la garantie d'une protection appropriée. La pratique de la PJJ montre aussi que des conditions de participation active à l'enquête doivent être créées dès le début de la procédure, notamment par le biais d'une protection adéquate pour les témoins. Etant donné que dans la plupart des cas le prévenu et le témoin se connaissent, les mesures procédurales telles que la garantie de l'anonymat durant la procédure sont le plus souvent insuffisantes. Il existe en effet un risque que l'auteur puisse remonter jusqu'à l'identité du témoin par déduction (p.ex. à l'aide du contenu de son témoignage) ou d'une autre manière.

En Suisse, une protection extraprocédurale des témoins serait également utile en rapport avec l'atténuation de peine prévue à l'art. 260<sup>ter</sup>, ch. 2, CP, qui se conçoit comme une «récompense» pour les transfuges d'organisations criminelles. Dans le monde du crime organisé, celui qui témoigne s'expose à un fort risque de représailles. Dans ce contexte, si la garantie d'une atténuation de la peine constitue une incitation à témoigner, c'est surtout l'octroi d'une protection appropriée qui est décisif. La mise en place de mesures extraprocédurales pourrait ainsi accroître l'importance pratique de cette disposition<sup>75</sup>.

### 5.3 Appréciation

De manière générale, il apparaît qu'en Suisse, comme à l'étranger, faute de preuves matérielles, l'efficacité de la lutte contre le terrorisme et le crime organisé dépend dans une large mesure des dépositions de témoins. Mais dans la plupart des cas, les témoins menacés ne se déclarent et ne restent prêts à déposer que s'ils reçoivent la garantie d'une protection adéquate. Les droits à une protection procédurale tels qu'ils sont définis dans le droit suisse et dans le P-CPP constituent un volet important de la protection des témoins, mais ils ne suffisent plus lorsque l'auteur de l'infraction connaît le témoin ou qu'il a pu se procurer son identité. En pareille situation, pour que le témoin maintienne sa déposition, des mesures de protection extraprocédurales (mesures appliquées en dehors des actes de procédure et après le procès) peuvent donc souvent à elles seules se révéler appropriées pour le mettre à l'abri de tout acte d'intimidation ou de représailles.

Faute d'une norme légale spécifique à la protection extraprocédurale des témoins, aucun programme de protection de témoins n'est actuellement mis en œuvre dans le cadre des procédures de la PJJ. En pratique, cela signifie que les témoins menacés, qui pourraient faire des révélations intéressantes sur les faits, refusent de déposer.

<sup>75</sup> A cet égard, voir Trechsel Stefan, *Kurzkommentar Schweizerisches Strafgesetzbuch*, 3<sup>e</sup> éd., ad art. 260<sup>ter</sup>, ch. 12. Vu l'évolution de la criminalité organisée, en 2004, la France a également adopté des dispositions introduisant des mesures extraprocédurales de protection des participants entendus comme témoins. Ces derniers peuvent ainsi bénéficier d'une réduction, voire d'une exemption de peine si leurs déclarations permettent de déjouer d'autres crimes.

De fait, l'administration des preuves ne peut être exhaustive dans la poursuite pénale du crime organisé<sup>76</sup>.

## **5.4 Mesures**

### **5.4.1 Possibilités de protection extraprocédurale des témoins**

Par référence à la littérature et au cinéma, on associe souvent les programmes de protection de témoins à un changement d'identité définitif et au début d'une nouvelle vie ailleurs. Dans la réalité, la protection extraprocédurale des témoins est plus nuancée et peut aller de la variante la plus simple comme le conseil sur la manière de se comporter, jusqu'à la variante maximale qui serait le changement d'identité définitif, en passant par des stades intermédiaires comme le logement temporaire dans un lieu sûr ou la mise à disposition d'une identité d'emprunt<sup>77</sup>. Le cercle des bénéficiaires peut aussi être défini de façon plus ou moins restrictive afin d'y inclure certaines catégories de témoins seulement, ou uniquement les témoins intervenant dans certains types d'enquêtes sur la grande criminalité, mais aussi, éventuellement, de l'élargir aux proches des témoins.

Les conséquences de la protection des témoins, notamment au niveau des coûts et du travail requis, ainsi que les problèmes juridiques et matériels qui peuvent se poser, dépendent fortement de la nature et de la durée des mesures de protection envisagées et varient donc selon les cas. Les conséquences financières et juridiques des mesures de protection deviennent considérables lorsque, à la mise à l'abri dans un lieu sécurisé, s'ajoute la mise à disposition temporaire d'une identité d'emprunt, voire un changement d'identité définitif. Pour créer une identité d'emprunt, et surtout pour prévenir une reconstitution de l'ancienne identité, il peut s'avérer nécessaire de manipuler les données de nombreux registres<sup>78</sup>. On notera aussi que le changement d'identité ne doit pas altérer le statut juridique des tiers, les créanciers par exemple. Les programmes menés à l'étranger montrent qu'il est possible de contrer ces effets de diverses manières<sup>79</sup>.

Par ailleurs, il faut relever que le fait de vivre plus ou moins longtemps sous une identité d'emprunt, dans un nouveau contexte social, peut provoquer un stress psychique chez le témoin et éventuellement chez ses proches. Cela peut aussi donner lieu à l'émergence d'une mentalité d'assisté qui peut ensuite poser problème lors du retour à la vie normale, une fois la menace disparue. Outre la vérification préalable des critères d'aptitude pour être intégré dans un programme, le service responsable

<sup>76</sup> Voir Hug Thomas, Zeugenschutz im Spannungsfeld unterschiedlicher Interessen der Verfahrensbeteiligten, RPS 116 1998, 405.

<sup>77</sup> Certains pays européens n'envisagent que la mise à disposition (temporaire) d'une identité d'emprunt (p. ex. Allemagne, Autriche, Norvège), tandis que d'autres permettent un changement d'identité à tous les effets (p. ex. Italie, Suède, Belgique).

<sup>78</sup> Commune, canton et Confédération, assurances sociales, armée, etc. Lors d'un changement d'identité définitif, la question des effets légaux en cas de divorce, de mariage, de naissance, etc. est complexe.

<sup>79</sup> Dans les affaires, le service de protection des témoins joue le rôle d'intermédiaire entre les deux identités et effectue les opérations nécessaires. L'usage abusif de l'identité d'emprunt peut entraîner l'exclusion du programme de protection.

de la protection des témoins doit aussi garantir un conseil et un suivi individuel appropriés.

Dans plusieurs pays, les tâches administratives et opérationnelles liées à la mise en œuvre de la protection des témoins sont généralement prises en charge par un service spécialisé<sup>80</sup>. L'instance de décision pour les mesures les plus lourdes, telles que la création d'une identité d'emprunt, se situe souvent à un niveau ministériel<sup>81</sup>. La pratique des pays étrangers montre que, dans bien des cas, des mesures d'assistance et de suivi ainsi que le logement temporaire dans un lieu sûr répondent adéquatement au besoin de protection des témoins.

Face aux cas de protection de témoins qui pourraient survenir dans des procédures pénales cantonales, il faudra, pour des questions de sécurité, s'efforcer de mettre en place une procédure de protection des témoins uniformisée sur le plan fédéral. Vu l'exiguïté du territoire helvétique, une protection efficace exige une coopération basée sur des conditions et des standards identiques. A cet égard, il faudra encore examiner dans quelle mesure une réglementation fédérale pourrait s'intégrer dans la répartition des compétences prévue par la Constitution fédérale<sup>82</sup>.

#### 5.4.2 Propositions pour la Suisse

Après avoir dûment pondéré les avantages et les inconvénients de la protection extraprocédurale des témoins, le Conseil fédéral considère que des mesures de cette nature, mises en œuvre dans un cadre de proportionnalité, peuvent contribuer concrètement à optimiser les poursuites pénales des autorités fédérales et à lutter contre le crime organisé.

Ces mesures viseraient en premier lieu les personnes qui sont menacées dans le cadre d'enquêtes sur la grande criminalité, notamment sur le crime organisé et le terrorisme, et qui détiennent des informations décisives pour l'issue de la procédure. Il s'agirait principalement des participants entendus comme témoins, des témoins par profession ainsi que des victimes appelées à déposer. Le cas échéant, la protection devrait également être étendue aux personnes menacées du fait de leur implication dans la procédure, par exemple les juges, et aux proches des témoins, la menace pesant sur eux pouvant représenter un moyen de pression efficace à l'encontre du témoin.

Pour le Conseil fédéral, l'option du changement d'identité définitif n'est pas prioritaire. Il penche plutôt pour des mesures telles que le transfert du domicile et la possibilité de créer une identité d'emprunt provisoire pour les témoins.

Vu les difficultés évoquées au ch. 5.2.2 de nouvelles dispositions doivent être adoptées afin d'instituer la protection extraprocédurale des témoins dans une loi formelle et de jeter les bases d'une action coordonnée et harmonisée, notamment en vue de la

<sup>80</sup> Dans des pays comme l'Autriche, la Belgique ou les Pays-Bas, la taille de ce service est d'environ un collaborateur pour un million d'habitants.

<sup>81</sup> Autriche, Belgique, Pays-Bas.

<sup>82</sup> Vu le lien étroit avec la procédure pénale, qui doit être considérée comme la cause de la protection des témoins, cette dernière ne peut être exclue a priori. Comparer avec la loi allemande du 11 décembre 2001 sur l'harmonisation de la protection des témoins (Gesetz zur Harmonisierung des Schutzes gefährdeter Zeugen).

coopération internationale<sup>83</sup>. Il s'agit donc de créer des normes qui confèrent aux autorités fédérales le droit d'adopter des mesures de protection dans leur sphère de compétences, qui définissent les conditions dans lesquelles des mesures de protection des témoins peuvent être prononcées et fixent les obligations des autorités et des entreprises privées en matière de collaboration (p.ex. création d'une identité d'emprunt provisoire pour bloquer les données communicables ou pour assurer le maintien du secret). Ces normes pourraient faire l'objet d'une loi spéciale sur la protection des témoins ou de modifications ponctuelles de lois existantes.

Le Conseil fédéral charge le DFJP de créer dans le droit fédéral les conditions en vue de la mise en œuvre de mesures extraprocédurales de protection des témoins.

## **6 Recours à l'exploration radio et à la surveillance des télécommunications**

### **6.1 Contexte**

Les ressources du DDPS dans le domaine de l'exploration radio (CGE) sont affectées à la recherche d'informations à l'étranger. Actuellement, elles sont exclusivement accessibles aux services de renseignement. L'exploration radio ne doit pas être confondue avec la surveillance des télécommunications, qui sert à se procurer des informations à l'intérieur des frontières nationales. Le DETEC (STS) accomplit la surveillance des télécommunications sur mandat des autorités de poursuite pénale.

L'évolution galopante des technologies de télécommunication et leur complexité croissante représentent un défi permanent pour les organismes chargés de l'exploration radio et de la surveillance des télécommunications. Dans la téléphonie en particulier, le mode de transmission actuel via les centrales de commutation des opérateurs va progressivement céder le pas à la téléphonie sur Internet (VoIP). Avec cette technologie, les communications sont transmises à travers le réseau Internet par paquets de données et ne passent plus par les centraux des fournisseurs de services de télécommunications. Or c'est justement à cet endroit que s'opère aujourd'hui la surveillance des télécommunications. De plus, les paquets de données sont acheminés individuellement à travers l'Internet, en fonction des disponibilités du réseau, et ne sont regroupés qu'à destination, ce qui complique grandement la surveillance du trafic.

Le postulat propose d'autoriser les autorités fédérales de poursuite pénale à recourir aux ressources de la guerre électronique. Il demande en particulier de vérifier si l'exploration radio peut être utilisée sur mandat du MPC dans le but de rechercher des informations à l'étranger lorsque l'entraide judiciaire est impossible. Dans ce chapitre, il s'agira de procéder à l'étude de cette question ainsi que d'autres mesures en vue d'une utilisation plus efficace des moyens de l'exploration radio et de la surveillance des télécommunications, car l'une comme l'autre s'appuient en partie sur des technologies comparables, sinon identiques.

<sup>83</sup> Voir la recommandation du 20 avril 2005 du Comité des ministres du Conseil de l'Europe (Recommandation Rec (2005)9 relative à la protection des témoins et des collaborateurs de justice), dont il faudra tenir compte si des bases légales sont élaborées en la matière.

## **6.2 Etat des lieux**

### **6.2.1 Recherche d'informations à l'étranger par les autorités fédérales de poursuite pénale**

Dans la recherche de documents et d'informations à l'étranger, le MPC et l'Office des juges d'instruction fédéraux, qui sont les instances fédérales de poursuite pénale et d'accusation, doivent se tenir aux règles de l'entraide administrative et judiciaire, qui sont régies par les législations internes des pays impliqués et par le droit des gens, lorsqu'il s'applique<sup>84</sup>. Généralement, les mesures de surveillance mises en œuvre pour acquérir des moyens de preuves empiètent fortement sur les droits fondamentaux des personnes soupçonnées. C'est pourquoi les exigences sont très strictes en ce qui concerne le degré de précision des bases légales applicables et l'examen de la légalité des décisions prises sur ces bases. Ces exigences s'étendent également au mode d'acquisition des informations produites comme moyen de preuve durant la procédure.

Selon le principe de territorialité, la recherche des moyens de preuve à l'étranger est en principe régie par le droit du pays concerné. Lorsque les documents requis ne sont pas librement accessibles, ils ne peuvent donc être acquis que par les autorités locales compétentes et être utilisés uniquement avec leur consentement, sur la base du droit local. L'acquisition de tels moyens de preuve aux fins de poursuite pénale sans l'autorisation expresse des autorités locales compétentes doit ainsi être considérée comme un acte de souveraineté accompli illégalement sur le territoire d'un Etat tiers. C'est pourquoi, la recherche d'informations dans les sources étrangères qui ne sont pas librement accessibles doit se faire par le biais de l'entraide judiciaire internationale, quels que soient les moyens techniques utilisés. Il n'existe actuellement aucune base légale permettant la surveillance des télécommunications étrangères au moyen de l'exploration radio de la CGE au profit des autorités de poursuite pénale de la Confédération.

### **6.2.2 Recherche d'informations à l'étranger par les services de renseignement**

L'art. 99 LAAM confie aux services de renseignement le soin de rechercher des informations à l'étranger<sup>85</sup>. L'exploration radio de la CGE est un moyen de collecter des informations. Aux termes de l'art. 9a OMSI, le SAP, à savoir le service de renseignement intérieur, peut confier des mandats de surveillance de télécommunications étrangères. En sa qualité d'autorité de surveillance des services de renseignement, la Délégation des Commissions de gestion des Chambres fédérales s'est penchée en 2003 sur le système d'interception des communications par satellite du DDPS (projet ONYX). Dans son rapport du 10 novembre 2003 elle recommandait au Conseil fédéral d'examiner l'opportunité d'introduire une référence explicite, dans la LAAM, aux interceptions de communications à l'étranger et de présenter une disposition légale régissant ce type d'interceptions dans le domaine de la sûreté intérieure. Ces points ont été pris en considération dans le cadre du projet LMSI II

<sup>84</sup> LOC (art. 2 ss.), CP (art. 351<sup>er</sup> ss.), EIMP (art. 27 ss. et 63 ss.), LCPI (art. 10 et 11, RS 351.6) et un grand nombre de traités internationaux.

<sup>85</sup> Les bases légales concernant la recherche d'informations relevant du renseignement en Suisse figurent essentiellement dans la LMSI.

qui devrait être mis en consultation courant 2006. Cette révision prévoit notamment d'intégrer dans la LMSI l'art. 9a OMSI sur l'exploration radio et d'introduire dans la LAAM une nouvelle disposition sur l'utilisation de l'exploration radio par les services de renseignement du DDPS.

### **6.2.3 Communication des découvertes fortuites**

Lorsque les organes de la CGE recueillent des informations à l'étranger dans le cadre de l'exploration radio permanente, ils peuvent les transmettre à fedpol si elles paraissent importantes pour la sûreté intérieure ou pour la poursuite pénale (communication de constatations ou de découvertes fortuites)<sup>86</sup>. En principe, ces informations recueillies fortuitement sont donc aussi accessibles au MPC. C'est d'ailleurs à ce dernier qu'il incombe d'examiner si ces éléments peuvent être utilisés dans la procédure pénale ou s'il convient de les corroborer par des moyens de preuve complémentaires. A noter que le matériel acquis à l'étranger dans le cadre de l'exploration radio permanente bénéficie de la protection des sources<sup>87</sup>.

Dans d'autres pays, les règles sur l'exploration radio autorisent l'échange d'informations ainsi que la collaboration entre les organes du renseignement et ceux de la justice, pour autant que cela soit dans la compétence matérielle des autorités impliquées. En Allemagne et en Autriche, l'échange et la collaboration ne sont toutefois possibles qu'au cas par cas. La réglementation des autorisations par nature des sources (comme dans l'OCGE) est donc une particularité helvétique.

### **6.3 Appréciation**

Que la CGE soit autorisée à transmettre des découvertes fortuites à fedpol si elles peuvent être importantes pour la sûreté intérieure ou pour la poursuite pénale et que ces informations puissent ensuite être mises à la disposition du MPC ne légitime pas ce dernier à donner un mandat direct et ciblé à la CGE pour acquérir des informations à l'étranger. Une surveillance directe des télécommunications à l'étranger par la CGE sur mandat et pour le compte du MPC semble donc non admise par le droit actuel.

Le fait qu'une telle surveillance ne soit possible que dans des cas exceptionnels, comme le suggère le postulat, par exemple lorsque l'entraide judiciaire est impossible ou lorsque le temps presse, ne changerait rien à la situation juridique. Il faut aussi se rendre compte que les informations acquises par le biais de l'exploration radio ne sont pas comparables à celles obtenues par la voie de l'entraide judiciaire. Les informations de la CGE ne sont jamais complètes et ne peuvent pratiquement pas être utilisées en justice, en raison de la clause de protection des sources, ce qui signifie que des moyens de preuve supplémentaires devraient de toute manière être recherchés. Dans les conditions actuelles, il n'est donc pas certain qu'un mandat de surveillance confié à la CGE par le MPC pour acquérir des informations à l'étranger soit réellement utile pour accroître l'efficacité de la lutte contre le terrorisme et le crime organisé. La preuve du besoin n'est pas encore faite. Par conséquent, le

<sup>86</sup> Art. 99, al. 2<sup>bis</sup>, LAAM; art. 5, al. 3, OCGE

<sup>87</sup> Art. 99, al. 4, LAAM

Conseil fédéral estime qu'il n'y a pas lieu, actuellement, d'envisager la création de bases juridiques dans une loi formelle – nécessaire à cette fin – pour utiliser les moyens de la CGE afin de rechercher des informations à l'étranger pour le MPC.

Les mêmes considérations sont valables en ce qui concerne des mandats de surveillance directe des télécommunications à l'étranger que la PJJ pourrait donner aux organes de la CGE en sa qualité de police judiciaire.

## **6.4 Mesures**

Etant donné qu'aucune intervention ne s'impose sur le plan législatif, les mesures destinées à exploiter plus efficacement les ressources de l'exploration radio et de la surveillance des télécommunications doivent se concentrer sur les aspects organisationnels.

### **6.4.1 Renforcement de la collaboration**

Les possibilités existantes de transmission des informations doivent être exploitées, et de manière plus ciblée. La collaboration dans le respect et les limites du droit en vigueur doit être encouragée et à cet égard, le 22 juin 2005, le Conseil fédéral a adopté des mesures destinées à améliorer les fonctions et la coordination des services de renseignement. Il est avant tout prévu de créer des plates-formes d'évaluation et d'analyse dans les domaines d'activités communs aux deux services de renseignement, au sein desquelles les services d'évaluation et d'analyse des deux services coordonneront leurs travaux et regrouperont les informations acquises dans les domaines du terrorisme, du crime organisé et de la prolifération. Puisque les plates-formes coordonneront les différents besoins de renseignements, cette coopération induira aussi une coordination de l'utilisation des moyens de recherche. De cette manière, les ressources de la CGE seront utilisées plus efficacement par le renseignement et la transmission d'éventuelles informations aux organes de poursuite pénale sera mieux coordonnée.

Etant donné que, comme cela a été évoqué en introduction, l'exploration radio et la surveillance des télécommunications reposent sur des technologies semblables voire identiques, la collaboration technique doit être intensifiée afin d'optimiser l'utilisation des ressources et du savoir-faire disponibles. Les échanges d'informations qui se pratiquent déjà doivent aussi être intensifiés entre les unités administratives impliquées. Un échange d'expériences périodique permettra d'identifier le potentiel de synergies et de l'exploiter. Cela pourrait aussi déboucher sur des études communes. Enfin, il faut préparer des projets pour l'acquisition commune de systèmes, jusqu'à une interconnexion future des moyens techniques.

### **6.4.2 Evaluation d'une utilisation des moyens de l'exploration radio en Suisse**

La loi actuelle ne permet pas à la CGE de surveiller des réseaux de communication suisses, l'art. 5, al. 1, OCGE restreignant les activités de cette division du DDPS à l'exploration radio à l'étranger. Vu la rapidité à laquelle évoluent les technologies,

on pourrait néanmoins envisager le recours aux ressources de la CGE affectées à l'exploration radio pour garantir une surveillance efficace des télécommunications sur le territoire national (cf. 6.1). S'agissant de la recherche d'informations par les services de renseignement, l'opportunité de procéder, sur mandat du SAP, à la surveillance de cibles à l'intérieur du pays à de strictes conditions sera examinée dans le cadre de la révision de la LMSI. S'agissant de la recherche d'informations par les autorités fédérales de poursuite pénale, la CGE et le STS, qui ont commencé à étudier les aspects techniques de cette question, poursuivront leurs travaux.

Le Conseil fédéral veut s'assurer que les autorités compétentes ne prennent aucun retard technologique et demande pour cela à être informé en permanence des nouvelles tendances. Il se réserve la possibilité, le moment venu, de prendre des mesures si cela s'impose.

## **7 Décryptage des communications**

### **7.1 Contexte**

Le postulat demande aussi que l'on examine la possibilité d'obliger légalement les fabricants de téléphones satellite à révéler la technique de chiffrement employée.

Les communications entre téléphones satellite sont partiellement cryptées, ce qui complique singulièrement le travail de surveillance et d'exploration des autorités de poursuite pénale et des services de renseignement. Les téléphones satellite n'étant pas le seul mode de communication utilisant le chiffrement, les considérations qui suivent sont applicables à tout type de télécommunication chiffrée.

L'obligation faite aux fabricants d'appareils de consigner la technique de chiffrement qu'ils utilisent pourrait simplifier la surveillance. Une disposition légale poursuivant cet objectif devrait contraindre les fabricants à consigner soit la clé de chiffrement soit la description des processus cryptologiques employés. Dans le premier cas, les autorités pourraient se procurer la clé consignée – en suivant une procédure strictement réglementée – afin de *déchiffrer* les communications qui les intéressent. Dans le deuxième cas, la description des processus techniques utilisés servirait à *décrypter* les données codées: le décryptage d'un message chiffré ou d'un processus consiste à reconstituer le texte en clair sans connaître la clé de chiffrement, mais cela suppose des déficits de sécurité dans le processus. Pour détecter les éventuelles lacunes de sécurité, il faut disposer d'une description détaillée des processus. Si les fabricants étaient contraints de livrer leurs processus cryptologiques, les bases du travail de décryptage s'en trouveraient améliorées.

### **7.2 Etat des lieux**

Le DDPS dispose d'un groupe d'experts en cryptologie qui, en collaboration étroite avec la CGE, procède au décryptage systématique de données de production. Les activités de décryptage sont presque exclusivement axées sur les besoins de l'exploration, en premier lieu pour le SRS. Pratiquement aucun décryptage (ciblé) n'est actuellement pratiqué au profit des autorités de poursuite pénale. Si des résultats remarquables ont été obtenus dans le secteur de la communication chiffrée, seule une petite partie des messages cryptés sont déchiffrés. Une législation limitant le

chiffrement des communications pourrait donc s'avérer utile dans cette perspective. En Suisse, ni la LTC, ni la LSCPT, ni aucune autre loi ne comporte de restriction en la matière. En vertu de l'art. 15, al. 4, LSCPT, les fournisseurs de services de télécommunication sont tout de même tenus de supprimer le chiffrement qu'ils ont opéré. Pour faciliter l'accès des organes de surveillance et d'exploration au contenu des messages chiffrés, les deux mesures techniques suivantes pourraient être introduites dans la législation.

### **7.2.1                   Système de consignation des clés et interdiction de chiffrement à l'aide de clés non consignées**

Si un système national de consignation des clés (key escrow system) était mis en place, les seules techniques de chiffrement dont l'utilisation serait autorisée en Suisse seraient celles dont les autorités pourraient, au besoin, se procurer la description et la clé. Il faudrait aussi empêcher, par des moyens techniques, que les usagers des appareils de chiffrement ne puissent utiliser des clés qui n'auraient pas été remises à l'organe de consignation (key escrow). On pourrait aussi imaginer un système de répartition des clés par l'organe de consignation. En contrepartie, tout chiffrement qui ne serait pas contrôlé par l'organe de consignation devrait être interdit.

### **7.2.2                   Interdiction des appareils de chiffrement dont l'algorithme n'a pas été consigné**

Beaucoup moins radical qu'un système de consignation des clés, un système de consignation des processus cryptographiques utilisés serait très simple à mettre en place sur le plan technique. Dans ce cas, la consignation des clés ne serait pas nécessaire et les utilisateurs pourraient donc définir et modifier à leur gré les clés employées. Comme dans le système de la consignation des clés, toute utilisation d'un processus non consigné devrait être sanctionnée.

### **7.2.3                   Tour d'horizon international**

La Suisse n'est pas le seul pays qui ne dispose d'aucune base juridique limitant l'utilisation des moyens cryptographiques. Les techniques de chiffrement peuvent également être appliquées sans restrictions dans l'UE. L'étude de droit comparé la plus récente sur les réglementations en matière de cryptologie a été publiée en 2000 par le «Electronic Privacy Information Center»<sup>88</sup>. Voici ce qui en ressort:

- Seuls quelques Etats limitent l'utilisation privée des techniques cryptographiques, essentiellement d'anciennes républiques soviétiques et des régimes autoritaires. Le seul pays occidental dont la réglementation peut être qualifiée de restrictive est la Grande-Bretagne.

<sup>88</sup> [www2.epic.org/reports/crypto2000](http://www2.epic.org/reports/crypto2000)

- La plupart des pays accordent une telle importance à la sécurité des informations numériques dans la perspective du commerce électronique, de la protection contre l'espionnage électronique et de la protection de la personnalité qu'ils préfèrent renoncer à limiter l'utilisation des techniques cryptographiques. Les «Lignes directrices de l'OCDE régissant la politique de cryptographie» publiées en 1997 et le rapport de la Commission européenne de 1998 soutiennent explicitement les politiques libérales en matière de développement de produits et de services de cryptologie. Suite à la publication de ces rapports, le Canada, l'Allemagne, l'Irlande et la Finlande ont adopté des stratégies nationales qui favorisent la libre utilisation des techniques cryptologiques. D'autres pays ont changé de politique, notamment la France qui a longtemps restreint l'utilisation du chiffrement et a opté pour une libéralisation totale en janvier 1999.

### 7.3 **Appréciation**

Si un système de consignation des clés était créé, tous les systèmes cryptographiques utilisés actuellement, qui sont coûteux, devraient être remplacés, ce qui entraînerait des coûts considérables pour les utilisateurs. Cette solution n'a donc aucun avenir politique. La concentration de toutes les clés de chiffrement dans un système national en ferait en outre une cible privilégiée pour l'espionnage économique. Les mesures techniques et organisationnelles nécessaires pour garantir la protection des clés consignées par les utilisateurs, de même que l'administration qui devrait être mise sur pied engendreraient des coûts massifs pour l'Etat, des coûts dont la répercussion sur les usagers serait discutable. Les Etats-Unis avaient d'ailleurs sérieusement envisagé la création d'un tel système au début des années 90 (initiative Clipper) avant d'y renoncer pour les motifs exposés ci-dessus.

Etant donné que la consignation des processus cryptographiques utilisés n'a de sens que si ceux-ci présentent des faiblesses, autrement dit des déficits de sécurité, une législation dans ce domaine reviendrait à suggérer que de nombreux systèmes cryptographiques propriétaires sont faibles. Cela pourrait même donner la fausse impression que tous les systèmes cryptographiques admis en Suisse sont faibles, ce qui pourrait s'avérer très dommageable pour l'industrie suisse du cryptage, mondialement reconnue. En effet, si une entreprise suisse devait consigner ses processus pour pouvoir travailler sur le marché intérieur, elle devrait automatiquement s'attendre à une baisse de ses exportations.

Ces deux mesures devraient s'accompagner d'une interdiction de tout autre système de chiffrement. Or il serait extrêmement difficile, pour ne pas dire impossible, de constater les infractions. Sur le plan pénal, la sanction maximale que pourraient justifier de telles infractions ne serait pas de nature à effrayer les criminels. On attendrait donc à tort de cette mesure qu'elle ait un effet préventif sur la grande criminalité. De plus, en créant de telles interdictions la Suisse se marginaliserait très clairement sur le plan international. Les mesures décrites ne sont donc ni appropriées ni efficaces pour simplifier le travail d'exploration et de surveillance. Le Conseil fédéral en conclut donc qu'aucune mesure législative ne s'impose pour faciliter le déchiffrement des télécommunications.

## **7.4 Mesures**

Le Conseil fédéral prévoit néanmoins les mesures suivantes:

### **7.4.1 Utilisation des systèmes de décryptage au profit des autorités de poursuite pénale**

Les compétences en matière de décryptage sont et seront encore longtemps un enjeu capital dans la recherche d'informations. Les ressources humaines disponibles aujourd'hui couvrent plus ou moins les besoins actuels de l'exploration stratégique. Pour garantir une exploration plus approfondie et pour couvrir les besoins croissants des autorités de poursuite pénale aussi, il faut examiner la possibilité d'accroître les ressources en personnel du domaine de la cryptologie.

### **7.4.2 Collaboration technique entre les autorités nationales concernées**

Toute activité sur Internet laisse des traces d'activité involontaires et inévitables dans les endroits les plus divers. C'est une chance pour le travail d'exploration et de surveillance. Mais les informations interceptées étant souvent fragmentaires, leur analyse et leur synthèse nécessitent une coopération entre les cryptologues et les spécialistes de systèmes et de réseaux. Le Conseil fédéral va s'assurer que les unités d'organisation concernées intensifient leur collaboration.

## **8 Augmentation de la durée de conservation des données de télécommunication**

### **8.1 Contexte**

Les auteurs du postulat sont d'avis que le délai de six mois qui s'applique à la conservation des données en vue d'un contrôle rétroactif des communications est trop court. Ils demandent donc d'examiner si et comment la LSCPT et l'OSCPT pourraient être adaptées au vu des expériences acquises. L'idée est de renforcer les exigences en matière de conservation de données qui sont de première importance pour la poursuite pénale, notamment en matière de lutte contre le terrorisme et le crime organisé.

Par données téléphoniques, il faut entendre toute forme de transmission au moyen de techniques de télécommunication au sens de l'art. 3 de la LTC. Il n'est pas uniquement question de toute transmission par téléphone fixe, mais également de toute transmission par la téléphonie mobile, les fax, les pagers et autres nouvelles formes de communication offertes notamment par Internet.

## **8.2 Etat des lieux**

### **8.2.1 Bases légales**

Le législateur a créé des normes aux fins de permettre aux autorités de poursuite pénale d'accomplir leur travail d'enquête, lorsque des éléments de preuve sont transmis par le biais de moyens de télécommunication. Ainsi, il a élaboré la LSCPT, dans laquelle il a ancré le principe de l'obligation faite aux fournisseurs de services de télécommunication de conserver pendant six mois les données relatives aux communications. Cette disposition est l'art. 15, al. 3, LSCPT qui doit être mise en rapport avec l'art. 45 LTC et l'art. 60 de l'ordonnance du 31 octobre 2001 sur les services de télécommunication (OST)<sup>89</sup>. D'autres dispositions<sup>90</sup> font mention d'une telle durée de conservation.

Les critères ayant amené à la fixation de la durée de conservation de six mois n'ont pas suscité de débats ou d'oppositions particulières lors de l'élaboration de la LSCPT. Dans le message du 1<sup>er</sup> juillet 1998 à l'appui de cette loi, il est relevé qu'un délai de conservation des données relatives au trafic et à la facturation d'une durée de six mois est requis pour permettre, même rétroactivement, l'identification des usagers. Il est aussi fait mention du fait que la durée de six mois correspond à celle durant laquelle les fournisseurs doivent conserver les données relatives à la facturation afin de fournir des preuves en cas de différends concernant les factures établies<sup>91</sup>. En outre, selon l'art. 45 LTC et l'art. 60 OST, les fournisseurs ont le droit de conserver les données de leurs clients aussi longtemps que cela est nécessaire à l'obtention du paiement dû à leurs prestations. Cette dernière disposition oblige les fournisseurs à conserver les données de leurs clients aussi longtemps que ceux-ci peuvent contester la facture.

### **8.2.2 Situation et tendances en Europe**

En Europe occidentale<sup>92</sup>, la conservation des données de communication est réglementée de façon différente. Ainsi, en Autriche il n'y a pas de délai précis, mais les données sont conservées aussi longtemps que les besoins de facturation l'exigent. En Allemagne, les fournisseurs de services de télécommunication sont tenus de détruire les données de trafic («Verkehrsdaten») immédiatement après la communication<sup>93</sup>. En Grande-Bretagne, en Espagne et au Luxembourg, la durée de conservation est d'un an. En France, la conservation des données relatives au trafic sur les réseaux et services de communications électroniques est actuellement d'un an. Ne sont à l'heure actuelle tenus de cette obligation que les opérateurs de télécommunications fixes et mobiles et les fournisseurs d'accès<sup>94</sup>. En Italie, un décret-loi impose aux opérateurs la conservation des données téléphoniques et télématiques jusqu'au 3 décembre 2007.

<sup>89</sup> RS 784.101.1

<sup>90</sup> Art. 2, let. d, et 19, al. 4, de l'OSCPT

<sup>91</sup> Cf. FF 1998 3716 et 3727

<sup>92</sup> Cf. Avis de droit 05-161 de l'Institut suisse de droit comparé de Lausanne du 16 décembre 2005.

<sup>93</sup> Le droit allemand différencie les données de trafic («Verkehrsdaten») des données destinées à la facturation qui sont enregistrables pendant six mois.

<sup>94</sup> En France le nouveau projet de loi de lutte contre le terrorisme prévoit pour les cybercafés l'obligation de stocker leurs données pendant un an.

Ces disparités, ainsi que les attentats de Madrid et Londres, ont amené le Parlement européen à se pencher sur la question de la conservation des données de communication. Le 14 décembre 2005, il a adopté une directive sur la rétention des données de télécommunication qui prévoit une conservation des données pendant une période de six mois pouvant aller jusqu'à 24 mois, à définir par les Etats membres. Cette directive a été adoptée formellement par les ministres européens de la Justice le 21 février 2006<sup>95</sup>.

### **8.2.3 Pratique de la surveillance rétroactive**

Dans le cadre d'une enquête pénale ou de l'exécution d'une demande d'entraide judiciaire, les autorités cantonales ou fédérales chargées de l'instruction peuvent confier au STS le soin d'exécuter des mesures de surveillance, en particulier des mesures de surveillance rétroactives. Après avoir reçu une décision de l'autorité d'instruction compétente, le STS vérifie que la décision qui lui a été adressée remplit les conditions formelles exigées. Si tel est le cas, le service charge le fournisseur de services de télécommunication concerné de lui livrer les données relatives au trafic et les données secondaires des six mois précédents correspondant à des ressources d'adressage (p.ex. le numéro d'appel d'un raccordement fixe). Les données de trafic et les données secondaires sont enregistrées durant six mois par les fournisseurs de services de télécommunication afin d'être livrées rétroactivement, en cas de besoin, à l'autorité de poursuite pénale qui en fait la requête. Ce n'est donc qu'une fois que la requête de surveillance rétroactive a été dûment ordonnée que les données correspondantes sont transmises au STS<sup>96</sup>.

### **8.2.4 Question de l'insuffisance de la durée actuelle de conservation**

Le fait de pouvoir disposer de données de télécommunication permet d'établir une certaine traçabilité des liens existant entre les participants à des activités criminelles. Face à une criminalité aux ramifications internationales et intercantionales, il est devenu crucial et incontournable d'avoir un maximum d'atouts rendant le travail d'enquête encore plus rapide et efficace. Parmi ces éléments indispensables, il y a celui de l'accès aux connexions téléphoniques ou électroniques utilisées par des suspects. C'est pourquoi la conservation des données de communication est devenue un élément central de lutte contre la grande criminalité. La période de conservation doit être suffisamment longue pour permettre aux autorités de poursuite pénale de trouver des preuves et de poursuivre les infractions à la loi. Il est essentiel pour les organes chargés de veiller à l'application de la loi de disposer de moyens souples et fiables susceptibles d'assurer que les preuves recueillies puissent servir à l'établissement d'un dossier solide.

<sup>95</sup> [http://europa.eu.int/eur-lex/lex/Result.do?direct=yes&lang=fr&xsl=celex-som,celex-txt&PgSize=128&where=CC:152010\\*](http://europa.eu.int/eur-lex/lex/Result.do?direct=yes&lang=fr&xsl=celex-som,celex-txt&PgSize=128&where=CC:152010*)

<sup>96</sup> Pour l'année 2004, on dénombre 2369 mesures de surveillance actives et 5187 mesures de surveillance rétroactives. On constate donc que le nombre des mesures de surveillance rétroactives représente plus du double de celui des mesures de surveillance actives. Il s'agit là d'une tendance qui avait débuté en 2002, mais de façon beaucoup moins marquée. Auparavant, la tendance était inverse.

Il ressort des expériences acquises par les autorités de poursuite pénale suisses que la limitation à six mois de la durée de conservation des données de communication pose de plus en plus de problèmes. Ceux-ci surgissent notamment dans les cas d'exécution de l'entraide judiciaire internationale. En effet, la procédure d'examen des requêtes d'entraide et d'entrée en matière peut prendre beaucoup de temps, en particulier dans des affaires complexes de terrorisme ou de crime organisé. Il est possible que la plus grande partie du délai de six mois soit échue entre le moment où l'autorité étrangère adresse sa requête et le moment où l'autorité suisse pourrait ordonner la mesure de surveillance technique, ce qui rend cette dernière inutile et diminue les chances de succès de l'affaire.

Dans la plupart des affaires, l'analyse des données rétroactives de communication constitue une très bonne base d'investigation pour définir l'environnement des principaux prévenus. C'est ainsi souvent sur la base de cette analyse que les priorités sont fixées pour les mesures d'enquête subséquentes. En cas d'absence ou d'insuffisance de telles données rétroactives de communication, l'environnement des principaux prévenus doit être analysé à l'aide d'autres mesures d'enquêtes, probablement plus lourdes, plus longues, plus risquées et plus coûteuses, comme les mesures de surveillance techniques actives, les mesures d'observation ou l'engagement d'agents infiltrés, par exemple. Ce problème est particulièrement aigu pour les affaires de terrorisme dans lesquelles les prévenus sont souvent inconnus des autorités de poursuite pénale et ne peuvent être identifiés que difficilement, après plusieurs mois de recherches préalables. L'absence ou l'insuffisance de données rétroactives de communication peut également priver définitivement les enquêteurs d'indices objectifs concernant des contacts très sporadiques. Une telle situation péjore gravement l'administration des preuves, surtout dans les affaires complexes où les prévenus nient toutes relations compromettantes en l'absence d'indices objectifs. En outre, une telle situation fait prendre du retard à toute l'enquête, ce qui n'est pas non plus sans conséquence sur l'issue de la procédure.

Plus grave encore, l'insuffisance de la durée actuelle de conservation des données peut même empêcher d'identifier les prévenus ou les victimes de crimes. Ce problème s'est, par exemple, posé dans de nombreuses et importantes affaires de pédophilie et de pornographie infantine dans lesquelles plusieurs centaines de détenteurs d'adresses IP n'ont pas pu être identifiés du fait de l'échéance du délai de six mois.

### **8.3                   Appréciation**

Le délai actuel de six mois complique ou, plus précisément, rend en partie impossible l'évaluation de données de conversations téléphoniques collectées lors de procédures pénales de longue durée. Face à des délits caractérisés par leurs structures complexes et à l'énergie criminelle considérable déployée par leurs auteurs, les autorités de poursuite pénale se trouvent confrontées à un nombre énorme de données qui ne fait que s'amplifier au fil du temps et la brièveté du délai de conservation met en péril l'établissement des preuves. Par conséquent, il est évident que la pratique parle en faveur d'une hausse de la durée de conservation des données. Il est tout aussi crucial que la Suisse prenne des mesures qui lui permettent de répondre aux attentes de ses partenaires étrangers. L'objectif poursuivi consiste notamment à faciliter la coopération policière et judiciaire pour les affaires criminelles d'enver-

gure supranationale, telles que celles menées contre le terrorisme ou le crime organisé.

En ce qui concerne la protection des données, il s'agit de procéder à une pesée des intérêts en présence, à savoir ceux de la sécurité publique et la protection des libertés individuelles de la personne dont on enregistre les données. Il est vrai que l'enregistrement touche toute personne à laquelle sont fournies des prestations de télécommunication. L'accès à ces données est cependant réservé exclusivement aux fournisseurs. Leur transmission rétroactive aux autorités de poursuite pénale a lieu selon une procédure bien définie, pour des finalités déterminées, explicites et prévues par la loi. Cette transmission rétroactive est du reste limitée aux seules données accessoires (données historiques comme la désignation des raccordements, la date, l'heure, la durée) et non au contenu des conversations ou des courriers électroniques. Il convient de relever que l'augmentation de la durée de conservation des données de communication peut aussi permettre de lever des soupçons contre des suspects potentiels. Une fréquence d'appels passés durant les six derniers mois pourrait être relativisée si les données pouvaient s'étendre sur une période de douze mois. Par conséquent, la prise éventuelle de mesures de contrainte susceptibles de porter une atteinte plus grave à la sphère privée et les coûts inhérents pourraient être évités.

Au vu de l'ensemble des considérations qui précèdent, le Conseil fédéral considère qu'une augmentation mesurée de la durée de conservation des données est compatible avec les droits fondamentaux des personnes visées, eu égard aux intérêts publics en jeu.

## 8.4 Mesures

Le Conseil fédéral partage l'avis émis par la CPS selon lequel la durée de six mois qui s'applique à la conservation des données de communication en vue du contrôle rétroactif des conversations téléphoniques est trop courte. Dans sa volonté d'améliorer la lutte contre le terrorisme et le crime organisé et de remédier aux problèmes susmentionnés rencontrés par les autorités de poursuite pénale, le Conseil fédéral estime que la prolongation du délai de conservation des données est une mesure appropriée, qui serait applicable à tous les modes de télécommunication.

En s'inspirant des standards adoptés par les pays voisins et l'UE, un délai de conservation de douze mois, qui représente la moitié du délai maximal préconisé par la directive européenne, est estimé raisonnable et proportionné.

Pour prolonger le délai de conservation des données de communication, il s'agira de procéder à des adaptations des normes où figure la durée de conservation prescrite actuellement (en particulier les art. 5, al. 2, et 15, al. 3, LSCPT ainsi que l'art. 2, let. d, et 19, al. 4, OSCPT).

Certes, l'augmentation de la durée de conservation occasionnerait certains coûts pour les fournisseurs<sup>97</sup>. Une obligation faite aux fournisseurs de conserver pour une durée de l'ordre de douze mois les données relatives aux communications n'engendrerait néanmoins pas, selon l'avis du Conseil fédéral, de surcoûts dispro-

<sup>97</sup> Le Conseil fédéral s'est déjà prononcé à ce sujet dans le cadre d'une réponse à une intervention parlementaire; cf. Ip. Frick du 13 décembre 2002 «Contrôle étatique des communications Internet».

portionnés d'investissement et d'exploitation. En outre, les fournisseurs enregistrent déjà les données ou une partie d'entre elles dans leur intérêt commercial. Pour la Confédération, l'augmentation préconisée pourrait donner lieu à des charges financières supplémentaires car il s'agirait éventuellement d'augmenter la capacité de la banque de données LIS du STS du DETEC.

Le 29 mars 2006, à la suite d'une note de discussion relative à la surveillance des télécommunications à des fins de poursuite pénale, le Conseil fédéral a donné mandat au DFJP et au DETEC de présenter un rapport sur la révision de la LSCPT d'ici au troisième trimestre de 2006. Il ne se prononcera sur les adaptations nécessaires de la LSCPT et de l'OSCPT liées à la prolongation de la durée de conservation des données de communication que lorsqu'il disposera de ce document.

## 9 Autres points abordés par le postulat

Hormis les questions qui ont été approfondies dans les chapitres précédents, le postulat aborde les quatre thèmes suivants qui ne seront traités que brièvement:

### 9.1 Interventions préventives

Le postulat constate que la procédure fédérale fixe le seuil d'intervention des autorités de poursuite pénale à un niveau trop élevé en cas de soupçons d'infraction. Avant toute chose, il faut relever que la PPF exige des soupçons «suffisants» pour pouvoir ouvrir l'enquête (art. 101, al. 1, PPF et art. 194, al. 1, ch. 2, P-CPP). Il est donc faux d'affirmer que les autorités de poursuite pénale doivent toujours attendre que l'accumulation des informations et des éléments permette de formuler des «soupçons graves» avant de pouvoir intervenir. De la même manière, des mesures de contrainte peuvent être ordonnées et exécutées sur la base de soupçons «simplement» suffisants (p.ex. un séquestre ou une perquisition domiciliaire). Toutefois, lorsque les mesures de contrainte portent gravement atteinte aux droits fondamentaux garantis par la Constitution fédérale, le principe de proportionnalité veut que les soupçons soient *graves* ou *imminents*. Tel est notamment le cas pour ordonner la détention préventive ou des mesures de surveillance des télécommunications (art. 44 PPF; art. 3, al. 1, let. a, LSCPT de même que art. 220, al. 1, P-CPP). On remarquera également que l'art. 260<sup>ter</sup> CP autorise déjà une intervention précoce des autorités de poursuite pénale, dans la mesure où il condamne un comportement avant qu'un délit n'ait été perpétré concrètement<sup>98</sup>. Pour ces raisons, le Conseil fédéral ne voit ni la raison ni la nécessité d'abaisser le seuil à partir duquel une procédure d'enquête peut être ouverte, pas plus que de prévoir une nouvelle possibilité d'intervention «préventive» (entendue comme une poursuite pénale sans soupçons suffisants) dans la PPF.

<sup>98</sup> Hans Baumgartner, in: Strafgesetzbuch II, Commentaire bâlois, Bâle 2003, notes 4 ss. ad art. 260<sup>ter</sup>.

## **9.2 Surveillance préventive**

On examinera dans le cadre de la révision de la LMSI (LMSI II) s'il est nécessaire de renforcer les instruments qui relèvent de la surveillance préventive. Le Conseil fédéral approuvera le message rédigé à ce sujet au cours du second semestre.

## **9.3 Risque de récidive**

Le postulat demande l'inscription du risque de récidive comme motif de détention dans la PPF. Cette requête est satisfaite dans le nouveau P-CPP qui, dans la version du Conseil fédéral transmise au Parlement le 21 décembre 2005, prévoit expressément ce motif de détention dans son art. 220, al. 1, let. c.

## **9.4 Prolongation de la durée de conservation des profils d'ADN**

Le postulat demande enfin d'envisager la prolongation de la durée de conservation des profils d'ADN aux fins de la procédure pénale.

La durée de conservation de ces données est réglementée dans les art. 16 et 17 de la loi sur les profils d'ADN. Le Conseil fédéral considère que les durées de conservation prévues par la loi actuelle constituent un compromis équilibré entre les intérêts de la protection des données et ceux de la poursuite pénale, les premiers exigeant la durée la plus brève possible et les seconds la durée la plus longue nécessaire. Exemple concret: conformément aux dispositions générales de la loi sur les profils d'ADN, le profil d'ADN d'une personne qui a été condamnée à une peine privative de liberté ferme pour participation à une organisation criminelle (ou terroriste; art. 260<sup>ter</sup> CP) n'est effacé que 20 ans après sa libération (art. 16, al. 4). La loi prévoit toutefois une garantie supplémentaire pour les personnes qui ont purgé une peine privative de liberté: le profil d'ADN ne peut en effet être effacé que si l'autorité judiciaire compétente y consent (art. 17). Si un risque de récidive persiste, le tribunal peut donc refuser l'effacement du profil, lequel pourra alors être conservé au-delà de la durée légale de 20 ans.

Compte tenu des expériences faites jusqu'ici dans le cadre de la lutte contre le terrorisme et le crime organisé, le Conseil fédéral considère que les durées de conservation des profils d'ADN prévues dans la loi sur les profils d'ADN donnent satisfaction et qu'il n'y a donc pas lieu d'engager une révision partielle de la loi.



**Lutter plus efficacemente contre le terrorisme et le crime organisé. Rapport du Conseil fédéral donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats (05.3006)**

In	Bundesblatt
Dans	Feuille fédérale
In	Foglio federale
Jahr	2006
Année	
Anno	
Band	1
Volume	
Volume	
Heft	26
Cahier	
Numero	
Geschäftsnummer	---
Numéro d'affaire	
Numero dell'oggetto	
Datum	04.07.2006
Date	
Data	
Seite	5421-5470
Page	
Pagina	
Ref. No	10 139 711

Die elektronischen Daten der Schweizerischen Bundeskanzlei wurden durch das Schweizerische Bundesarchiv übernommen.

Les données électroniques de la Chancellerie fédérale suisse ont été reprises par les Archives fédérales suisses.

I dati elettronici della Cancelleria federale svizzera sono stati ripresi dall'Archivio federale svizzero.