13.025

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

du 27 février 2013

Madame la Présidente,
Monsieur le Président,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'une révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication.

Nous vous proposons simultanément de classer les interventions parlementaires suivantes:

2007	M	06.3170	Cybercriminalité. Protection des enfants (N 22.6.2007; E 11.12.2007, Schweiger Rolf)
2010	M	07.3627	Enregistrement obligatoire des cartes d'accès sans fil à prépaiement (N 3.6.2009, Glanzmann-Hunkeler Ida; E 18.3.2010)
2010	P	10.3097	Identification des auteurs d'actes de cybercriminalité (E 10.6.2010, Commission des affaires juridiques CE)
2011	M	10.4133	Relever la durée de conservation des journaux d'attribution d'adresses IP (N 18.3.2011, Barthassat Luc; E 20.9.2011)
2012	M	10.3831	Révision de la LSCPT (N 16.3.2012, Schmid-Federer Barbara; E 24.9.2012)
2012	M	10.3876	Révision de la LSCPT (N 16.3.2012, Eichenberger-Walther Corina; E 24.9.2012)
2012	M	10.3877	Révision de la LSCPT (N 16.3.2012, [von Rotz Christoph] Schwander Pirmin; E 24.9.2012)
2012	P	11.4042	Surveillance au moyen de chevaux de Troie (1) (N 28.2.2012, Commission des affaires juridiques CN)
2012	P	11.4043	Surveillance au moyen de chevaux de Troie (2) (N 28.2.2012, Commission des affaires juridiques CN)
2012	P	11.4210	Coût de la surveillance pénale des télécommunications (E 5.3.2012, Recordon Luc)

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

27 février 2013

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ueli Maurer
La chancelière de la Confédération, Corina Casanova

Condensé

La présente révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) vise à faire en sorte que les surveillances nécessaires de la correspondance par poste et télécommunication ne puissent pas être tenues en échec par l'utilisation de nouvelles technologies (comme p.ex. la téléphonie par Internet cryptée), ni actuellement ni dans les prochaines années. L'objectif n'est pas de surveiller plus mais mieux. Pour ce faire, il est prévu d'adapter la LSCPT et le code de procédure pénale (CPP) à l'évolution technologique de ces dernières années et, dans la mesure du possible, aux développements futurs prévisibles en la matière.

Contexte

Les importants progrès technologiques de ces dernières années dans le domaine des télécommunications offrent aux utilisateurs une multitude de possibilités d'interactions. Celles-ci sont en grande majorité utilisées de manière licite. Il n'empêche qu'elles peuvent ausi être utilisées à des fins criminelles. Force est de constater, en effet, que les nouvelles technologies – p.ex. dans le domaine de la téléphonie par Internet cryptée – facilitent la commission d'infractions. Il est donc nécessaire de se donner les moyens permettant d'éclaircir les infractions commises au moyen de ces technologies.

L'application du droit suisse continue toutefois d'être limitée par le principe de la territorialité; les poursuites pénales dans les cas présentant un caractère international (p.ex. en cas d'utilisation de comptes e-mail auprès de fournisseurs établis à l'étranger) sont de ce fait rendues plus difficiles. La «globalisation virtuelle» représente un problème fondamental pour l'application du droit dans le domaine d'Internet, que la présente révision ne résout d'ailleurs pas.

L'objectif principal de la présente révision totale de la LSCPT est de permettre la surveillance des personnes fortement soupçonnées d'avoir commis des infractions graves. Comme c'est déjà le cas aujourd'hui, il n'est pas question d'autoriser une surveillance de monsieur tout le monde sans qu'il y ait soupçon d'infraction ni même d'autoriser des surveillances préventives; la liberté personnelle est ainsi sauvegardée. Un autre objectif est de pouvoir effectuer des surveillances, en dehors d'une procédure pénale, dans le but de retrouver des personnes disparues et de rechercher une personne en fuite.

Les dispositions procédurales de la LSCPT ont été transférées dans le code de procédure pénale (CPP), qui est entré en vigueur le 1er janvier 2011. Les objectifs de la présente révision de la LSCPT appellent non seulement une révision totale de cette loi mais également l'adaptation de quelques dispositions procédurales dans le CPP. De nouvelles possibilités de surveillance sont par ailleurs inscrites dans le CPP et la procédure pénale militaire (PPM).

Contenu du projet

La présente révision modifie la structure de la LSCPT et instaure une systématique conséquente, avec une nouvelle numérotation. Les articles sont précisés et complétés. Des questions importantes, qui n'étaient jusqu'à présent réglées que dans une ordonnance, sont désormais traitées dans la loi.

Le projet contient les adaptations et nouveautés matérielles suivantes:

- *Les tâches du service de surveillance de la correspondance par poste et télécommunication sont clarifiées et étendues.*
- *Le champ d'application à raison des personnes est considérablement étendu. Différentes catégories de personnes seront tenues de collaborer.*
- *L'étendue de l'obligation de collaborer est réglée de manière échelonnée pour chaque catégorie en fonction de l'activité spécifique de celle-ci.*
- *Les données collectées lors de la surveillance sont conservées de manière centralisée et l'accès à ces données, la consultation et la durée de conservation de celles-ci sont réglés.*
- *La durée de conservation des données secondaires passe de six à douze mois.*
- *Des bases légales claires permettant le recours à des dispositifs spéciaux de surveillance (tels que les IMSI-catchers) et à des programmes informatiques spéciaux («GovWare») sont instituées.*
- *La réglementation relative à la protection du secret professionnel est adaptée.*
- *Comme c'est déjà le cas aujourd'hui, il sera possible de recourir à une surveillance en dehors d'une procédure pénale pour retrouver une personne disparue. Il sera en outre possible, ce qui est nouveau, de rechercher une personne à l'encontre de laquelle une peine privative de liberté ou une mesure privative de liberté a été prononcée.*
- *Des dispositions pénales spécifiques ainsi qu'une disposition relative à la surveillance administrative sont créées.*
- *Les voies de droit contre les décisions du service et les griefs recevables sont nouvellement réglés dans la loi.*

Le régime actuel relatif aux émoluments et indemnités est maintenu.

Table des matières

Condensé **2381**

1 Présentation du projet **2385**

1.1 Contexte 2385

1.2 Dispositif proposé 2385

1.3 Genèse 2386

1.3.1 Mandat du Conseil fédéral 2386

1.3.2 Groupe d'experts 2387

1.3.3 Avant-projet et procédure de consultation 2387

1.3.4 Adaptations après la consultation 2389

1.4 Principales modifications 2390

1.4.1 Champ d'application à raison des personnes 2390

1.4.2 Organe consultatif 2391

1.4.3 Conservation centralisée de longue durée des données collectées lors de la surveillance 2391

1.4.4 Interface entre le système informatique exploité par le service et le réseau de systèmes d'information de police de l'Office fédéral de la police 2392

1.4.5 Examen matériel des ordres de surveillance par le service 2392

1.4.6 Obligations de collaborer 2393

1.4.7 Allongement de la durée de conservation des données secondaires et de la période durant laquelle celles-ci peuvent être obtenues 2393

1.4.8 Informations sur la nature et les caractéristiques des services 2394

1.4.9 Respect des obligations et conséquences en cas de violation («compliance») 2394

1.4.10 Surveillances en dehors d'une procédure pénale 2395

1.4.11 Dispositions pénales 2395

1.4.12 Surveillance administrative 2396

1.4.13 Voies de droit contre les décisions de surveillance du service 2397

1.4.14 Recours à des dispositifs techniques de surveillance 2397

1.4.15 Recours à des Government Software 2397

1.4.16 Blocage de l'accès aux services de télécommunication 2398

1.4.17 Comparaison avec le droit étranger, notamment européen 2399

1.5 Classement d'interventions parlementaires 2400

2 Commentaire des dispositions **2400**

2.1 Section 1 Dispositions générales 2400

2.2 Section 2 Système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication 2407

2.3 Section 3 Tâches du service 2417

2.4 Section 4 Obligations dans le domaine de la surveillance de la correspondance par poste 2425

2.5 Section 5 Renseignements relatifs à la surveillance de la correspondance par télécommunication 2427

2.6 Section 6 Obligations dans le domaine de la surveillance de la correspondance par télécommunication 2434
2.7 Section 7 Garantie de la disponibilité des fournisseurs de services de télécommunication à renseigner et à surveiller 2442
2.8 Section 8 Recherche en cas d'urgence et de personnes condamnées 2449
2.9 Section 9 Frais et émoluments 2452
2.10 Section 10 Dispositions pénales 2455
2.11 Section 11 Surveillance et voies de droit 2458
2.12 Section 12 Dispositions finales 2462
3 Conséquences 2479
3.1 Conséquences pour la Confédération 2479
3.2 Conséquences pour les cantons 2480
3.3 Conséquences économiques 2481
4 Relation avec le programme de la législature 2481
5 Aspects juridiques 2481

Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) *(Projet)* **2483**

Message

1 Présentation du projet

1.1 Contexte

Le domaine des télécommunications, en particulier d'Internet, a connu ces dernières années d'importants progrès technologiques. Ces progrès offrent aux utilisateurs une multitude de possibilités de communication. Les nouvelles technologies (en particulier dans le domaine d'Internet) peuvent toutefois, à l'instar des moyens de communication classiques, être utilisées à des fins illégales, notamment dans les domaines de la pornographie enfantine, de la criminalité organisée et des stupéfiants. La variété, la grande disponibilité et la simplicité d'usage de ces nouvelles technologies de communication facilitent en outre la commission d'infractions.

L'évolution technologique ne rend pas seulement les surveillances de la correspondance par télécommunication plus difficiles à exécuter d'un point de vue technique; la technologie peut en effet également «dépasser» la législation. Ainsi, une surveillance techniquement exécutable peut être problématique d'un point de vue juridique, voire inadmissible, du fait qu'elle ne serait plus (clairement) couverte par une base légale. L'absence de moyen juridique permettant d'obliger les purs fournisseurs de services e-mail à conserver les données secondaires ou la surveillance de la communication cryptée au moyen d'e-mails ou de la téléphonie par Internet, qui n'est souvent possible qu'au moyen de programmes informatiques spéciaux (GovWare), lesquels sont très contestés au regard du droit en vigueur, sont quelques exemples qui illustrent cette insécurité du droit. Il y a donc lieu de faire en sorte que les surveillances nécessaires pour éclaircir des infractions ne puissent être tenues en échec par l'utilisation de nouvelles technologies. L'extension des fournisseurs obligés de collaborer, en particulier, permettra d'atteindre cet objectif.

Le principe de la territorialité des lois pose des limites à l'application du droit suisse. Dans les cas transnationaux (p.ex. lors de l'utilisation de comptes e-mail d'un fournisseur établi à l'étranger), une poursuite pénale rapide et efficace est en effet rendue plus difficile, étant donné que seule la voie de l'entraide judiciaire est ouverte. Dans ces circonstances, les données souhaitées ne souvent pas être obtenues en temps utile (ou pas du tout). Le projet ne change rien à cet état de fait.

1.2 Dispositif proposé

Le but de la révision totale de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[1] consiste en résumé avant tout à pouvoir surveiller non pas plus mais mieux. Il s'agit en premier lieu de permettre la surveillance de personnes fortement soupçonnées d'avoir commis une infraction grave. Par contre, il n'y a aucun motif de permettre la surveillance de citoyens en l'absence d'un soupçon ou des surveillances préventives. En dehors de procédures pénales, la surveillance n'est autorisée que dans les cas de recherche de personnes disparues ou condamnées.

1 RS **780.1**

Le projet (P-LSCPT) clarifie et complète les tâches du service de surveillance de la correspondance par poste et télécommunication (service). Le champ d'application à raison des personnes a été considérablement étendu; l'étendue des obligations de collaborer est toutefois réglée, dans le respect de la proportionnalité, de manière échelonnée pour chaque catégorie de personnes en fonction de l'activité spécifique de celle-ci. Il est prévu que les données collectées lors de surveillances seront conservées durant une longue période dans le système de traitement du service.

L'obligation de conserver les données secondaires est étendue de six à douze mois, de même que la durée pendant laquelle ces données sont à la disposition des autorités de poursuite pénale.

La nouvelle LSCPT régit en outre – ce qui est également nouveau – les conséquences, sur les plans pénal et administratif, applicables aux fournisseurs obligés de collaborer qui ne respecteraient pas leurs obligations. Elle contient de plus une disposition relative aux voies de droit contre les décisions du service et aux griefs recevables.

Les dispositions procédurales de la LSCPT ont été transférées dans le nouveau code de procédure pénale (CPP)[2] qui est entrée en vigueur le 1er janvier 2011. Les objectifs poursuivis ne nécessitent donc pas seulement la révision totale de la LSCPT mais également la révision de quelques dispositions procédurales du CPP. Deux nouvelles possibilités de surveillance ont en outre été intégrées dans le CPP: on pourra à l'avenir recourir à des dispositifs techniques spéciaux de surveillance (p.ex. les IMSI-catchers) et à des programmes informatiques spéciaux (lesdits «GovWare») en se fondant sur des bases légales claires. La réglementation relative à la protection du secret professionnel a également été adaptée. Toutes ces modifications ont par conséquent également été opérées dans la procédure pénale militaire du 23 mars 1979 (PPM)[3].

Ces divers aspects sont examinés en détail ci-après (voir ch. 1.4 et 2).

1.3 Genèse

1.3.1 Mandat du Conseil fédéral

En mars 2006, le Conseil fédéral a chargé le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) ainsi que le Département fédéral de justice et police (DFJP) d'examiner les questions ouvertes concernant la surveillance des télécommunications utilisée à des fins de poursuite pénale et la réglementation de l'indemnisation des fournisseurs de services de télécommunication pour les activités qu'ils déploient dans le cadre de cette surveillance. Ce mandat a donné lieu à un rapport du Secrétariat général du DFJP (SG DFJP), mentionnant les domaines dans lesquels une révision de la LSCPT était souhaitable. Au mois de mai 2007, le SG DFJP a confié le mandat à l'Office fédéral de la justice (OFJ) d'élaborer un avant-projet (AP-LSCPT) et un rapport explicatif.

2 RS **312.0**
3 RS **322.1**

1.3.2 Groupe d'experts

En septembre 2008, l'OFJ a constitué un groupe d'experts pour le conseiller, composé de représentants du Ministère public de la Confédération (MPC), de la Police judiciaire fédérale (PJF), de l'Office fédéral de la communication (OFCOM), de l'Association Suisse des Télécommunications (asut), des autorités de poursuite pénale cantonales, du Service Surveillance de la correspondance par poste et télécommunication relevant du Centre de services informatiques DFJP (service) et de l'OFJ. Celui-ci a tenu compte des discussions ayant eu lieu dans le cadre de ce groupe d'experts pour l'élaboration de l'AP-LSCPT.

1.3.3 Avant-projet et procédure de consultation

Le Conseil fédéral a mis l'AP-LSCPT[4] et le rapport explicatif y relatif[5] en consultation le 19 mai 2010. La consultation a duré jusqu'au 18 août 2010. Elle s'est adressée à tous les cantons, aux partis politiques, aux organisations actives dans le domaine de la poursuite pénale, à celles actives dans le domaine des télécommunications et à plusieurs autres organisations intéressées[6].

Le DFJP a reçu 106 prises de positions, représentant au total quelque 700 pages. Tous les cantons, 6 partis politiques et 74 organisations intéressées se sont prononcés. Les réponses ont été synthétisées dans un rapport daté de mai 2011[7].

En substance, il importe tout d'abord de relever que tous les participants ont reconnu ou, du moins, n'ont pas remis en cause, la nécessité d'adapter la LSCPT aux évolutions techniques de ces dernières années. Cependant, nombre de réserves, en partie structurelles et générales, ont été émises en ce qui concerne les diverses dispositions proposées. Un remaniement complet a même parfois été requis. Les principaux thèmes ayant suscité des réactions sont les suivants:

- Champ d'application à raison des personnes. Passablement de participants soutiennent son extension. Nombre d'entre eux y sont en revanche opposés ou demandent une reformulation de son cadre, à l'art. 2, al. 1, let. b AP-LSCPT, pour des raisons de clarté ou du fait qu'il va trop loin, notamment quant à sa portée et quant à ses implications économiques pour les personnes concernées. Fut également contestée la question de savoir s'il fallait intégrer des fournisseurs tels que les fournisseurs d'hébergement (hosting providers), constituant des fournisseurs de services Internet, dans le champ d'application à raison des personnes.
- Conservation centralisée de longue durée des données collectées lors de la surveillance dans le système informatique du service. Ce mode de conservation a été soutenu par plusieurs participants, qui ont préconisé toutefois des aménagements, parfois importants, que l'on retrouve dans le système actuel, notamment le maintien de l'envoi par la poste, sur des supports de données, des données n'étant pas issues de surveillances Internet. Un nombre plus

4 www.admin.ch/ch/f/gg/pc/documents/1719/Vorlage.pdf
5 www.admin.ch/ch/f/gg/pc/documents/1719/Bericht.pdf
6 www.admin.ch/ch/f/gg/pc/documents/1719/Adressatenliste.pdf
7 www.admin.ch/ch/f/gg/pc/documents/1719/Rapport_C_surveillance_correspondance_par_poste_et_telecommunication.pdf

important de participants a souligné le caractère extrêmement compliqué de la réglementation prévue, éventuellement son incompatibilité avec le CPP. D'autres participants encore se sont dits opposés à la conservation centralisée et à l'accès online – également du prévenu et de son défenseur, pour des raisons de sécurité – auprès du service.

– Absence d'obligation du service de vérifier la légalité des surveillances ordonnées. Un grand nombre de participants a demandé que le service soit soumis à l'obligation de vérifier la légalité des ordres de surveillance qui lui sont transmis.

– Personnes obligées de collaborer: Pour un groupe important de participants, les obligations concrètes n'étaient pas réglées de manière suffisamment claire.

– Obligation générale d'identification, par les fournisseurs de services de télécommunication, des utilisateurs qui accèdent à Internet. Un nombre relativement important de participants s'est félicité de la disposition y relative, en particulier en relation avec l'utilisation des systèmes mis à la disposition de la clientèle par les hôtels, avec la connexion via les cybercafés, etc. De nombreux participants ont en revanche demandé la suppression ou l'adaptation de la disposition considérée, car cette obligation serait disproportionnée, voire irréalisable, et inefficace.

– Allongement de la durée de conservation des données secondaires de 6 à 12 mois. Sur le principe, de nombreux participants se sont félicités de cet allongement. Un grand nombre s'est toutefois opposé à la disposition y relative ou a demandé qu'elle soit modifiée; à l'appui de cette position, ces participants ont invoqué le fait que cette disposition permet de conserver – pendant une période encore plus longue – systématiquement à titre préventif des données sur des personnes au-dessus de tout soupçon ou ont invoqué les frais élevés causés par cet allongement.

– Suppression de l'indemnisation des fournisseurs de services postaux et de télécommunication. Plusieurs participants se sont félicités de cette suppression, estimant qu'une indemnisation est en disharmonie avec le système. De nombreux participants se sont cependant exprimés contre ladite suppression, soulignant le fait que la poursuite pénale est une tâche qui incombe à l'Etat, et qu'elle doit donc être prise en charge par la collectivité; d'autres ont relevé la nécessité de se doter d'une infrastructure coûteuse pour satisfaire aux nouvelles exigences légales ou ont exprimé le souhait qu'une réglementation plus nuancée soit mise en place.

– Voies de droit contre les décisions de surveillance du service. Un grand nombre de participants a demandé que soit expressément prévue la possibilité pour les fournisseurs obligés de collaborer de faire examiner par un tribunal la légalité de la décision de surveillance qui leur a été notifiée par le service.

– Interception de données par l'introduction de GovWare dans des systèmes informatiques de tiers. Un nombre important de participants s'est félicité de la possibilité de recourir à des GovWare, en particulier du fait que la problématique du cryptage des données a tendance à se répandre fortement. Un groupe important de participants s'est toutefois déclaré opposé à cette utili-

sation de GovWare ou a émis d'importantes réserves à ce sujet. Ces derniers ont en particulier invoqué la grave atteinte à la vie privée des personnes concernées que constituerait la possibilité d'accéder à toutes les données contenues dans un système informatique (perquisition en ligne). Ils ont également fait valoir les risques trop élevés pour la sécurité informatique ainsi que pour la fiabilité et l'intégrité des moyens de preuve ou la nécessité de ne pouvoir recourir à ce mode de surveillance que pour une partie des infractions (les plus graves) mentionnées à l'art. 269, al. 2 CPP.

1.3.4 Adaptations après la consultation

Le message se base sur l'AP-LSCPT, envoyé en consultation, et tient compte des principales objections, remarques et propositions fondées exprimées dans les prises de positions. Il importe de mentionner que le message a subi d'importantes modifications, parfois fondamentales, par rapport à l'AP-LSCPT.

Les changements apportés sont en particulier les suivants:

- Le champ d'application à raison des personnes a été précisé et étendu à diverses catégories de personnes et de fournisseurs («personnes obligées de collaborer»); ces catégories sont caractérisées par leurs activités spécifiques.
- Les obligations respectives des différentes catégories de personnes obligées de collaborer ont été précisées et complétées. L'étendue des obligations de collaborer a ce faisant été définie au moyen de l'activité spécifique de chaque catégorie de personnes considérée.
- Le DFJP pourra créer un organe consultatif pour favoriser une exécution sans difficultés des surveillances et un développement continu dans ce domaine. Cet organe sera composé de représentants des milieux intéressés.
- Concernant la conservation centralisée de longue durée des données collectées lors de la surveillance dans le système informatique du service, des dispositions plus pertinentes, plus simples et plus praticables pour les autorités sont prévues, en particulier pour les autorités de poursuite pénale. Ceci implique pour le service une charge administrative réduite.
- Dans un souci d'efficacité, le projet institue une base légale pour une interface permettant le transfert par voie électronique de copies de données collectées lors de la surveillance du système exploité par le service dans une banque de données prévue dans la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[8].
- Le service pourra procéder à un examen matériel plus étendu, sous l'angle du droit administratif, des ordres de surveillance qui lui sont transmis. Il aura un devoir d'avis à l'autorité qui a ordonné la surveillance et à celle habilitée à l'autoriser s'il estime qu'il y a un problème suite à cet examen. Cette disposition ne vise pas un examen matériel par rapport à des questions relevant de la procédure pénale.

8 RS **361**

– Il est renoncé à imposer aux fournisseurs de services de télécommunication une obligation générale d'identification des utilisateurs qui accèdent à Internet.

– Le projet prévoit des dispositions concernant le respect («compliance») par les fournisseurs de services de télécommunication des obligations relatives à l'exécution des surveillances de la correspondance par télécommunication. Sont également prévues des dispositions relatives aux conséquences en cas de violation de ces obligations.

– La suppression de l'indemnisation des fournisseurs de services postaux et de télécommunication n'a pas été retenue.

– Le service sera compétent pour la poursuite et le jugement des infractions prévues dans la LSCPT. La loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA)[9] est applicable.

– Les personnes obligées de collaborer pourront faire examiner par un tribunal la légalité de la décision de surveillance qui leur a été notifiée par le service.

– L'interception de données relevant de la correspondance par télécommunication par l'introduction de GovWare dans des systèmes informatiques de tiers devra être autorisée pour des infractions pour lesquelles une investigation secrète serait autorisée (voir catalogue de l'art. 286, al. 2, CPP). Le catalogue d'infractions plus étendu, pour lesquelles une surveillance de la correspondance par poste et télécommunication est possible (voir art. 269, al. 2 CPP), n'est pas applicable lors du recours à des GovWare.

1.4 Principales modifications

1.4.1 Champ d'application à raison des personnes

Le champ d'application à raison des personnes est considérablement étendu. Il détermine qui est soumis à la loi, c'est-à-dire qui a des obligations en vertu de celle-ci. Selon la LSCPT en vigueur, le champ d'application à raison des personnes ne contient que les fournisseurs de services postaux ou de télécommunication, dont font partie les fournisseurs d'accès à Internet, et les exploitants de réseaux de télécommunication internes et de centraux domestiques. Il existe toutefois d'autres personnes ou des entreprises qui peuvent posséder des données relatives à la correspondance par poste ou télécommunication dont les autorités de poursuite pénale peuvent avoir besoin. Au vu des problèmes précités, le champ d'application à raison des personnes a été précisé et porte désormais sur six catégories de personnes différentes («les personnes obligées de collaborer»), caractérisées par des activités spécifiques. Ces catégories de personnes sont les suivantes:

– les fournisseurs de services postaux (la Poste suisse, des services de coursier, etc.);

– les fournisseurs de services de télécommunication (p.ex. opérateurs téléphoniques classiques);

9 RS **313.0**

– les fournisseurs de services qui se fondent sur des services de télécommunication («fournisseurs de services de communication dérivés»; p.ex. purs fournisseurs de services e-mail);
– les exploitants de réseaux de télécommunication internes (p.ex. réseaux internes à des entreprises, «intranet»);
– les personnes qui laissent leur accès à un réseau public de télécommunication à la disposition de tiers (p.ex. hôtels ou cybercafés);
– les revendeurs professionnels de cartes ou autres moyens semblables (cartes à prépaiement, etc.) qui permettent l'accès à un réseau public de télécommunication.

L'étendue des obligations de collaborer est réglée, dans le respect de la proportionnalité, séparément pour chaque catégorie de personnes (voir ch. 1.4.6).

Pour les détails, voir le commentaire de l'art. 2.

1.4.2 Organe consultatif

Le DFJP pourra créer un organe consultatif composé de représentants des différents acteurs dans le domaine de la surveillance de la correspondance par poste et télécommunication (DFJP, service, cantons, autorités de poursuite pénale et fournisseurs de services postaux et de télécommunication) pour favoriser une exécution sans difficultés des surveillances et un développement continu dans ce domaine. Au vu des intérêts parfois contradictoires de ces acteurs, la collaboration de ceux-ci au sein d'un organe est – comme l'expérience l'a démontré – essentielle. Une telle collaboration existe déjà sur une base informelle, sans être prévue dans un texte de loi.

Pour les détails, voir le commentaire de l'art. 5.

1.4.3 Conservation centralisée de longue durée des données collectées lors de la surveillance

En vertu du droit en vigueur, le service transmet par la poste, sur des supports de données, toutes les données collectées lors de la surveillance de la correspondance par télécommunication aux autorités (de poursuite pénale). Dès que celles-ci en ont confirmé la réception au service, celui-ci les efface dans son système. Les données sont conservées au dossier judiciaire, comme n'importe quel autre moyen de preuve.

On prévoit désormais de passer à la conservation centralisée de longue durée des données précitées dans le système informatique du service. Ceci vaut pour toutes les données issues de surveillances de la correspondance par télécommunication, aussi bien pour celles issues de surveillances téléphoniques traditionnelles que pour celles issues de surveillances Internet. L'argument plaidant avant tout pour ce changement est le fait que les données, particulièrement celles issues de surveillances Internet, sont de plus en plus nombreuses, ce qui a pour conséquence qu'il est de plus en plus difficile de les transmettre par la poste sur des supports de données, et le fait que ces supports peuvent de plus en plus difficilement être stockés et administrés.

Dans le nouveau fonctionnement proposé, l'accès des autorités (de poursuite pénale) aux données concernant des dossiers relevant de leur compétence se fait au moyen d'un accès en ligne au système informatique du service. Les parties, y compris le prévenu et son avocat, peuvent également y accéder en ligne. A certaines conditions, les données pourront comme actuellement être transmises sur des supports de données mobiles.

Pour les détails, voir le commentaire des art. 6 à 14.

1.4.4 Interface entre le système informatique exploité par le service et le réseau de systèmes d'information de police de l'Office fédéral de la police

Le réseau de systèmes d'information de police de l'Office fédéral de la police est en particulier utilisée par celui-ci et les polices cantonales pour exploiter les informations obtenues dans le cadre d'enquêtes pénales. Le transfert par voie électronique, en ligne, d'une copie des données contenues dans le système informatique exploité par le service dans les systèmes d'information visés aux art. 10 et 13 LSIP présente par rapport au transfert «manuel» plusieurs avantages. Il permet en particulier des gains en temps et financiers ainsi qu'une sécurité des données accrue (risque de perte des données réduit et risque d'erreur, affectant la qualité des données, diminué). Le passage au mode de transfert électronique des données ne doit pas avoir pour conséquence d'éluder les règles applicables à l'accès au système exploité par le service et au système d'information considéré au sens de la LSIP.

Pour les détails, voir le commentaire de l'art. 14.

1.4.5 Examen matériel des ordres de surveillance par le service

En plus de l'examen formel qu'il peut déjà effectuer sur la base du droit en vigueur, le service pourra nouvellement procéder à un examen matériel, sous l'angle du droit administratif, des ordres de surveillance qui lui sont transmis et aura le devoir d'aviser l'autorité qui a ordonné la surveillance (en principe, le ministère public) et celle habilitée à l'autoriser (en principe, le tribunal des mesures de contrainte) s'il estime qu'il y a un problème suite à cet examen. Le service pourra ainsi examiner si l'ordre de surveillance transmis est prévu par la législation, techniquement approprié et exécutable. Le service ne pourra en revanche pas effectuer un examen matériel par rapport à des questions relevant de la procédure pénale, cet examen relevant de la compétence de l'autorité habilitée à autoriser les surveillances.

L'autorité ayant ordonné la surveillance et l'autorité habilitée à l'autoriser pourront – sans y être contraintes – tenir compte de l'avis du service pour révoquer la surveillance ordonnée ou ne pas l'autoriser. Ce mécanisme évite que le service ne doive «aveuglément» émettre une décision suite à un ordre de surveillance posant problème et que des questions problématiques ne puissent être examinées, par une autorité judiciaire, que suite à un recours du fournisseur concerné. De nombreux problèmes peuvent de la sorte déjà être réglés en amont et de manière simple. Une voie de droit particulière n'est toutefois pas nécessaire pour régler par voie de justice les éventuelles divergences entre le service et l'autorité qui a ordonné la surveillance. Une telle

voie de droit est d'autant plus superflue que la protection juridique des personnes obligées de collaborer a été étendue.

Pour les détails, voir le commentaire de l'art. 16, let. b.

1.4.6 Obligations de collaborer

Les obligations de collaborer ne sont pas assez claires dans la LSCPT en vigueur. Les personnes obligées de collaborer doivent de plus fournir des prestations supplémentaires, au vu du progrès technique.

Aux art. 26 à 30, les obligations des différentes catégories de personnes obligées de collaborer ont donc été, pour chaque catégorie, systématisées, formulées de manière plus précise, complétées et définies en fonction de l'activité spécifique de chaque catégorie.

Au vu du caractère technique de la matière, il n'est pas opportun de définir les obligations dans le détail dans la loi; les détails seront réglés par le Conseil fédéral par voie d'ordonnance; l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (OSCPT)[10] est destinée – à l'instar de ce qui est le cas dans le droit en vigueur – à accueillir ces dispositions. A certaines conditions, le Conseil fédéral pourra dispenser des fournisseurs de services de télécommunication de certaines obligations. Il peut toutefois également soumettre certaines personnes obligées de collaborer (p.ex. des fournisseurs de service e-mail) à tout ou partie des obligations plus étendues des fournisseurs de services de télécommunication.

Quant aux dispositions d'exécution techniques et administratives, qui ont pour objectif la bonne exécution au moindre coût des types de surveillances usuels, elles ne figureront plus, comme aujourd'hui, dans des directives du service mais dans des ordonnances du DFJP.

Il importe de mentionner que, pour des raisons de praticabilité, il est renoncé à imposer aux fournisseurs de services de télécommunication une obligation générale d'identification des utilisateurs qui accèdent à Internet, malgré le fait que l'on tolère ainsi une lacune dans la surveillance.

Pour les détails, voir le commentaire des art. 19 à 30.

1.4.7 Allongement de la durée de conservation des données secondaires et de la période durant laquelle celles-ci peuvent être obtenues

A la différence des données dites de contenu, les données secondaires ne fournissent pas d'information sur le contenu de l'envoi ou de la télécommunication, mais uniquement sur le fait de savoir qui a été en correspondance ou en communication avec qui, quand, d'où, etc. Afin de permettre une poursuite plus efficace des infractions, il est prévu d'allonger de six mois à douze mois la durée de conservation des données secondaires. Ces données sont conservées en «réserve» pour d'éventuelles futures

10 RS **780.11**

enquêtes pénales et sont indispensables pour lutter contre la criminalité. Les données secondaires ne peuvent être obtenues à titre préventif mais en principe uniquement dans le cadre d'une procédure pénale, avec l'autorisation de l'autorité compétente pour autoriser les surveillances.

Cet allongement est à mettre en relation avec les exigences de la motion Schweiger 06.3170 (Cybercriminalité. Protection des enfants) et celles de la motion Barthassat 10.4133 (Relever la durée de conservation des journaux d'attribution d'adresses IP). La problématique soulevée par ces motions concerne non seulement les données secondaires de télécommunication mais également les données secondaires postales. Il ressort des expériences faites par les autorités de poursuite pénale que la durée pendant laquelle les données secondaires doivent être conservées en vertu du droit en vigueur, soit 6 mois, est trop courte, puisque ce délai est souvent totalement ou en grande partie échu lorsque l'autorité est en mesure d'ordonner une surveillance.

Pour les détails, voir le commentaire des art. 19, al. 4 et 26, al. 5 ainsi que 273, al. 3 CPP et 70*d*, al. 3 PPM.

1.4.8 Informations sur la nature et les caractéristiques des services

Afin de garantir l'exécution correcte des surveillances, le service doit également anticiper les difficultés qui pourraient survenir dans le cadre de surveillances futures. Il ne doit pas se contenter de réagir à des problèmes qui se seraient passés lors de l'exécution d'une nouvelle surveillance. Les fournisseurs de services de télécommunication devront donc, à la demande du service, lui expliquer quels sont les services qu'ils ont mis sur le marché ou qu'ils ont l'intention de mettre sur le marché dans les six mois et ce qu'ils permettent de faire, étant entendu que les collaborateurs du service sont soumis au secret de fonction (art. 320 CP).

Pour les détails, voir le commentaire de l'art. 25.

1.4.9 Respect des obligations et conséquences en cas de violation («compliance»)

Afin de garantir une bonne exécution des surveillances, la loi contient désormais des dispositions applicables au respect des obligations par les fournisseurs de services de télécommunication et règle les conséquences en cas de violation de ces obligations («compliance»). Ces dispositions règlent notamment la capacité de fournir les renseignements et d'effectuer les surveillances. Les fournisseurs pourront confier à leur frais l'exécution de leurs tâches (en tout ou en partie) à des tiers; ils continueront toutefois d'être liés par les obligations correspondantes.

Ces dispositions portent également sur la preuve de la capacité de renseigner et de surveiller. Elles règlent en outre les conséquences financières en cas de manquement.

Pour les détails, voir le commentaire des art. 31 à 34.

1.4.10 Surveillances en dehors d'une procédure pénale

La surveillance de la correspondance par poste et télécommunication qui peut être effectuée en cas d'urgence, pour retrouver une personne disparue, n'est plus, contrairement à ce que prévoit l'art. 3 de la LSCPT en vigueur, limitée aux données secondaires. Elle permettra également d'obtenir le contenu des envois, dans le domaine de la correspondance par poste, et celui des communications, dans le domaine de la correspondance par télécommunication, étant donné que ces informations sont aussi susceptibles de donner des renseignements sur le lieu où se trouve la personne disparue. Cette surveillance est subsidiaire aux autres mesures qui peuvent être entreprises pour trouver la personne recherchée. Le recours aux dispositifs techniques de surveillance (IMSI-catchers, voir art. 269bis CPP) est également autorisé, toutefois de manière subsidiaire par rapport aux mesures de recherche susmentionnées. Ce mode de surveillance est susceptible de permettre de retrouver une personne disparue même lorsque les mesures de surveillance de la correspondance par télécommunication classiques se sont révélées inopérantes. En cas de nécessité, il demeure possible, à l'instar de ce que prévoit l'art. 3, al. 1 de la LSCPT en vigueur, de surveiller la correspondance par poste et télécommunication qui n'est pas celle de la personne recherchée mais celle d'un tiers non impliqué.

On doit également pouvoir recourir à une surveillance dans le sens décrit ci-dessus pour rechercher une personne condamnée à une peine privative de liberté ou qui fait l'objet d'une mesure entraînant une privation de liberté. La surveillance est possible dans le cadre d'une procédure pénale en cours; elle doit donc d'autant plus être admissible dans les cas où on n'est pas uniquement en présence de soupçons (art. 269, al. 1, let. a CPP), mais en présence d'un jugement définitif et exécutoire.

La procédure relative aux surveillances en dehors d'une procédure pénale est, en principe, régie par analogie par les art. 274 à 279 CPP.

Pour les détails, voir le commentaire des art. 35 à 37 et le ch. 1.4.14.

1.4.11 Dispositions pénales

La présente révision contient des dispositions qui sanctionnent la violation d'obligations susceptible d'entraver une surveillance. Une telle sanction doit toutefois n'être prononcée que subsidiairement par rapport à des dispositions pénales plus sévères dont les conditions seraient également remplies. On pense ici, par exemple, aux dispositions pénales concernant la protection du secret de fonction (art. 320 CP) ou du secret des postes et des télécommunications (art. 321ter CP) ou à l'entrave à l'action pénale (art. 305 CP). L'expérience montre que les fournisseurs importants de services de télécommunication sont en principe conscients de leurs obligations et y satisfont.

En cas d'inobservation des injonctions du service, une norme pénale qui reprend le mécanisme de l'art. 292 CP devra être applicable. Au regard des économies qu'une personne obligée de collaborer est susceptible de réaliser pour le cas où elle n'exécute pas une injonction du service, l'amende maximale de 10 000 francs prévue par l'art. 292 CP ne saurait toutefois être dissuasive. Il est donc justifié de prévoir une disposition spécifique contenant une peine plus sévère.

Sur la base de la motion Schweiger 06.3170 (Cybercriminalité. Protection des enfants), une autre disposition pénale qui sanctionne la violation de l'obligation de conserver les données secondaires a été instituée. Sera réprimée en outre la violation d'obligations de documentation (en particulier l'enregistrement de données personnelles, ou de clients) lors de la remise de cartes ou d'autres moyens semblables permettant l'accès à un réseau public de télécommunication sans souscrire à un abonnement (p.ex. au moyen de cartes SIM à prépaiement). L'expérience montre en effet qu'une telle sanction est nécessaire pour faire respecter ces obligations de documentation[11]. Comme c'est le cas aujourd'hui, l'inobservation à l'égard de tiers du secret sur la surveillance sera également punie.

La poursuite et le jugement des infractions susmentionnées incomberont au service. Plusieurs arguments plaident en faveur de cette solution: Le service est le mieux placé pour avoir connaissance des faits susceptibles de constituer une telle infraction. En outre l'art. 39 sanctionne le non-respect des injonctions du service lui-même. De plus, la LSCPT confère des tâches de surveillance administrative au service. Enfin, la poursuite et le jugement de ces infractions requièrent des connaissances techniques assez pointues, que les autorités de poursuite pénale des cantons sont moins susceptibles de posséder que le service.

Au vu des compétences du service, ces infractions sont poursuivies et jugées conformément à la DPA.

Pour les détails, voir le commentaire des art. 39 s.

1.4.12 Surveillance administrative

Il faut pouvoir s'assurer que seules les personnes et entreprises soumises à la LSCPT qui respectent les prescriptions relatives à la surveillance de la correspondance par poste et télécommunication puissent être actives sur le marché. Le fait de rendre l'art. 58 de la loi du 30 avril 1997 sur les télécommunications (LTC)[12] en partie applicable par analogie contribue à la réalisation de cet objectif. Le service pourra ainsi prononcer des sommations en cas de violation des prescriptions relatives à la surveillance de la correspondance par poste et télécommunication. On instaure ainsi un système de sanctions administratives, distinct et complémentaire au système des sanctions pénales (voir le ch. 1.4.11). Le service exercera ses compétences de surveillance de manière contraignante à l'égard des personnes obligées de collaborer. Tel n'est toutefois pas le cas à l'égard des autorités qui ordonnent des surveillances et de celles habilitées à les autoriser, étant donné qu'il ne possède pas de compétence décisionnelle qui s'impose à ces autorités (voir ch. 1.4.5).

Pour les détails, voir le commentaire de l'art. 41.

11 Thomas Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2e éd., Saint-Gall 2006, n. 2 ad art. 19*a* OSCPT.

12 RS **784.10**

1.4.13 Voies de droit contre les décisions de surveillance du service

La LSCPT actuelle ne contient pas de disposition régissant les voies de recours contre les décisions du service. Seul l'art. 32 de l'actuelle OSCPT est applicable.

Pour des raisons de clarté et de sécurité juridique, une disposition régissant les voies de recours contre les décisions du service a été inscrite dans la loi.

La disposition considérée reprend les principes en vigueur. Les personnes obligées de collaborer peuvent ainsi faire examiner par un tribunal la légalité de la décision de surveillance qui leur a été notifiée par le service, sans toutefois pouvoir invoquer des questions relevant de la procédure pénale (comme, p.ex., le fait de savoir si on est en présence de graves soupçons en vertu de l'art. 269, al. 1, let. a, CPP ou le fait de savoir si les conditions pour la surveillance d'un tiers prévues à l'art. 270, let. b, CPP sont remplies).

Considérant en particulier le caractère urgent qu'a souvent une surveillance, le recours contre une décision de surveillance du service n'a pas d'effet suspensif. Il est prévu toutefois que l'autorité de recours puisse attribuer l'effet suspensif au recours.

Pour les détails, voir le commentaire de l'art. 42.

1.4.14 Recours à des dispositifs techniques de surveillance

Le complément apporté au CPP (et à la PPM) doit permettre au ministère public (et au juge d'instruction militaire) d'utiliser plus largement des dispositifs tels que les IMSI-catchers afin d'identifier des appareils de communication mobiles (et pas seulement les appareils de téléphonie mobile) et, partant, leurs utilisateurs. Cette utilisation de l'IMSI-catcher vient ainsi s'ajouter à celles qui consistent à écouter et enregistrer des communications et à localiser les appareils ou les utilisateurs précités. Ce complément, outre le fait qu'il constitue une mesure nécessaire dans la poursuite des infractions, se justifie également du fait que l'identification est une mesure qui touche moins fortement la sphère privée des utilisateurs en comparaison de la localisation, de l'écoute et de l'enregistrement des conversations[13].

Le recours à un IMSI-catcher ordonné par le ministère public est, comme mesure de surveillance de la correspondance par télécommunication faisant l'objet de l'art. 269 CPP, soumis à l'autorisation du tribunal des mesures de contrainte.

Pour les détails, voir le commentaire de l'art. 269bis CPP ainsi que de l'art. 70bis PPM.

1.4.15 Recours à des Government Software

Le projet complète le CPP (et la PPM) par une base légale ad hoc qui permet au ministère public (et au juge d'instruction militaire) d'ordonner, dans une procédure pénale – et non à titre préventif –, à des conditions strictes (dont l'autorisation par le

[13] Sophie de Saussure, Le IMSI-Catcher: fonctions, applications pratiques et légalité, Jusletter 30.11.2009, n. 45 à 56 et 70.

tribunal des mesures de contrainte), l'utilisation de programmes informatiques communément appelés GovWare. L'usage de GovWare doit être subsidiaire aux mesures classiques de surveillance, le principe de la proportionnalité demeurant bien entendu réservé.

Le GovWare est introduit dans un système informatique dans le but d'intercepter le contenu des communications et des données secondaires. Le recours à des GovWare n'est toutefois admissible que pour des infractions pour lesquelles une investigation secrète serait autorisée (voir catalogue de l'art. 286, al. 2 CPP). Le catalogue d'infractions plus étendu, pour lesquelles une surveillance de la correspondance par poste et télécommunication est possible (voir art. 269, al. 2 CPP), n'est pas applicable lors du recours à des GovWare. Cette introduction doit bien entendu avoir lieu à l'insu du détenteur du système informatique visé. Ce procédé de surveillance ne requiert pas la collaboration d'un fournisseur de services de télécommunication. Et le service n'a aucun rôle particulier à jouer dans l'utilisation de GovWare.

Peuvent ainsi être obtenues non seulement les données relatives à la téléphonie par Internet et à la correspondance par e-mails, mais toutes les données relevant de la correspondance par télécommunication, dont fait partie la correspondance par Internet. Par «système informatique», on entend tout appareil permettant la correspondance par télécommunication, par le réseau de téléphone ou par un autre moyen comme les ordinateurs (portables) ou les téléphones portables.

La perquisition en ligne au moyen d'un GovWare d'un système informatique, laquelle permet d'accéder à toutes les données personnelles (p.ex. documents, photos), est interdite. Il est également exclu de recourir à un GovWare pour utiliser la caméra ou le micro d'un ordinateur dans un autre but que la surveillance de la correspondance par télécommunication, par exemple pour surveiller une pièce.

Des autorités de poursuite pénale (Confédération et cantons) ont, à de rares reprises, eu recours à des GovWare sur la base des dispositions de procédure pénale en vigueur avant l'entrée en vigueur du CPP. Les opinions sont partagées sur le fait de savoir si le droit en vigueur permet l'utilisation de GovWare, la majorité d'entre elles réfutant cette possibilité[14]. Il apparaît donc nécessaire de créer une base légale ad hoc si l'on veut pouvoir recourir à des GovWare aux fins et conditions susmentionnées.

Pour plus de détails, voir le commentaire de l'art. 269ter CPP ainsi que de l'art. 70ter PPM.

1.4.16 Blocage de l'accès aux services de télécommunication

Le projet prévoit l'obligation, à des conditions déterminées, pour les fournisseurs de services de télécommunication de bloquer l'accès de certains clients à la téléphonie et à Internet. Ceci, dans l'optique de contribuer à identifier les personnes qui accèdent à ces services sans avoir souscrit d'abonnement (p.ex. au moyen de cartes SIM à prépaiement).

Pour les détails, voir le commentaire de l'art. 6*a* LTC.

14 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 16; contra Sylvain Métille, op. cit., n. 37.

1.4.17 Comparaison avec le droit étranger, notamment européen

Les pays voisins de la Suisse connaissent des régimes de surveillance de la correspondance par poste et télécommunication semblables à celui qui fait l'objet du présent projet. Il existe toutefois quelques différences par rapport à la réglementation prévue dans celui-ci.

Concernant les données secondaires, il importe tout d'abord de mentionner la directive de l'Union européenne 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006[15]. Cette directive autorise, pour ces données, une durée de conservation allant de 6 mois au minimum à, en principe, 2 ans au maximum, à compter de la date de la communication.

En Allemagne, le recours à des dispositifs tels que les IMSI-catchers est autorisé. Le fait de savoir si la surveillance de données relevant de la correspondance par télécommunication au moyen de GovWare est légalement admissible dans le cadre d'une procédure pénale est fort contesté. Toutefois, le recours à des GovWare est, à des conditions strictes, admissible pour effectuer à titre préventif une perquisition en ligne, qui couvre en somme la surveillance de données relevant de la correspondance par télécommunication. La conservation des données secondaires, prévue pour une durée de 6 mois à compter de la date de la communication, est également controversée. La Cour constitutionnelle allemande a, en effet, déclaré les prescriptions relatives à l'enregistrement de ces données contraires au droit, tout en précisant que le principe de la conservation desdites données ne l'était pas, à condition que leur utilisation ne soit possible qu'en relation avec les infractions les plus graves.

En Autriche, la durée de conservation des données secondaires est de 6 mois à compter de la date de la communication. Le recours à l'IMSI-catcher est également autorisé. Le gouvernement autrichien a exprimé le souhait de créer une base légale permettant de procéder dans certains cas à une perquisition en ligne – couvrant en somme la surveillance de données relevant de la correspondance par télécommunication – au moyen de GovWare. Le projet y relatif était encore en main du parlement autrichien ces derniers mois.

En France, la durée de conservation des données secondaires est de 12 mois à compter de la date de la communication. Le recours à l'IMSI-catcher est permis. La perquisition en ligne au sens précité, par le recours à des GovWare, est à certaines conditions également autorisée.

En Italie, la durée de conservation des données secondaires varie de 12 mois à 24 mois à compter de la date de la communication, ce en fonction du type de données considéré. Le recours à l'IMSI-catcher et à des GovWare ne semble pas être explicitement réglé.

15 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54.

1.5 Classement d'interventions parlementaires

Les interventions ayant trait à la révision de la LSCPT, qui sont encore en suspens[16], seront traitées dans le cadre des dispositions pertinentes du présent projet. Le Conseil fédéral propose de classer ces interventions.

2 Commentaire des dispositions

2.1 Section 1 Dispositions générales

Art. 1 Champ d'application à raison de la matière

L'*art. 1* définit le champ d'application matériel de la LSCPT.

L'*al. 1* ne subit pas de changement fondamental par rapport à la version en vigueur. Le champ d'application matériel comprend la surveillance de la correspondance par poste. Il comprend également la surveillance de la correspondance par télécommunication, au sens de l'art. 269, al. 1, CPP et au sens où la notion de télécommunication est définie aux art. 2 et 3, let. c, LTC. La correspondance par Internet, qui comprend notamment la correspondance par messagerie électronique[17], est un type particulier de correspondance par télécommunication. Sa surveillance tombe donc dans le champ d'application matériel de la LSCPT. Il va de soi que la téléphonie par Internet, qui constitue de la correspondance par Internet, est également de la correspondance par télécommunication, ce qui implique que sa surveillance tombe aussi dans ce champ d'application. Le fait de savoir si une surveillance est admissible ne saurait dépendre du chemin de transmission des données et des technologies utilisées. Comme la téléphonie conventionnelle, la téléphonie par Internet est soumise au secret des télécommunications selon l'art. 43 LTC. Quant à l'art. 269 CPP, il contient la base légale pour la levée de ce secret dans le but d'obtenir des preuves dans le cadre d'une procédure pénale[18].

16 Cf. infra, ch. 2.4, 2.6 et 2.10 (ad art. 19, 26 et 39) ad 06.3170 Mo. Schweiger Rolf: Cybercriminalité. Protection des enfants, du 24.3.2006; ch. 2.1 et 2.6 (ad art. 2, 21, 26, 28 et 29) ad 07.3627 Mo. Glanzmann-Hunkeler Ida: Enregistrement obligatoire des cartes d'accès sans fil à prépaiement, du 3.10.2007; ch. 2.6 (ad art. 26) ad 10.4133 Mo. Barthassat Luc: Relever la durée de conservation des journaux d'attribution d'adresses IP, du 17.12.2010; ch. 2.2, 2.3, 2.6, 2.9 et 2.12 (ad art. 6 à 18, 26 et 38, art. 269bis et 269ter CPP et art. 70bis et 70ter PPM) ad 10.3831 Mo. Schmid-Federer Barbara: Révision de la LSCPT, du 1.10.2010; ch. 2.2, 2.3, 2.6, 2.9 et 2.12 (ad art. 6 à 18, 26 et 38, art. 269bis et 269ter CPP et art. 70bis et 70ter PPM) ad 10.3876 Mo. Eichenberger-Walther Corina: Révision de la LSCPT, du 1.10.2010; ch. 2.2, 2.3, 2.6, 2.9 et 2.12 (ad art. 6 à 18, 26 et 38, art. 269bis et 269ter CPP et art. 70bis et 70ter PPM) ad 10.3877 Mo. (von Rotz Christoph) Schwander Pirmin: Révision de la LSCPT, du 1.10.2010; ch. 2.12 (ad art. 269bis et 269ter CPP et art. 70bis et 70ter PPM) ad 11.4042 Po. Commission des affaires juridiques CN: Surveillance au moyen de chevaux de Troie (1), du 11.11.2011; ch. 2.12 (ad art. 269bis et 269ter CPP et art. 70bis et 70ter PPM) ad 11.4043 Po. Commission des affaires juridiques CN: Surveillance au moyen de chevaux de Troie (2), du 11.11.2011; ch. 2.9 (ad art. 38) ad 10.4210 Po. Recordon Luc: Coût de la surveillance pénale des télécommunications, du 23.12.2011.

17 Bernard Corboz, Les infractions en droit suisse, vol. II, Berne 2010, n. 6 ad art. 321ter CP.

18 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 14.

L'*al. 1, let. a* est modifié, en ce sens que les mentions au caractère fédéral ou cantonal de la procédure pénale sont supprimées. Ces mentions ne sont en effet plus nécessaires, avec l'entrée en vigueur du CPP, qui s'applique aux procédures fédérales et cantonales et qui prévoit la possibilité de mise en œuvre de surveillances de la correspondance par poste et télécommunication dans le cadre de ces procédures.

L'*al. 1, let. b* ne change pas en substance par rapport à sa formulation dans la LSCPT en vigueur.

La mention du sauvetage contenue dans l'*al. 1, let. c* de la LSCPT en vigueur peut être supprimée, car cet objectif découle logiquement de la volonté de rechercher la personne disparue (art. 35). Est également couverte par l'*al. 1, let. c* la recherche de personnes en cas de catastrophes (voir commentaire de l'art. 35).

L'*al. 1, let. d* prévoit que la LSCPT est nouvellement applicable lors de la recherche d'une personne condamnée à une peine privative de liberté, indépendamment de l'infraction commise, ou qui fait l'objet d'une mesure de privation de liberté, sur la base d'un jugement définitif et exécutoire (voir commentaire de l'art. 36).

L'*al. 2* concerne, comme l'al. 3 de la LSCPT en vigueur, les renseignements sur les services de paiement soumis à la loi du 17 décembre 2010 sur la poste (LPO)[19]. Les mentions au caractère fédéral ou cantonal de ces dispositions sont supprimées suite à l'entrée en vigueur du CPP, lequel est applicable aux procédures fédérales et cantonales et régit l'obligation de témoigner et l'obligation de renseigner les autorités aux art 284 et 285. La poste doit, concernant son activité relative au trafic des paiements, être qualifiée d'«établissement similaire» à une banque, au sens de l'art. 284 du code précité. Le renvoi opéré à l'*al. 2* porte par exemple également sur les dispositions considérées contenues dans la PPM.

Art. 2 Champ d'application à raison des personnes

L'*art. 2* détermine, comme cela est le cas à l'art. 1, al. 2 de la LSCPT en vigueur, le champ d'application à raison des personnes, c'est-à-dire les personnes soumises à la loi, qui ont des obligations en vertu de celle-ci. L'ensemble de ces personnes est défini dans le projet et dans le présent message par l'expression générique «personnes obligées de collaborer». Les diverses obligations de surveillance de chacune de ces différentes catégories de personnes sont, quant à elles, réglées en particulier aux art. 19 à 30 du projet.

Les avis exprimés durant la procédure de consultation furent partagés s'agissant de l'extension du champ d'application à raison des personnes proposé dans l'AP-LSCPT. Passablement de cantons et d'organisations en matière de poursuite pénale soutiennent une telle extension. Mais nombreux sont aussi ceux, notamment les organisations de protection des consommateurs et des fournisseurs de services de télécommunication, qui s'opposent à l'extension proposée ou qui demandèrent une reformulation de celle-ci, telle qu'elle était proposée à l'art. 2, al. 1, let. b AP-LSCPT. Se posait la question de savoir si l'art. 2, al. 1, let. b AP-LSCPT était formulé de manière compréhensible et s'il n'allait pas trop loin, notamment quant à sa portée et quant à ses implications économiques pour les personnes concernées. S'est également posée la question de savoir si le fait d'intégrer les fournisseurs d'hébergement (hosting providers), constituant des fournisseurs de services Internet,

19 RS **783.0**

dans le champ d'application à raison des personnes était une bonne chose. Pour le surplus, voir le rapport de consultation[20].

Le champ d'application à raison des personnes n'est effectivement pas assez clair dans le droit en vigueur. Ceci vaut en particulier pour la teneur de l'art. 2, al. 1, let. b AP-LSCPT. On pouvait l'interpréter en ce sens que serait tombée dans le champ d'application toute personne qui, d'une manière ou d'une autre, avait affaire à des données de communication (p.ex. une entreprise se limitant à offrir des solutions en matière de sécurité des réseaux). Ceci allait trop loin, y compris par rapport aux coûts engendrés pour les personnes concernées. Cette absence de clarté fut par conséquent corrigée dans le projet.

Le projet prévoit de conférer diverses obligations à diverses catégories de personnes (voir commentaire des let. a à f), caractérisées par leurs activités, chacune de ces activités devant à cet égard être considérée indépendamment des autres. Une même entreprise peut donc fort bien tomber dans plusieurs catégories, en fonction des activités qu'elle propose, et donc avoir des obligations de surveillance distinctes, en fonction de ces activités (voir art. 19 à 30). La LSCPT s'applique à toute personne, que ce soit une personne physique ou un organisme, peu importe que celui-ci revête la qualité de personne morale ou non ou qu'il soit étatique ou non, qui remplit les conditions des différentes catégories précitées.

Le champ d'application à raison des personnes est ainsi précisé et modifié par rapport au droit en vigueur; celui-ci ne mentionne, en effet, que les fournisseurs de services postaux ou de télécommunication, dont font partie les fournisseurs d'accès à Internet, et les exploitants de réseaux de télécommunication internes et de centraux domestiques. D'autres personnes en effet que celles précitées peuvent, à un moment ou à un autre, détenir des données relatives à la correspondance par poste ou télécommunication susceptibles d'intéresser les autorités de poursuite pénale dans le cadre de la lutte contre la délinquance. Il est donc légitime qu'elles soient également soumises à des obligations dans le domaine de la surveillance de cette correspondance. Citons, entre autres, les fournisseurs de services Internet que sont les fournisseurs d'hébergement (hosting providers) (voir commentaire de la let. c).

Le champ d'application à raison des personnes est aussi modifié par rapport à la loi actuelle, du fait que, à la différence de celle-ci, la nouvelle LSCPT ne prévoit pas que les fournisseurs de services postaux ou de télécommunication doivent être soumis à concession ou à l'obligation d'annoncer pour tomber dans ledit champ d'application (voir commentaire des let. a et b)[21].

La *let. a* vise non seulement La Poste Suisse, en tant que fournisseur de services postaux, mais également tous les autres acteurs sur le marché postal, fournissant ces services. Contrairement à ce que prévoit la LSCPT actuelle, l'assujettissement d'un fournisseur de services postaux à la nouvelle LSCPT ne dépend pas du fait de savoir si celui-ci est soumis à concession ou à l'obligation d'annoncer. Ceci implique en particulier que même les fournisseurs qui ne sont pas soumis à l'obligation d'annonce ordinaire au sens de l'art. 3 de l'ordonnance du 29 août 2012 sur la poste[22] tombent dans le champ d'application à raison des personnes. A titre d'exemple, citons les fournisseurs de services de courrier et de services de poste

20 www.admin.ch/ch/f/gg/pc/documents/1719/Rapport_C_surveillance_correspondance_par_poste_et_telecommunication.pdf
21 Thomas Hansjakob, op. cit. (note 11), n. 24 ad art. 1 LSCPT.
22 RS **783.01**

rapide. En revanche, les fournisseurs de services postaux offrant des services bancaires ne sont, pour cette activité-ci, pas visés ici (voir aussi commentaire de l'art. 1, al. 2).

La *let. b* vise les acteurs centraux dans le domaine de la surveillance de la correspondance par télécommunication que sont les fournisseurs de services de télécommunication. C'est la législation en matière de télécommunications, à savoir l'art. 3, let. a à c, en particulier la let. b, LTC et l'art. 2 de l'ordonnance du 9 mars 2007 sur les services de télécommunication (OST)[23], qui définit ce qu'est un fournisseur de services de télécommunications au sens de la LSCPT. Ce qui est ou n'est pas un fournisseur de services de télécommunication en vertu de la législation précitée l'est ou, respectivement, ne l'est également pas en vertu de la LSCPT. En résumé, le fournisseur de services de télécommunication s'engage à transporter, à transmettre lui-même pour le compte d'un tiers, pour le public, au moyen de techniques de télécommunication (au sens de l'art. 3, let c LTC), des informations (au sens de l'art. 3, let. a LTC). Les personnes visées par la let. c, tels que les fournisseurs d'hébergement (hosting providers), ne constituent pas des fournisseurs de services de télécommunication puisqu'elles ne transmettent, ne transportent pas, *a fortiori* elles-mêmes, de données (voir commentaire de la let. c). Il en va de même des personnes visées à la let. e, comme les Internet ou cybercafés et les hôtels, étant donné qu'elles ne transmettent pas elles-mêmes des données (voir commentaire de la let. e). La situation est la même pour les personnes visées à la let. d puisqu'elles ne transmettent pas des données pour le compte d'un tiers, pour le public (voir commentaire de la let. d). Constituent par exemple des fournisseurs de services de télécommunication les grands opérateurs actifs sur le marché suisse tels que Swisscom, Orange, Sunrise et Cablecom, qui permettent aux usagers de téléphoner, au moyen d'un téléphone fixe ou mobile, ou d'accéder à Internet. Les fournisseurs d'accès à Internet constituent en effet des fournisseurs de services de télécommunication au sens de la législation en matière de télécommunications et, par conséquent, au sens de la LSCPT; ce, indépendamment du fait de savoir s'ils exercent, en outre, une autre activité, comme celle d'opérateur téléphonique. Il n'en va, en revanche, pas de même des autres fournisseurs Internet, tels que les fournisseurs de services Internet, notamment les fournisseurs d'hébergement (hosting providers). Ceux-ci sont, le cas échéant, saisis à la let. c (pour le surplus, voir commentaire de la let. c).

La *let. b* ne prévoit pas, contrairement à la LSCPT en vigueur, que seuls les fournisseurs de services de télécommunication soumis à concession ou à l'obligation d'annoncer (art. 4, al. 1 LTC) tombent dans le champ d'application à raison des personnes. Il est donc théoriquement possible qu'un fournisseur de services de télécommunication soit dispensé d'obligations découlant de la législation en matière de télécommunications, en vertu des art. 4, al. 2, LTC et 3 OST, mais ne le soit pas en vertu de la législation en matière de surveillance de la correspondance par poste et télécommunication, étant entendu que celle-ci peut aussi prévoir de telles dispenses (voir commentaire de l'art. 26, al. 6).

La *let. c* vise des personnes qui ne constituent ni des fournisseurs d'accès à Internet ni, partant, des fournisseurs de services de télécommunication au sens de la loi (voir commentaire de la let. b) mais jouent également un rôle dans le processus de correspondance par télécommunication en particulier par Internet, en fournissant des services qui ne peuvent être offerts qu'en relation avec l'activité d'un fournisseur de

23 RS **784.101.1**

services de télécommunication, plus précisément d'un fournisseur d'accès à Internet. Ces personnes ne sont pas des fournisseurs de services de télécommunication, étant donné qu'elles ne transmettent, ne transportent pas, *a fortiori* elles-mêmes, des données. Sans fournisseur de services de télécommunication, transmettant des données, lesdites personnes, qui sont des fournisseurs de services Internet, ne peuvent pas fournir leurs services. Elles sont donc désignées ci-après «fournisseurs de services de communication dérivés».

Sont visés à la *let. c* les fournisseurs de services Internet qui permettent une communication unilatérale, rendant possible le chargement de documents (p.ex. Google docs ou Microsoft office.live.com), et ceux qui permettent une communication multilatérale, rendant possible la communication entre usagers (p.ex. Facebook); peu importe si on a affaire à une communication synchrone ou asynchrone. Sont, par exemple, à qualifier comme tels les fournisseurs d'espace de stockage d'e-mails, les différents types de fournisseurs d'hébergement (hosting providers) qui fournissent, par exemple, un hébergement d'applications ou services e-mail (p.ex. .gmx), un hébergement «colocation de serveurs» ou «server housing» avec accès (p.ex. Green.ch et Colt), un hébergement «Facility Management» sans service de communication (colocation pure) ou des services «cloud», les plates-formes de chat, les plates-formes d'échange de documents et les fournisseurs de services de téléphonie par Internet du type peer-to-peer (p.ex. Skype peer-to-peer). Il convient de préciser qu'une entreprise qui propose un produit permettant le cryptage ne «permet» pas la communication, au sens de la *let. c*, mais ne fait au plus que la faciliter, raison pour laquelle elle n'est pas saisie par cette disposition et, partant, par le champ d'application à raison des personnes. Il y a lieu de noter qu'une même entreprise, par exemple Swisscom, peut fort bien, en fonction de ses activités considérées, constituer à la fois un fournisseur de services de télécommunication et une personne visée à la let. c, pour son activité d'e-mail provider ou de fournisseur d'hébergement (hosting providers). Le cas échéant, elle pourra avoir des obligations de surveillance distinctes, en fonction de ces différentes activités (voir art. 26 et 27).

Relevons, toutefois, que – comme cela ressort déjà des exemples d'entreprises susmentionnées – l'intégration des personnes visées par la *let. c* dans le champ d'application à raison des personnes ne saurait susciter des espoirs démesurés pour la surveillance de la correspondance par télécommunication. En effet, beaucoup de fournisseurs importants de services Internet ont leur siège et leur infrastructure à l'étranger. L'ouverture de certains comptes e-mail sis à l'étranger par des personnes vivant en Suisse, soit des services en soi techniquement contrôlables, est un exemple qui illustre cet état de fait. Prévoir, de manière générale, que les autorités suisses pourraient sans problème accéder aux données voulues serait donc irréaliste et problématique, puisque cela se heurterait au principe de la territorialité des lois. Une telle réglementation n'existe pas dans le droit en vigueur. Concernant l'obligation de dépôt des fournisseurs de services de communication dérivés portant sur des données (secondaires), nous renvoyons au commentaire de l'art. 27, al. 2.

Les personnes saisies à la *let. d* ne constituent pas des fournisseurs de services de télécommunication (voir commentaire de la let. b), parce qu'elles ne fournissent pas des services à des tiers, au public, mais uniquement à un cercle restreint de personnes ayant une qualité particulière; ces réseaux ne sont donc pas accessibles à tous. On peut citer à titre d'exemple une entreprise mettant un réseau de télécommunication à la disposition de ses collaborateurs pour communiquer entre eux ou une collectivité publique qui permettrait à ses employés de communiquer ensemble au

moyen d'un tel réseau (voir art. 2 OST). Les personnes visées sont les mêmes que celles mentionnées à l'art. 1, al. 4 de la LSCPT en vigueur. On ne parle toutefois plus d'exploitants de centraux domestiques, mais uniquement d'exploitants de réseaux de télécommunication internes, car la notion de central domestique, qui implique également l'existence d'un réseau, est couverte par celle de réseau de télécommunication interne. Voir le commentaire de l'art. 28.

La *let. e* vise des personnes qui laissent leur accès à la disposition de tiers. Il peut s'agir d'hôtels, de restaurants, de cafés, de cafés Internet ou cybercafés, d'hôpitaux, d'écoles, etc. qui mettent leur accès à Internet (Wi-Fi, fixe ou autre) à la disposition de tiers, en particulier de leurs clients, patients, écoliers, etc. Il peut aussi s'agir du simple particulier qui en fait de même, volontairement ou non, pour des tiers. L'intégration de ces personnes dans le champ d'application à raison des personnes est en particulier une conséquence de ce que demande la motion 07.3627 Glanzmann-Hunkeler. En effet, elles ne sont pas mentionnées aujourd'hui. Ces personnes ne constituent pas des fournisseurs de services de télécommunication, étant donné qu'elles ne transmettent pas elles-mêmes des informations pour le compte de tiers, cette fonction étant dévolue aux fournisseurs de services de télécommunication comme Swisscom, Orange, Sunrise et Cablecom (voir commentaire de la let. b). Pour la relation des obligations des personnes objet de la let. e avec la motion 07.3627 Glanzmann-Hunkeler, nous renvoyons au commentaire de l'art. 29.

La *let. f* est formulée de manière relativement ouverte afin de tenir compte des évolutions technologiques. Elle concerne en particulier non seulement le domaine de la téléphonie mobile mais également celui de la téléphonie fixe et d'Internet et vise donc aujourd'hui avant tout les revendeurs des moyens que sont les cartes SIM à prépaiement et les cartes d'accès sans fil à Internet à prépaiement. Ne sont en revanche pas concernés les revendeurs de simples cartes téléphoniques permettant, en lieu et place de l'argent, de téléphoner dans des cabines téléphoniques (p.ex. «taxcards», contenant un crédit, vendues dans les kiosques). Les revendeurs visés par la *let. f* (p.ex. Interdiscount, Media Markt et Mobilezone) ne constituent pas des fournisseurs de services de télécommunication (voir commentaire de la let. b) mais des revendeurs de moyens de ceux-ci (p.ex. Swisscom, Orange et Sunrise). L'intégration des revendeurs de cartes d'accès sans fil à Internet à prépaiement dans le champ d'application à raison des personnes est notamment une conséquence de ce que demande la motion 07.3627 Glanzmann-Hunkeler. Les personnes visées par la *let. f* ne sont aujourd'hui pas saisies par le champ d'application de la loi. Cette disposition a en outre pour objectif de contribuer à combler une lacune par rapport à l'obligation des fournisseurs de services de télécommunication d'enregistrer des données de leurs clients à qui ils remettent des cartes SIM à prépaiement (voir commentaire de l'art. 30). Pour les obligations des revendeurs de cartes d'accès sans fil à Internet à prépaiement, voir le commentaire de l'art. 30.

Art. 3 Service de surveillance

L'*art. 3* reprend l'art. 2 de la LSCPT en vigueur et le complète.

Il découle de l'*al. 1* que le service est l'interface entre les autorités de poursuite pénale, qui ordonnent les surveillances, et les personnes tombant dans le champ d'application de la loi (en particulier les fournisseurs de services de télécommunication), qui exécutent les surveillances ordonnées. Il importe ici de préciser que le service ne joue ce rôle que pour les mesures de surveillances de la correspondance

par poste et télécommunication relevant de l'art. 269 CPP, c'est-à-dire en relation avec les surveillances classiques. Il ne joue en revanche aucun rôle particulier dans l'utilisation de dispositifs techniques de surveillance, tels que les IMSI-catchers, ou de GovWare, ce qui implique qu'aucun ordre de surveillance y relatif n'a à lui parvenir (pour les détails, voir le commentaire des art. 269bis et 269ter CPP).

L'*al. 2* reprend l'art. 2, al. 2, de l'actuelle LSCPT. L'indépendance du service concerne toutefois la relation avec le DFJP et le Conseil fédéral et non celle avec les autorités de poursuite pénale. Par rapport à celles-ci, le service est de toute façon indépendant d'un point de vue hiérarchique (c'est-à-dire qu'il n'existe pas de droit de donner des directives au service ou d'agir à la place de celui-ci dans son domaine de compétences). Le service est toutefois lié par les ordres de surveillance exécutables rendus par les autorités de poursuite pénale. Son indépendance du DFJP et du Conseil fédéral est primordiale pour lui permettre d'accomplir cette fonction d'exécution: Il devrait servir deux maîtres s'il était en même temps lié à l'ordre autorisé par une autorité judiciaire et aux éventuelles directives du DFJP. En tant qu'autorité politique, le DFJP serait en outre dans une position inconfortable si, en tant qu'autorité de surveillance, il devait assumer la responsabilité d'actes du service prédéfinis par des ordres autorisés par des autorités judiciaires. Pour ce qui concerne le droit du personnel, la loi du 24 mars 2000 sur le personnel de la Confédération[24] et l'ordonnance du 3 juillet 2001 sur le personnel de la Confédération[25] sont applicables aux rapports de travail des employés du service.

La collaboration visée à l'*al. 3* doit être réciproque. Il appartient en particulier aux autorités visées dans cet alinéa, notamment à l'OFCOM et aux autorités de poursuite pénale, de soutenir dans les limites de la loi le service dans l'exécution de ses tâches. L'al. 3 n'a pas pour objet de conférer une tâche de contrôle aux partenaires du service portant sur le respect de la législation relative à la surveillance de la correspondance par poste et télécommunication. La surveillance administrative fait en effet l'objet de l'art. 41.

Art. 4 Traitement des données personnelles

L'*art. 4* s'inspire de l'actuel art. 7, al. 1, OSCPT. Il concerne en particulier la police; ce non seulement dans les cas où elle peut agir de son propre chef mais également lorsqu'elle agit sous les ordres du ministère public. Les détails relatifs aux modalités de ce traitement demeurent réglés dans l'ordonnance précitée.

Art. 5 Organe consultatif

Au vu des intérêts contradictoires que peuvent avoir les différents acteurs dans le domaine de la surveillance de la correspondance par poste et télécommunication, la collaboration de ceux-ci, au sein d'un organe consultatif, est essentielle pour permettre la bonne exécution des surveillances et un développement efficace dans ce domaine. C'est ce que montre l'expérience. Une telle collaboration existe déjà sur une base informelle, sans être prévue dans un texte de loi. La nouvelle disposition soulignera toutefois l'importance de la collaboration et encouragera les acteurs à s'engager pleinement dans un organe formellement constitué. Pour atteindre l'objectif précité, il n'est pas nécessaire de conférer à l'organe des compétences

24 RS **172.220.1**
25 RS **172.220.111.3**

décisionnelles. Il suffit de lui conférer un rôle consultatif, qu'il peut toutefois exercer de manière active, en émettant des recommandations de sa propre initiative. L'*art. 5* permettra au DFJP de formaliser cette collaboration.

L'*al. 1* constitue la base légale pour une collaboration formelle entre ces différents acteurs dans le domaine de la surveillance de la correspondance par poste et télécommunication. Il donne la possibilité au DFJP de prévoir un organe consultatif à cet effet, composé de représentants des différents acteurs en la matière.

L'*al. 2* dresse un cadre sommaire pour les activités de l'organe consultatif et mentionne les objectifs visés par celui-ci.

L'*al. 3* confie la tâche au DFJP d'adopter les dispositions de détail relatives à la composition et au fonctionnement de l'organe consultatif qu'il a la possibilité de mettre en place en vertu de l'al. 1.

Le DFJP décidera quelles organisations participeront à l'organe consultatif et qui pourra déterminer les personnes physiques qui représentent ces organisations. Sachant que l'on vise en premier lieu un échange d'expériences entre les autorités et entreprises concernées, la composition de l'organe devrait aussi pouvoir se déterminer ad hoc, en fonction des connaissances spéciales (de nature technique ou administrative) requises. En ce sens, on peut par exemple prévoir que chaque organisation pourra déléguer une personne en fonction des thèmes abordés et des compétences de celle-ci. Doit en outre être tranchée la question de savoir si d'autres personnes encore peuvent être invitées à participer à l'organe consultatif, le cas échéant avec quelles compétences. Le DFJP devra également déterminer les personnes qui assureront la présidence et le secrétariat de l'organe consultatif, ainsi que leurs compétences, comment seront prises les décisions au sein de celui-ci, si et comment seront publiées les prises de positions et les recommandations de l'organe consultatif et quelles informations doivent, le cas échéant, être soumises au secret de fonction. Les membres ne seront pas indemnisés par la Confédération, mais par l'organisation qu'ils représentent.

2.2 Section 2 Système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication

Les art. 6 à 14 régissent le fonctionnement, sous l'angle du traitement des données, du nouveau système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication exploité par le service, à savoir l'«Interception System Schweiz» (ISS). Celui-ci contiendra, en particulier, les données collectées lors de surveillances de la correspondance par télécommunication relevant de l'art. 269 CPP, c'est-à-dire en relation avec les surveillances classiques. Il ne contiendra en revanche pas les données collectées lors de surveillances effectuées au moyen de dispositifs techniques de surveillance tels que les IMSI-catchers ou de GovWare. L'ISS n'est, en effet, censé recevoir que des données ayant une relation avec les activités du service. Or celles obtenues au moyen d'un IMSI-catcher ou d'un GovWare n'en sont pas et l'ISS n'est pas un système policier (pour les détails, voir le commentaire de l'art. 269bis et 269ter CPP).

Suite à sa réponse au ch. 3 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT), le Conseil fédéral a étudié la question de savoir s'il serait judicieux de soumettre ce système à la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[26]. Il est arrivé à la conclusion que tel n'est pas le cas parce que la LSIP ne s'applique en vertu de ses art. 1 et 2 qu'à des systèmes d'information exploités par fedpol, alors que le nouveau système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication relèvera uniquement de la compétence du service. Parle également en faveur de ce qui précède le fait que le service ne constitue pas une autorité pénale, en particulier une autorité de poursuite pénale.

La conservation centralisée de longue durée des données et les art. 6 à 13 AP-LSCPT, en particulier les art. 9 à 11 AP-LSCPT, ont été accueillis de manières diverses dans le cadre de la procédure de consultation. Plusieurs cantons, des organisations issues du milieu de la poursuite pénale et la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) ont soutenu le principe de la conservation centralisée, tout en demandant des aménagements que l'on retrouve dans le système actuel. D'autres participants à la consultation, en particulier des cantons, ont demandé que seules les données issues de surveillances Internet soient, au vu de la quantité qu'elles représentent, conservées de manière centralisée, les autres données continuant d'être envoyées par la poste sur des supports de données. Un nombre plus important de cantons et d'organisations en matière de poursuite pénale était plus critique. Certains ont souligné le caractère extrêmement compliqué de la réglementation prévue dans ces articles, éventuellement leur incompatibilité avec le CPP. D'autres se sont opposés à la conservation centralisée de ces données auprès du service et à l'accès online de ces données, également du prévenu et de son défenseur, pour des raisons de sécurité, préférant obtenir celles-ci sur des supports de données. D'autres encore ont avancé les deux critiques.

Après examen de la question, le Conseil fédéral a finalement opté, en particulier avec le soutien du service et de certains représentants des autorités de poursuite pénale, pour la conservation centralisée de longue durée des données collectées lors de la surveillance de la correspondance par télécommunication dans le système informatique exploité par le service. Ceci s'appliquera à toutes les données issues de surveillances de la correspondance par télécommunication, aussi bien à celles issues de surveillances téléphoniques traditionnelles qu'à celles issues de surveillances Internet. Le présent projet prévoit toutefois des dispositions plus pertinentes, plus simples et plus praticables pour cette conservation que celles qui figuraient dans l'AP-LSCPT (voir le commentaire des art. 9 à 11).

La procédure proposée remplace le régime actuel, aux termes duquel le service transmet par la poste, sur des supports de données, toutes les données collectées aux autorités (de poursuite pénale). En vertu de la réglementation en vigueur, dès que celles-ci en ont accusé réception au service, celui-ci les efface dans son système. Les données, éventuellement retranscrites par la police ou par un autre service, sont conservées au dossier judiciaire, comme n'importe quelle pièce faisant partie du dossier.

26 RS **361**

Dans la procédure proposée, l'accès des autorités (de poursuite pénale) aux données issues de surveillances de la correspondance par télécommunication concernant des dossiers relevant de leur compétence se fait au moyen d'un accès en ligne au système exploité par le service. Les parties, y compris le prévenu et son avocat, peuvent également y accéder en ligne en faisant usage d'un terminal d'accès mis à leur disposition auprès de l'autorité en charge du dossier. Comme c'est le cas actuellement, les données issues de surveillances de la correspondance par télécommunication pourront cependant, sur demande et à certaines conditions, continuer à être transmises, toutefois cryptées, sur des supports de données mobiles. Il n'est pas souhaitable que des autorités étrangères aient, dans les cas de procédure d'entraide judiciaire internationale, accès au système exploité par le service pour obtenir ces données.

L'argument qui, malgré les réticences émises en consultation, plaide avant tout pour un abandon du système actuel au profit d'un système de conservation centralisée (de longue durée) des données dans le système informatique du service, est le fait que les données collectées, en particulier celles issues de surveillances Internet, sont, pour chaque surveillance, de plus en plus nombreuses, ce qui implique qu'elles peuvent de plus en plus difficilement être transmises par la poste sur des supports de données aux autorités. De plus, ces supports peuvent de plus en plus difficilement être stockés et administrés, notamment pour des raisons de place, en tout cas dans les grands cantons. Cette tendance ne fera que se confirmer ces prochaines années, avec les futurs développements techniques. Le changement proposé permet de remédier à ce problème. Il permet, en outre, d'améliorer la sécurité des données, en évitant certains risques liés au système actuel, qui prévoit l'envoi des données par la poste (p.ex. perte, vol et multiplication des supports de données). Il instaure par ailleurs une meilleure collaboration entre les différentes autorités de poursuite pénale en charge du dossier dont relèvent les données de communication. Le système proposé implique que le service devra, en tenant compte de l'évolution de la technique, assurer sur le long terme de manière centralisée la lisibilité des données contenues dans le système qu'il exploite; ceci présente de plus l'avantage d'éviter que chaque canton doive individuellement effectuer cette tâche. Cette modification permettra, en outre, une utilisation plus aisée des programmes nécessaires à l'exploitation des données, en évitant les risques d'incompatibilité entre le système exploité par le service et ceux qui seraient exploités, de manière décentralisée, par les cantons.

La conservation centralisée de longue durée des données collectées lors de la surveillance de la correspondance par télécommunication entraînera un surcroît de dépenses pour la Confédération. Elle pourrait par contre se traduire par une baisse des coûts pour les cantons en ce qui concerne les charges d'équipement. Le surcroît de dépenses pour la Confédération dû à l'augmentation des délais de conservation des données auprès du service est susceptible d'avoir des incidences sur les émoluments payés par les autorités de poursuite pénale, notamment par celles des cantons (art. 38, al. 3). Ces frais supplémentaires seront toutefois acceptables, au vu des améliorations que ce changement amènera et au vu du fait que les coûts liés aux surveillances sont très faibles au regard de la totalité de coûts liés à la poursuite pénale. Ces coûts sont distincts de ceux liés à l'acquisition de l'ISS. Nous renvoyons également au ch. 3.1.

Art. 6 Principe

L'*art. 6* s'inspire de l'al. 1 de l'art. 8 de l'actuelle OSCPT. Il confère le droit au service d'exploiter un tel système. Le système peut être composé de plusieurs sous-systèmes et fonctionner sur des serveurs différents. Les données contenues dans le système sont énoncées à l'art. 8. Le système ne contient pas les données collectées lors de la surveillance de la correspondance par poste, celles-ci étant directement transmises à l'autorité qui a ordonné la surveillance, conformément à l'art. 19. Il sera sécurisé de manière adéquate (voir en particulier le commentaire de l'art. 12).

Art. 7 But du système de traitement

L'objectif mentionné à la *let. a* est le but premier de l'ISS. Il est conforme au but actuel du système de traitement des données relatives à la surveillance de la correspondance par télécommunication, sous réserve de la consultation en ligne. Les données visées sont les données de contenu des communications et les données secondaires de télécommunication. Pour le surplus, voir le commentaire de l'art. 8, let. a et b. C'est l'art. 9 qui détermine qui a accès aux données considérées et dans quelles conditions cet accès ne peut être effectué en ligne. Pour le surplus, voir les explications introductives concernant le ch. 2.2.

La conservation centralisée de longue durée des données vise à atteindre l'objectif de la *let. b*. Pour le surplus, voir les explications introductives ci-dessus, concernant le ch. 2.2.

La *let. c* porte sur les renseignements faisant l'objet des art. 15, 21 et 22. L'art. 23 régit les modalités applicables à ces renseignements, notamment quant à l'accès. Pour le surplus, voir le commentaire des art. 15 et 21 à 23.

Les données que le système informatique permettra selon la *let. d* de traiter sont celles énoncées à l'art. 8. Les fonctions de traitement ne sont pas destinées au prévenu (ou à son représentant). Celui-ci aura accès aux données le concernant (voir commentaire de l'art. 9, al. 1) dans le respect des dispositions de la procédure pénale. L'exploitation par les autorités de poursuite pénale des données collectées lors de surveillances aura lieu dans les systèmes d'information pertinents du réseau de systèmes d'information de police de l'Office fédéral de la police (voir commentaire de l'art. 14).

La *let. e* vise l'exécution des ordres de surveillance de la correspondance par télécommunication et le contrôle de cette exécution (p.ex. controlling, saisie des mandats, attribution des mandats et administration).

Art. 8 Contenu du système de traitement

Les données mentionnées à l'*art. 8, let. a et b,* sont celles que l'on peut obtenir dans le cadre d'une surveillance de la correspondance par télécommunication. Pour les détails, voir le commentaire de l'art. 26, al. 1. Concernant les *let. c et d*, voir le commentaire de l'art. 7, let. c et e.

Art. 9 Accès au système de traitement

L'art. 9 AP-LSCPT a été critiqué par passablement de monde durant la procédure de consultation en particulier au motif que la réglementation proposée était trop compliquée, ne tenait pas compte du risque de dysfonctionnement qu'il engendre ainsi

que des possibilités actuelles de se dessaisir d'un dossier, de joindre et disjoindre des procédures et qu'il était de surcroît inutile. Le Conseil fédéral considère que ces critiques sont pour une bonne part justifiées. Partant, le présent projet propose une réglementation plus pertinente, plus simple et plus praticable pour les autorités, en particulier pour les autorités de poursuite pénale; la charge administrative du service s'en touve du même coup réduite par rapport à ce que proposait l'art. 9 AP-LSCPT.

L'*al. 1* correspond sur le fond au régime actuel. Il appartientdra au service de mettre en œuvre dans le système de traitement les droits d'accès en ligne. Et c'est l'autorité qui a ordonné la surveillance ou celle qui dirige subséquemment la procédure dont relèvent les données collectées lors de cette surveillance, c'est-à-dire, en somme, l'autorité en charge du dossier, qui aura accès au système de traitement. La formulation proposée à l'*al. 1* permet donc bien entendu à l'autorité qui a repris un dossier dont relèvent des données collectées lors d'une surveillance d'accéder à ces données, même si elle n'a pas ordonné elle-même cette surveillance. Sont en particulier visées par cette hypothèse l'autorité qui se saisit du dossier suite à une jonction de causes ou celle qui s'en saisit suite à un recours. L'autorité visée à l'*al. 1* est le maître du fichier (voir art 13). Conformément au principe de la proportionnalité, une autorité mentionnée à l'*al. 1* ne peut accéder qu'aux données contenues dans le système de traitement qui ont été collectées lors d'une surveillance déterminée, et non à toutes les données collectées lors d'une surveillance, qui figurent dans le système. Selon la réglementation proposée, par exemple, les policiers travaillant sur un dossier pourront aussi accéder en ligne aux données collectées lors d'une surveillance, avec l'autorisation du ministère public en charge du dossier. Seules des autorités suisses pourront accéder au système exploité par le service. Il n'est en effet pas souhaitable que des autorités étrangères puissent, en particulier dans les cas de procédures d'entraide judiciaire internationale, y avoir accès (voir al. 4). Il sied de noter que les parties, y compris le prévenu et son avocat, pourront également, dans l'exercice du droit d'être entendu (art. 29, al. 2 de la Constitution [Cst.][27]), accéder en ligne aux données de télécommunication les concernant, en faisant usage d'un terminal d'accès mis à leur disposition auprès de l'autorité en charge du dossier.

La réglementation prévue à l'*al. 2* permet d'éviter que les autorités visées à l'al. 1 et les personnes désignées par celles-ci accèdent aux données lorsqu'elles ne sont plus en charge du dossier, c'est-à-dire à des données dont elles n'ont plus besoin. Une autorité peut demeurer en charge d'un dossier pendant de nombreuses années. Il n'est pas forcément nécessaire que son accès aux données demeure actif pendant toute cette période. Durant celle-ci, il peut donc être judicieux de prévoir un mécanisme de désactivation après un certain temps et de réactivation de l'accès considéré. Le Conseil fédéral pourra édicter des dispositions y relatives en vertu de l'art. 12, al. 2.

Le devoir d'information visé à l'*al. 3* a, d'une part, pour but de permettre le respect de l'al. 2 et, d'autre part, de permettre au service de savoir, lorsqu'il est contacté par une autorité autre que celle à qui il garantissait l'accès au système en relation avec la surveillance considérée, s'il doit lui permettre d'accéder en ligne aux données collectées lors de cette surveillance selon l'al. 1 (voir aussi commentaire de l'al. 1). Le Conseil fédéral pourra fixer les modalités de l'information faisant l'objet de l'*al. 3*.

27 RS **101**

L'*al. 4* prévoit que les données issues de surveillances de la correspondance par télécommunication pourront cependant, comme c'est le cas aujourd'hui, continuer à être transmises – si possible cryptées – sur des supports de données mobiles dans deux hypothèses: lorsque l'autorité suisse en charge du dossier doit transmettre ces données à une autorité étrangère (*let. a*), sachant qu'il n'est pas souhaitable que des autorités étrangères puissent obtenir ces données par un accès en ligne au système, et lorsque des problèmes techniques ne permettent pas de consulter les données en ligne (*let. b*). Concernant le cryptage, voir aussi le commentaire de l'art. 12, al. 2.

Art. 10 Droit de consulter le dossier et droit d'accès aux données

L'art. 10 AP-LSCPT a également été contesté par un grand nombre de participants à la procédure de consultation. Il a, en particulier, été allégué qu'il était en partie inutile, au motif que le CPP contient les dispositions idoines pour protéger les données personnelles, et que les renvois qui y étaient opérés étaient superflus, voire non pertinents. De l'avis du Conseil fédéral, ces critiques sont en partie justifiées. Le présent projet propose donc une réglementation revue, tenant compte de ces critiques.

L'*al. 1* règle les droits de consultation et d'accès s'agissant des données collectées dans le cadre d'une procédure pénale (art. 1, al. 1, let. a) ou d'une demande d'entraide judiciaire (art. 1, al. 1, let. b), que celle-ci soit une demande d'extradition ou une demande portant sur un autre cas d'entraide judiciaire. Il distingue les droits dans le cadre d'une procédure pendante (*let. a*) de ceux après la clôture de la procédure (*let. b*). L'*al. 1, let. a* dispose que, dans le cadre d'une procédure pendante, c'est le droit de la procédure applicable qui s'applique au droit de consulter le dossier et au droit aux renseignements. Ces droits sont donc régis par le CPP ou les autres dispositions de la procédure applicables, comme la PPM. De fait, l'*al. 1* renvoie en particulier aux art. 97, 101 et 279 CPP. L'*al. 1, let. b*, concerne le droit d'accès aux données après la clôture de la procédure. Il en découle en somme que ce sont en particulier les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[28] qui s'appliquent à ce droit lorsque l'autorité en charge de la demande d'entraide judiciaire est une autorité de la Confédération. Lorsque l'autorité saisie de la demande d'entraide judiciaire est une autorité d'un canton, l'art. 37, al. 1 LPD s'applique à titre subsidiaire au droit d'accès aux données si le droit cantonal n'assure pas un niveau de protection adéquat.

Quelques particularités relatives à la procédure d'entraide judiciaire doivent être relevées. Lorsque ces données ont été collectées lors de l'exécution d'une demande d'extradition, ces droits sont régis par les art. 18*a*, al. 4 de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP)[29], les art. 26 et 27 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[30] – applicable en vertu de l'art. 12, al. 1, phr. 1 EIMP – et les art. 8 et 9 LPD. Dans les autres cas d'entraide judiciaire, les droits de la personne concernée sont régis par les art. 18*a*, al. 4 et 80*b* EIMP, l'art. 9 de la loi fédérale du 3 octobre 1975 relative au traité conclu avec les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale[31] et l'art. 46 de la loi fédérale du 22 juin 2001 sur la coopération avec la Cour

28 RS **235.1**
29 RS **351.1**
30 RS **172.021**
31 RS **351.93**

pénale internationale (LCPI)[32] ainsi que par les art. 8 et 9 LPD (si l'autorité saisie de la demande d'entraide judiciaire est une autorité de la Confédération) ou par le droit cantonal (si cette autorité est celle d'un canton). Il sied de noter que la loi fédérale du 21 décembre 1995 relative à la coopération avec les tribunaux internationaux chargés de poursuivre les violations graves du droit international humanitaire (art. 2)[33] et les Conventions internationales conclues par la Suisse en matière d'entraide judiciaire internationale avec les Etats étrangers (p.ex. avec le Canada et le Brésil) prévoient l'application de l'EIMP, dont les art. 18*a*, al. 4 et 80*b*. Lorsque l'autorité saisie de la demande d'entraide judiciaire est le ministère public d'un canton, l'art. 37, al. 1 LPD est applicable (voir ci-dessus). L'autorité saisie dans le cadre de l'exercice des droits considérés doit être en mesure, dans l'hypothèse où ces droits sont restreints et dans la mesure où cela est nécessaire, de répondre à la demande de manière à ne pas révéler des informations couvertes par le secret de fonction.

L'*al. 2* est applicable au droit d'accès aux données concernant des données collectées dans le cadre de la recherche de personnes disparues (art. 1, al. 1, let. c) ou condamnées (art. 1, al. 1, let. d). Ce sont les art. 8 et 9 LPD qui s'appliquent à ce droit lorsque l'autorité en charge du dossier est une autorité de la Confédération. Quant à l'art. 37, al. 1, LPD, il s'applique à titre subsidiaire au droit d'accès aux données collectées lors d'une surveillance – lorsque l'autorité en charge du dossier est une autorité d'un canton – si le droit cantonal n'assure pas un niveau de protection adéquat. L'art. 279 CPP s'applique en outre par analogie, en ce sens que la personne qui a fait l'objet d'une surveillance doit en être informée (par l'autorité qui a ordonné la surveillance) (voir aussi l'art. 37, al. 2 et le commentaire y relatif).

La réglementation prévue à l'*al. 3* reflète clairement – même si cela peut sembler évident – que ce n'est pas le service, uniquement détenteur des données, qui est le maître du fichier, mais, conformément à l'art. 13, les autorités ayant accès au système de traitement, en vertu de l'art. 9. Il va de soi que si la dernière autorité à avoir été en charge du dossier n'existe plus formellement (p.ex. en cas de fusion avec une autre autorité ou d'intégration dans celle-ci), c'est celle qui lui a succédé qui est compétente au sens de l'*al. 3*. Si une demande d'accès aux données est formulée auprès du service, celui-ci doit sans délai la transmettre à l'autorité compétente.

L'*al. 4* donne mandat au Conseil fédéral de régler l'exercice des droits en tenant compte des particularités techniques du système de traitement. Est en particulier visé le cas où la livraison – commandée par la procédure applicable, en particulier par l'art. 102, al. 3 CPP – de copies contenant les résultats de surveillances est problématique d'un point de vue technique, par exemple parce qu'elles portent sur une quantité de données très importante (voir aussi les explications introductives concernant le ch. 2.2). Les milieux concernés seront consultés sur les dispositions y relatives du Conseil fédéral.

32 RS **351.6**
33 RS **351.20**

Art. 11 Délai de conservation des données

L'art. 11 AP-LSCPT a aussi été contesté par bon nombre de participants à la procédure de consultation. Ceux-ci ont, en particulier, prétendu que la réglementation proposée, notamment le système d'annonce projeté, serait trop complexe et coûteux et générerait une charge administrative inutile. Il a en outre été soutenu que le délai de conservation devrait être fixé par les règles existantes du CPP, afin d'éviter d'avoir plusieurs réglementations concourantes. Le Conseil fédéral estime que ces critiques sont pour une part justifiées. Le présent projet propose par conséquent une réglementation plus simple, qui occasionne aux autorités, en particulier de poursuite pénale, une charge administrative réduite par rapport à ce que proposait l'art. 11 AP-LSCPT.

Le contenu de l'*al. 1*, lequel concerne les données collectées dans le cadre d'une procédure pénale (art. 1, al. 1, let. a), s'impose en somme comme une évidence. Le CPP ou les autres droits de la procédure pénale applicables, comme la PPM, contiennent en effet des dispositions adaptées pour la conservation des dossiers de la procédure. Il serait en outre contradictoire d'avoir plusieurs réglementations – une découlant du droit de la procédure pénale applicable et une autre spécifique contenue dans la LSCPT – susceptibles de s'appliquer. De fait, l'*al. 1* renvoie en particulier au régime découlant des art. 99, al. 2, 100 et 103, al. 1 CPP. Les données doivent être conservées au dossier (art. 100 CPP) – elles peuvent y être intégrées par un renvoi où elles sont stockées – et le dossier doit être conservé tant que le délai de prescription de l'action pénale et de la peine n'est pas atteint (art. 103, al. 1 CPP). Partant, les données personnelles doivent être conservées (au dossier) tant que ce délai de prescription n'a pas expiré (art. 99, al. 2 CPP).

La durée de conservation maximale des données dans le système de traitement, mentionnée à l'*al. 2* (art. 1, al. 1, let. b) se justifie en particulier par le fait que les procédures d'entraide judiciaire durent souvent longtemps. Cette durée correspond aux délais maximaux de prescription de l'action pénale et de la peine connus en droit suisse (si on fait abstraction des cas d'imprescriptibilité et de prolongation de la peine). Il sied de surcroît de noter que ces délais applicables dans un cas concret peuvent être supérieurs dans le droit de l'Etat requérant.

La durée de conservation maximale des données dans le système de traitement prévue à l'*al. 3* (art. 1, al. 1, let. c) se justifie en particulier par le fait que ce qui est en jeu est le bien juridique le plus précieux, à savoir la vie humaine, et par le fait qu'une personne peut être portée disparue pendant une très longue période.

Pour les mêmes raisons que celles mentionnées dans le commentaire de l'al. 1, le contenu de l'*al. 4*, *phr. 1* (art. 1, al. 1, let. d) s'impose en somme aussi de soi. L'*al. 4*, *phr. 1* renvoie en particulier au régime découlant des art. 99, al. 2, 100 et 103, al. 1 CPP (pour le surplus, voir le commentaire de l'al. 1). Quant à la durée de conservation maximale des données dans le système de traitement mentionnée à l'*al. 4*, *phr. 2* (art. 1, al. 1, let. d), elle se justifie notamment par le fait que ce qui est susceptible d'être en jeu est le bien juridique le plus précieux, à savoir la vie humaine, et par le fait qu'une personne peut ne pas pouvoir être localisée pendant une très longue période. Il faut relever qu'il n'y a pas de prescription de la sanction que constitue une mesure entraînant une privation de liberté, à la différence de ce qui est en principe le cas pour la sanction que constitue une peine privative de liberté. Lorsque les données ont été collectées lors de la recherche d'une personne condamnée à une peine privative de liberté et faisant l'objet d'une mesure entraînant une

privation de liberté, leur durée maximale de conservation est celle qui est la plus longue parmi celles applicables à ces deux cas de figure.

Aux termes de l'*al. 5*, il appartient à l'autorité en charge du dossier ou, s'il n'y en a plus, à la dernière à l'avoir été d'entreprendre les démarches nécessaires afin que les données conservées dans le système de traitement soient supprimées par le service à l'expiration des délais visés aux al. 1 à 4. Pour ce faire, cette autorité doit assurer sur le long terme un contrôle de ces délais. Ceci est bien entendu susceptible d'impliquer une augmentation des tâches administratives des autorités considérées; cette augmentation est toutefois admissible, car gérable au moyen d'une organisation appropriée de contrôle des délais. Cette solution est préférable à celle, proposée par l'art. 11, al. 5 AP-LSCPT, qui consisterait à confier au service la responsabilité de contrôler le respect des délais mentionnés aux al. 1 à 4 et d'informer – par le truchement d'une autorité centrale – l'autorité en charge du dossier ou la dernière à l'avoir été de l'échéance prochaine du délai. Cette autre solution nécessiterait en effet une charge administrative disproportionnée aussi bien pour le service que pour les autorités précitées. Ces différentes autorités devraient tout d'abord communiquer au service, pour chaque surveillance, le délai applicable visé aux al. 1 à 4. Cette communication serait indispensable, étant donné que ce délai varie en fonction du contenu du dossier (p.ex. la peine prévue pour l'infraction considérée détermine le délai de prescription de l'action pénale et la peine prononcée influe sur le délai de prescription de la peine) et étant donné que le service n'a pas accès au dossier. Il ne faut à cet égard pas perdre de vue que l'infraction en question ainsi que la peine prononcée et, par conséquent, le délai de conservation sont susceptibles de changer au fil des différentes instances; ceci ne rendrait le travail de contrôle des délais du service que plus lourd. Il est en outre logique que les démarches précitées doivent être entreprises par l'autorité en charge du dossier (ou la dernière à l'avoir été), et non par le service, étant donné que celle-ci est considérée comme étant le maître du fichier (voir art. 13). L'autorité en charge du dossier ou la dernière à l'avoir été informe également le service d'un éventuel transfert des données considérées devant être effectué afin de respecter le droit en vigueur, avant que ces données ne soient supprimées du système par le service. Est en particulier visé ici le respect des éventuelles dispositions fédérales et cantonales en matière d'archivage. En matière d'archivage, on applique les dispositions de la collectivité (Confédération ou cantons) dont relève l'autorité en charge du dossier (ou la dernière à l'avoir été), celle-ci étant le maître du fichier des données considérées (voir art. 13). Pour la portée de la notion d'«autorité en charge du dossier», voir le commentaire de l'art. 10, al. 3.

La tâche conférée au service de contacter l'autorité compétente trente ans après la fin de la surveillance pour s'informer du sort à réserver aux données encore contenues dans le système de traitement est en somme une mesure de précaution. Elle a, en effet, pour but de s'assurer que les données qui auraient dû être supprimées du système conformément aux al. 1 à 4, mais ne l'ont pas été (p.ex. l'autorité a oublié d'informer le service), le soient.

Dans l'exercice de la compétence que lui confère l'*al. 6*, le Conseil fédéral devra notamment tenir compte des particularités techniques du système de traitement. Il pourra par exemple prévoir que l'autorité de poursuite pénale puisse saisir le délai de conservation de tout ou partie des données considérées dans le système de traitement et prévoir que cette autorité devra contacter le service et lui donner des instructions un nombre de jours déterminé avant l'expiration du délai de conservation, de manière à lui laisser suffisamment de temps pour exécuter ces instructions. Le Conseil

fédéral pourra par exemple aussi prévoir que tout ou partie des données seront automatiquement effacées si l'autorité visée ne contacte pas le service en temps utile.

Art. 12 Sécurité

La réglementation prévue à l'*al. 1* se justifie du fait que le service – même s'il n'est pas maître du fichier (voir aussi commentaire de l'art. 13) – exploite le système de traitement dans lequel les données sont contenues; il est donc le détenteur des données.

Se fondant sur l'*al. 2*, le Conseil fédéral pourra notamment édicter des dispositions sur le contrôle de l'accès aux données et sur le fait de savoir quand celles-ci devront être cryptées (voir aussi art. 9 et commentaire y relatif). Les milieux concernés seront consultés sur les dispositions proposées par le Conseil fédéral en vertu de l'*al. 2*.

L'*al. 3* s'inspire de l'art. 9, al. 2 de l'OSCPT actuelle. Par sécurité des données au sens de cette disposition, on entend en particulier la confidentialité et l'intégrité de celles-ci.

Art. 13 Responsabilité

L'*art. 13* établit que ce sont les autorités qui ont accès au système de traitement qui sont à considérer comme maîtres du fichier, et non le service, qui n'est que le détenteur des données contenues dans le système de traitement et ne fait que mettre en œuvre les droits d'accès à celui-ci (voir aussi commentaire des art. 9 et 12).

Art. 14 Interface avec le réseau de systèmes d'information de police de l'Office fédéral de la police

L'*al. 1* constitue une base légale expresse prévoyant la copie et le transfert par voie électronique, en ligne, des données contenues dans le système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication exploité par le service, en particulier de celles collectées lors de cette surveillance, dans les systèmes d'information visés aux art. 10, 12 et 13 LSIP. Ceci, afin de permettre leur traitement dans lesdits systèmes. Pour que cette copie et ce transfert puissent avoir lieu, il est bien entendu nécessaire que la législation applicable à ces systèmes autorise le traitement des données considérées dans ceux-ci (*let. a*).

Seules les personnes en charge de la procédure concernée doivent pouvoir accéder aux données dans le système d'information considéré au sens de la LSIP (*let. b*). Cette dernière condition devrait en somme figurer dans la LSIP. Ladite intégration ne se laisse toutefois pas réaliser de manière satisfaisante, pour des raisons liées à la systématique législative. Une révision de la LSIP est toutefois envisagée; elle permettra de régler la question de l'accès aux données contenues dans le système d'information considéré au sens de la LSIP en l'insérant comme il se doit d'un point de vue systématique, à savoir dans la LSIP.

Les systèmes d'information précités sont exploités par fedpol et sont, en particulier, utilisés par celle-ci et les polices cantonales pour exploiter les informations collectées dans le cadre d'enquêtes pénales, qui comprennent les données collectées lors

de surveillances de la correspondance par télécommunication. La copie et le transfert électroniques présentent par rapport à la copie et au transfert «manuels» plusieurs avantages, dont des gains de temps et des gains financiers ainsi qu'une sécurité des données accrue (risque de perte des données réduit et risque d'erreur, affecaffectant la qualité des données, diminué). Les données contenues dans le système exploité par le service demeurent dans ce système après leur transfert dans le système d'information considéré au sens de la LSIP, raison pour laquelle on parle de copie.

Selon l'*al. 2*, la copie et le transfert des données visés à l'al. 1 seront déclenchés par un ordre donné par une personne habilitée à accéder aussi bien au système de traitement exploité par le service (art. 9) qu'au système d'information considéré au sens de la LSIP. En effet, le passage au mode de transfert électronique des données ne doit pas avoir pour conséquence d'éluder les règles applicables à l'accès à ces systèmes. Les autorités de poursuite pénale, et non le service, sont responsables de la légalité de la copie et du transfert des données du système de traitement exploité par le service dans le système d'information considéré au sens de la LSIP.

2.3 Section 3 Tâches du service

Les tâches du service sont liées à l'exécution des ordres de surveillance de la correspondance par poste et télécommunication. Le présent projet ne confère en revanche pas de compétences normatives et réglementaires au service pour l'exécution des surveillances, ces compétences étant du ressort du DFJP (art. 31, al. 3). Ce qui précède répond à l'exigence du ch. 1 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT), selon laquelle les tâches normatives et réglementaires du service doivent en substance être distinguées de ses tâches d'exécution des surveillances.

Art. 15 Renseignements sur les services de télécommunication

L'*art. 15* reprend pour l'essentiel en substance l'art. 14, al. 2 et 2bis de la LSCPT en vigueur, à l'exception du renvoi qui y est effectué (voir commentaire de l'art. 21). Toutefois, alors même que la notion de «raccordements (de télécommunication)» est comprise dans un sens large, il a été jugé opportun de remplacer cette notion dans le présent projet par celle de «services (de télécommunication)», étant donné que la notion de «raccordements (de télécommunication)» s'est révélée trop restrictive, avec l'évolution de la technique. Une personne n'obtient en effet d'un fournisseur qu'un service ou une application, sans pouvoir exiger de celui-ci un raccordement donné. Les services de télécommunication visés comprennent également les services concernant Internet (voir aussi commentaire de l'art. 1, al. 1).

L'*al. 1*, *let. a* est complétée, par rapport à l'al. 2, let. a de l'art. 14 de l'actuelle LSCPT. Contrairement à ce que peut laisser entendre le texte de cette dernière disposition – qui résulte probablement d'une inadvertance du législateur –, les renseignements considérés ne doivent bien évidemment pas seulement pouvoir être demandés dans le but de déterminer les services et les personnes à surveiller, afin de les mettre sous surveillance; il faut également pouvoir les requérir dans le but de

déterminer qui communique avec le service surveillé, ce même dans le cas où on ne souhaiterait pas également ordonner la surveillance du service de chacun de ces interlocuteurs[34]. Afin de mieux satisfaire aux exigences de la légalité, il est précisé que les données peuvent également être fournies à l'autorité (de poursuite pénale) désignée par l'autorité qui peut ordonner ou autoriser une surveillance, et non plus seulement à celle-ci. La police notamment pourra obtenir ces données vu qu'elle sera, en principe, chargée de les exploiter.

L'*al. 1*, *let. b* reprend la let. b de l'al. 2 de l'art. 14 de la LSCPT en vigueur. Cette disposition ne vise pas que les tâches de police en relation avec des procédures pénales mais également celles que la police assume en dehors de celles-ci[35]. Il importe ici de préciser que cette disposition implique qu'il n'est nullement besoin d'un ordre du ministère public pour que les instances policières citées dans ladite disposition obtiennent les renseignements en question, lesquels ne sont pas soumis au secret des télécommunications et dont l'obtention ne constitue pas une mesure de contrainte (voir le commentaire de l'art. 21). Ces instances policières peuvent, en particulier dans le cadre des art. 306 s. CPP, demander ces renseignements de leur propre chef au service et les obtenir de celui-ci.

L'*al. 1*, *let. c* correspond à l'art. 14, al. 2, let. c de la LSCPT en vigueur.

L'*al. 2, let. a* reprend en substance l'al. 2bis de l'art. 14 de l'actuelle LSCPT, en adaptant, comme conséquence au changement de structure du projet, le renvoi qui y est effectué.

L'art. 23 de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale (LCD)[36], en relation avec l'art. 10, al. 3 LCD, donne à la Confédération le droit de porter plainte contre un acte de concurrence déloyale si des intérêts collectifs sont concernés. En l'état actuel, la mise en œuvre de ce droit est très difficile en relation avec l'acte de concurrence déloyale, visé par l'art. 3, al. 1, let. u LCD, que constitue l'appel publicitaire non sollicité. En effet, au vu du fait que les entreprises publicitaires appelantes ou les centres d'appels changent apparemment souvent leur numéro d'appel, la Confédération a souvent affaire à des réclamations uniques concernant des numéros uniques. Ceci a pour conséquence que, en l'absence d'un intérêt collectif, la Confédération n'est pas légitimée à déposer plainte pénale, alors même que, dans de nombreux cas, on est susceptible d'avoir affaire à une seule et même entreprise qui utilise divers numéros d'appel. Les données que la Confédération peut désormais obtenir en vertu de l'al. *2, let. b* sont nécessaires pour lever les incertitudes quant à son droit de porter plainte dans les cas concrets où elle a affaire à des appels publicitaires non désirés et, partant, contribuent à lui permettre de lutter efficacement contre ceux-ci. L'autorité de la Confédération en principe compétente pour déposer plainte pénale au sens précité est le Secrétariat d'Etat à l'économie[37].

34 Thomas Hansjakob, op. cit. (note 11), n. 16 ad art. 14 LSCPT.
35 Thomas Hansjakob, op. cit. (note 11), n. 18 ad art. 14 LSCPT; cf. le message du 1er juillet 1998 relatif à la LSCPT en vigueur, FF **1998** 3727.
36 RS **241**
37 Voir art. 1, al 1 de l'ordonnance du 12 octobre 2011 concernant le droit de la Confédération d'intenter une action dans le cadre de la loi contre la concurrence déloyale (RS **241.3**)

Art. 16 Tâches générales dans le domaine de la surveillance

L'*art. 16* mentionne les tâches du service que l'on retrouve dans le domaine de la surveillance de la correspondance par poste et dans celui de la surveillance de la correspondance par télécommunication. Ces tâches sont reprises des art. 11 et 13 de l'actuelle LSCPT. Contrairement à celle-ci, le présent projet ne prévoit plus d'article relatif à des tâches spécifiques du service dans le domaine de la surveillance de la correspondance par poste, à la différence de ce qui est le cas pour la surveillance de la correspondance par télécommunication (voir commentaire de l'art. 17).

La *let. a*, qui s'inspire des art. 11, al. 1, let. a et 13, al. 1, let. a de la LSCPT en vigueur, concerne l'examen formel que fait le service de l'ordre de surveillance. Cette disposition vise en somme une tâche de coordination du service. Ce contrôle porte également sur le caractère complet et la clarté de l'ordre de surveillance[38]. Le service devra en particulier, comme c'est déjà le cas aujourd'hui, vérifier que l'infraction considérée figure dans le catalogue des infractions pouvant faire l'objet d'une surveillance. Pour permettre une éventuelle rectification dans les meilleurs délais de l'ordre de surveillance, le service doit pouvoir s'adresser directement à l'autorité qui a ordonné la surveillance (en plus de l'autorité habilitée à autoriser la surveillance, qui doit être informée de cette prise de contact en vue de sa future décision sur la décision ordonnée); ceci est particulièrement indiqué si le service estime que l'ordre de surveillance n'est pas clair par rapport à ce qui est demandé. Le Conseil fédéral pourra au besoin fixer dans une ordonnance le délai dans lequel le service devra contacter l'autorité susmentionnée. Nonobstant ce devoir d'aviser du service, il importe de préciser que la responsabilité de la validité de la décision de surveillance revient à l'autorité qui l'a ordonnée; ceci se justifie d'autant plus que cette autorité n'est pas tenue de suivre l'avis du service. Pour le surplus, voir par analogie le commentaire de la let. b.

La *let. b* prévoit un examen matériel, sous l'angle du droit administratif, de l'ordre de surveillance par le service. Cette disposition attribue en somme une tâche de coordination au service. Allant ainsi dans le sens de la demande formulée par un grand nombre de participants à la procédure de consultation, le présent projet renforce le pouvoir d'examen du service par rapport à ce qui était prévu dans l'AP-LSCPT concernant la surveillance de la correspondance par télécommunication. Cette disposition ne vise pas un examen matériel de l'ordre de surveillance par rapport aux dispositions de procédure pénale applicables, mentionnées aux art. 269 ss CPP ou 70 ss PPM, c'est-à-dire par rapport à des questions relevant purement de la procédure pénale. Partant, il n'appartient par exemple pas au service de déterminer si la surveillance ordonnée est susceptible de donner ou non des résultats exploitables intéressants pour une enquête pénale donnée. L'examen précité revient en effet exclusivement à l'autorité habilitée à autoriser la surveillance (voir également le commentaire de l'art. 42, al. 2).

La tâche du service mentionnée à la *let. b* a pour but d'éviter que le service ne doive, sans y avoir au préalable rendu attentives l'autorité qui a ordonné la surveillance et l'autorité habilitée à autoriser la surveillance, transmettre à une personne tombant dans le champ d'application de la loi un ordre de surveillance dont il estime qu'il remplit l'une des caractéristiques mentionnées dans cette disposition. Ce mécanisme sert en particulier à rendre l'autorité qui a ordonné la surveillance et l'autorité habili-

38 Thomas Hansjakob, op. cit. (note 11), n. 2 à 10 ad art. 11 LSCPT.

tée à l'autoriser davantage conscientes des problèmes liés à un tel ordre de surveillance. L'autorité ayant ordonné la surveillance et l'autorité habilitée à l'autoriser pourront tenir compte de cet avis pour, le cas échéant, révoquer la surveillance ordonnée ou ne pas l'autoriser. Elles ne sont toutefois pas obligées de tenir compte de l'avis du service. Les tenants de l'introduction d'une voie de droit (procédure d'opposition ou de recours) pour régler les éventuelles divergences d'opinion entre le service et l'autorité qui a ordonné la surveillance considèrent que ce mécanisme de contrôle (devoir d'avis du service) n'est pas suffisant. Ils affirment en particulier que l'expérience a montré que ces divergences ne peuvent pas toutes être résolues par la voie du dialogue. Ils estiment également qu'il ne serait pas logique que le service ait un pouvoir de cognition limité concernant la décision de surveillance, alors que l'autorité de recours saisie, par exemple, par un fournisseur de services de télécommunication mécontent d'une décision ne connaîtrait pas cette limitation. Nonobstant ce qui précède, on considère que le mécanisme de contrôle proposé (devoir d'avis du service) est nécessaire et suffisant pour, notamment, éviter les complications inutiles qui découleraient d'un recours, formé, par exemple, par un fournisseur de services de télécommunication contre la décision du service de faire exécuter une surveillance présentant une caractéristique énumérée à la *let. b*. Il n'est en revanche pas nécessaire de créer une voie de droit, même dépourvue d'effet suspensif, pour régler les éventuelles divergences d'opinion entre le service et l'autorité qui a ordonné la surveillance. Il ne faut pas perdre de vue que le service est en somme une autorité d'exécution, une interface entre les autorités de poursuite pénale et les fournisseurs de services de télécommunication, de sorte qu'une telle voie de recours serait en soi contraire au système. Il importe de noter que le service a pleine compétence pour examiner l'ordre de surveillance, qui fonde sa décision de surveillance destinée à un fournisseur de services de télécommunication, sous l'angle du droit administratif et pour le cas échéant le compléter. Le service ne dispose donc pas d'un «pouvoir de cognition» limité par rapport à celui du Tribunal administratif fédéral. De plus, il y a lieu de préciser que le dialogue entre le service et les autorités de poursuite pénale découlant nécessairement de la *let. b* permet une sorte de reconsidération légale des ordres de surveillance. Il faut voir aussi dans ce contexte les progrès qu'apportera le nouvel instrument que constitue l'organe consultatif, prévu à l'art. 5. Les autorités de poursuite pénale pourront dans ce cadre en particulier être informées de ce qui est techniquement possible et le service pourra plus précisément saisir l'utilité des surveillances ordonnées. L'ordre de surveillance transmis au service fera en outre l'objet d'un contrôle d'une autorité judiciaire, soit le tribunal des mesures de contrainte (art. 274 CPP), auquel le service doit d'ailleurs, aux termes de la let. b, transmettre sa position. Cette autorité indépendante peut fort bien décider de ne pas autoriser la surveillance ordonnée, pour des raisons relevant de la procédure pénale, auquel cas les informations recueillies seront en principe détruites et ne pourront pas être exploitées (art. 277 CPP). Introduire une voie de droit pour régler les éventuelles divergences d'opinion entre le service et l'autorité qui a ordonné la surveillance se justifierait d'autant moins que les fournisseurs de services de télécommunication auront désormais la possibilité de se défendre, dans le cadre de l'art. 42, al. 2, devant le Tribunal administratif fédéral contre les décisions de surveillance transmises par le service. Outre le service, l'autorité qui a ordonné la surveillance pourra être invitée par le Tribunal administratif fédéral à s'expliquer sur son ordre de surveillance. Un tel recours peut aboutir à ce que l'ordre de surveillance rendu par une autorité de poursuite pénale ne doive pas être exécuté par le fournisseur de services de télécommunication considéré lui-même (pour les

détails, voir le commentaire de l'art. 42). Rappelons, enfin, que la responsabilité de la validité de la décision de surveillance revient, nonobstant le devoir d'aviser qui incombe au service, à l'autorité qui l'a ordonnée; ceci se justifie d'autant plus que cette autorité n'est pas tenue de suivre l'avis du service.

Sont considérés comme inappropriés au sens de la *let. b* les ordres de surveillance qui, de par les caractéristiques techniques liées au cas d'espèce, ne sont pas en mesure d'apporter des résultats exploitables. Le fait de savoir si une surveillance est couverte par un type de surveillance prévu par la loi se détermine en particulier en fonction de la LSCPT, de l'OSCPT et du CPP. Il y a lieu de préciser que le critère que doit prendre en compte le service pour déterminer si l'exécution de la surveillance est techniquement possible n'est pas le fait de savoir si la personne qui doit exécuter la décision possède les possibilités techniques pour ce faire mais l'état de la technique existant au moment où la surveillance devrait être exécutée. Si la personne précitée n'est pas en mesure de s'exécuter, le service pourra exécuter lui-même la surveillance ou la confier à un tiers (voir art. 34, al. 1 et commentaire y relatif).

Le délai mentionné à la *let. b* dans lequel le service devra informer l'autorité qui a ordonné la surveillance et l'autorité habilitée à autoriser la surveillance doit bien évidemment être particulièrement court, notamment pour permettre à l'autorité ayant ordonné cette surveillance d'en ordonner, cas échéant, rapidement une autre. Le Conseil fédéral pourra au besoin fixer ce délai.

La tâche du service mentionnée à la *let. c* est à lire en relation avec les art. 20 et 24. On vise donc ici, contrairement à ce qui est le cas de l'art. 26, al. 2, des informations à obtenir avant d'ordonner une surveillance.

La *let. d* reprend en substance les art. 11, al. 1, let. b et 13, al. 1, let. b de l'actuelle LSCPT. Cette disposition présente une certaine analogie avec l'art. 33, al. 5, lequel ne s'inscrit toutefois pas dans une procédure d'exécution d'une surveillance mais dans une procédure de preuve de la disponibilité à renseigner et à surveiller, y compris suite à une surveillance qui ne s'est pas déroulée de manière optimale. Quant à la mention de la tâche de contrôle de l'exécution de la surveillance par le service, elle ne fait que souligner le rôle d'intermédiaire que joue celui-ci entre les autorités de poursuite pénale et les fournisseurs de services de télécommunication.

La *let. e* reprend en substance l'art. 13, al. 1, let. f de l'actuelle LSCPT, applicable à la surveillance de la correspondance par télécommunication. Cette tâche est étendue à la surveillance de la correspondance par poste, étant donné qu'elle a également tout son sens dans ce domaine. Cette disposition est à mettre en relation avec les art. 271 et 274, al. 4, let. a, CPP et les art. 70*b* et 70*e*, al. 4, let. a, PPM. Ces articles mentionnent le régime applicable à la surveillance considérée, lorsqu'il s'agit de protéger un secret professionnel, dont l'autorité de poursuite pénale ne doit pas avoir connaissance (voir commentaire des art. 271 CPP et 70*b* PPM). Le service prend les dispositions nécessaires permettant la mise en œuvre des mesures décidées dans le cadre des articles précités; mais il ne procède pas lui-même au tri dont il est fait mention dans ces articles (art. 271, al. 1 CPP et art. 70*b*, al. 1 PPM).

La *let. f* s'inspire des art. 11, al. 1, let. d et 13, al. 1, let. g de l'actuelle LSCPT. Le service doit désormais obtenir un écrit, c'est-à-dire une copie de la demande de prolongation.

La *let. g* reprend les art. 11, al. 1, let. c et 13, al. 1, let. h de l'actuelle LSCPT.

La *let. h* reprend les art. 11, al. 1, let. g et 13, al. 1, let. k de l'actuelle LSCPT.

La *let. i* répond à une nécessité vu la complexité du système considéré.

La *let. j* reprend en substance les art. 11, al. 2, phr. 1 et 13, al. 2, let. e de l'actuelle LSCPT et les complète en mentionnant les conseils opérationnels.

Les tâches mentionnées à l'al. 2, let. a à d de l'art. 13 de l'actuelle LSCPT ne sont pas reprises dans l'*art. 16*. Elles ne correspondent en effet plus à des tâches qui doivent être effectuées sur demande par le service ou à des tâches que l'on doit encore attendre de celui-ci, soit par manque de moyen, soit parce que cela n'est plus nécessaire.

Art. 17 Tâches dans le domaine de la surveillance de la correspondance par télécommunication

L'*art. 17* énonce les tâches du service propres aux surveillances ordonnées dans le domaine de la correspondance par télécommunication, à l'exclusion de la correspondance par poste. Cet article est aussi applicable aux surveillances exécutées par des fournisseurs de services de communication dérivés, si le Conseil fédéral fait usage de la compétence que lui attribue l'art. 27, al. 3 (voir art. 27, al. 3 et commentaire y relatif).

La *let. a* s'inspire de l'art. 15, al. 2, phr. 1 de l'actuelle LSCPT. L'expression «numéro d'appel» pourrait en somme être remplacée par la notion de «raccordement», dès lors qu'elle ne convient pas également dans le contexte de la correspondance par Internet. Au vu de l'évolution technique, il est toutefois plus opportun de remplacer cette notion par celle de «services» (voir commentaire de l'art. 15 *in initio*). Demeure cependant le principe en vigueur qui veut que la surveillance soit confiée au fournisseur de services de télécommunication qui est préposé à la gestion du service considéré. La *let. a* suppose bien entendu que le service soit en mesure de déterminer à quel fournisseur de services de télécommunication l'exécution technique de la surveillance occasionne la moins grande charge, ce qui n'est pas toujours possible. Le service prend à cet égard en considération l'ordre de l'autorité qui a ordonné la surveillance pour confier l'exécution de celle-ci. La consigne de l'autorité sur ce point ne lie toutefois pas le service: En principe, l'autorité qui ordonne la surveillance ne doit pas se prononcer de manière contraignante sur ces aspects. En vertu de sa fonction et de ses tâches, le service est compétent – éventuellement après avoir pris langue avec l'autorité qui a ordonné la surveillance (voir art. 16, let. a, ch. 3 et let. b) – pour déterminer quel est le fournisseur approprié. Au préalable, le service devra donner à ladite autorité les informations qu'il pourra obtenir pour lui permettre d'ordonner la surveillance (art. 16, let. c).

La *let. b* s'inspire de l'art. 13, al. 1, let. c de l'actuelle LSCPT. Elle l'adapte au fonctionnement du nouveau système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication, lequel ne prévoit en principe plus la mise à la disposition de ces données aux autorités concernées au moyen d'envois postaux de supports de données et de documents mais au moyen d'un droit d'accès à ce système (voir art. 6 ss). Afin de satisfaire aux exigences de la légalité, il est en outre précisé dans la disposition, en s'inspirant par analogie du contenu des art. 15, al. 1, let. b et 23, let. b de l'actuelle OSCPT, que le service permet également la consultation des communications considérées à l'autorité (de poursuite pénale) désignée par l'autorité qui a ordonné la surveillance, et non plus seulement à celle-ci. La police notamment pourra prendre connaissance des données vu qu'elle sera, en principe, chargée de les exploiter.

La *let. c* modifie et complète le texte de l'art. 13. al. 1, let. d de l'actuelle LSCPT, qui règle la modalité particulière et exceptionnelle d'exécution d'une surveillance que constitue le branchement direct. Les données obtenues dans le cadre d'une surveillance ordonnée passent en principe par le service, en tant qu'interface entre les fournisseurs de services de télécommunication chargés d'exécuter les surveillances ordonnées et les autorités ayant ordonné celles-ci, et sont enregistrées dans le système exploité par le service. Ceci vaut également lorsque la surveillance ordonnée est une surveillance dite en temps réel, c'est-à-dire qui n'est pas une surveillance rétroactive. Lorsque l'exécution de la surveillance ordonnée a lieu sous la forme d'un branchement direct, les données provenant du fournisseur de services de télécommunication sont transférées par celui-ci directement à l'autorité concernée, sans passer par le service, ce qui exclut l'enregistrement de ces données dans le système exploité par celui-ci. L'autorité en question enregistre donc elle-même ces données. La *let. c* définit les conditions dans lesquelles la modalité du branchement direct peut être utilisée dans le cadre d'une surveillance. Les cas dans lesquels il est possible de recourir au branchement direct correspondent à des situations dans lesquelles le service n'est, pour des raisons techniques, pas en mesure de jouer le rôle d'interface entre les fournisseurs de services de télécommunication et les autorités concernées. L'art. 271, al. 2 CPP et l'art. 70*b*, al. 2 PPM, dans sa version découlant du CPP, sont réservés. Ce recours restrictif au branchement direct ne diminuera pas l'efficacité du travail des autorités de poursuite pénale, en ce sens qu'il ne retardera pas leur travail: les données obtenues dans le cadre d'une surveillance en temps réel qui n'a pas lieu par branchement direct sont mises à la disposition des autorités concernées de suite, avec quelques fractions de seconde de retard seulement, par le biais du système exploité par le service. Afin de mieux satisfaire aux exigences de la légalité, il est précisé dans la disposition, en s'inspirant par analogie du contenu des art. 15, al. 1, let. b et 23, let. b de l'actuelle OSCPT, que les communications considérées peuvent également directement être transmises à l'autorité (de poursuite pénale) désignée par l'autorité qui a ordonné la surveillance, et non plus seulement à celle-ci. Ces communications pourront ainsi en particulier directement être transmises à la police, qui est en principe chargée de l'exploitation des communications obtenues.

La *let. d* s'inspire de l'art. 13, al. 1, let. e de la LSCPT en vigueur. La notion de données secondaires y est adaptée par rapport à celle qui est contenue dans cette disposition. Le commentaire de l'art. 26, al. 1, let. b, expose les raisons et la portée de ces changements. La *let. d* adapte le texte de l'art. 13, al. 1, let. e de la LSCPT en vigueur au fonctionnement du nouveau système informatique de traitement des données relatives à la surveillance de la correspondance par télécommunication, lequel ne prévoit en principe plus la mise à la disposition de ces données aux autorités concernées au moyen d'envois postaux de supports de données et de documents mais au moyen d'un droit d'accès à ce système (voir art. 6 ss). Afin de mieux satisfaire aux exigences de la légalité, il est en outre précisé dans la disposition, en s'inspirant par analogie du contenu des art. 15, al. 1, let. b et 23, let. b de l'actuelle OSCPT, que le service permet la consultation des données considérées également à l'autorité (de poursuite pénale) désignée par l'autorité qui a ordonné la surveillance, et non plus seulement à celle-ci. La police notamment pourra prendre connaissance des données vu qu'elle sera, en principe, chargée de les exploiter.

La tâche visée à la *let. e* est le corollaire des mesures devant être prises par le service mentionnées aux articles cités dans cette disposition.

La *let. f* renvoie aux art. 32 à 34.

Le tri prévu à la *let. g* – qui se distingue de celui faisant l'objet de l'art. 271 CPP et 70*b* PPM en relation avec la protection du secret professionnel – ne peut être effectué que sur demande de l'autorité qui a ordonné la surveillance. Le service n'est en mesure d'effectuer qu'un tri automatisé, les autres types de tris étant très compliqués, voir impossibles à réaliser. Si un tri permettant d'isoler certains types de données composant un flux de données doit avoir lieu, il doit, à la différence de ce que prévoyait l'avant-projet, en principe être effectué par le service. Il est plus délicat de confier cette tâche à quelqu'un d'autre, en particulier aux fournisseurs de services de télécommunication, ce ne serait-ce que pour des questions de responsabilité quant à l'intégrité des données. Parmi le flux de données en question, il s'agit, par exemple, de séparer les données relatives à la TV de celles concernant le trafic e-mail. Une telle demande de l'autorité qui a ordonné la surveillance n'interviendra en principe que si elle ne souhaite pas pouvoir consulter plus de données ou dans la mesure où cela est techniquement nécessaire pour pouvoir exploiter correctement les données désirées faisant partie du flux en question, dès lors que la quantité de données composant un flux de données peut être telle qu'elle rend celles-ci très difficilement exploitables, voire inexploitables. Dans un souci de transparence nécessaire à une appréciation objective des preuves, le dossier judiciaire devra, cas échéant, faire mention du fait que les données au dossier ne constituent qu'une partie du flux des données considéré.

Art. 18 Contrôle de qualité

L'*art. 18* vise, comme les art. 32 à 34, à garantir une bonne exécution des surveillances ordonnées.

L'*al. 1* a pour objectif de permettre au service de prendre les mesures de contrôle pour remédier à un problème de qualité qui aurait été constaté, par l'autorité de poursuite pénale ou par lui-même, en relation avec les données livrées par les fournisseurs de services de télécommunication. Un tel problème se pose, par exemple, lorsque l'autorité de poursuite pénale constate que les données secondaires obtenues lors d'une surveillance rétroactive révèlent des communications qui ne figurent pas sur les enregistrements des conversations obtenus lors d'une surveillance en temps réel. L'objectif de cette disposition est aussi de permettre au service d'anticiper ces situations, en effectuant des contrôles à titre préventif, afin de vérifier qu'aucun problème n'est susceptible de venir affecter le bon fonctionnement des surveillances. Il va de soi, sur la base de l'art. 3, al. 3, voire de l'art. 5, que le service doit informer l'autorité de poursuite pénale concernée des éventuels problèmes relatifs à la qualité des données; celles-ci sont en effet susceptibles d'être déterminantes pour une procédure.

Si, pour effectuer les contrôles précités, le service doit prendre connaissance du contenu des données livrées par les fournisseurs de services de télécommunication – ce qui est le cas lorsqu'il effectue un contrôle de données concernant une surveillance réelle, c'est-à-dire portant sur une «cible» et des données réelles –, il doit au préalable, en vertu de l'*al. 2*, pour des motifs tenant à la protection des données, en obtenir l'autorisation de l'autorité qui a ordonné la surveillance ou qui est subséquemment en charge du dossier. Le service ne peut, en effet, prendre connaissance du contenu des données, même si celles-ci sont en sa possession, puisqu'enregistrées dans le système qu'il exploite. Une telle autorisation n'est en revanche pas néces-

saire si le service effectue un contrôle ne nécessitant pas de devoir prendre connaissance des données considérées, comme c'est le cas lors d'une surveillance fictive dans le cadre d'un contrôle préventif, c'est-à-dire portant sur une «cible» test (fictive) et des données fictives.

2.4 Section 4 Obligations dans le domaine de la surveillance de la correspondance par poste

Art. 19 Obligations des fournisseurs de services postaux

L'*art. 19* remplace l'art. 12 de la LSCPT en vigueur.

L'*al. 1* reprend pour l'essentiel l'art. 12, al. 1 de l'actuelle LSCPT. Les envois postaux et données secondaires postales doivent directement être livrés à l'autorité qui a ordonné la surveillance (ou à l'autorité désignée par celle-ci), et non au service, contrairement à ce qui vaut en principe pour les données devant être fournies dans le cadre d'une surveillance de la correspondance par télécommunication (voir art. 26, al. 1). L'*al. 1* mentionne deux grands types de surveillances, quant aux données concernées, qui existent déjà dans le système de la LSCPT en vigueur, à savoir la surveillance portant sur le contenu de la correspondance par poste (données de contenu) (let. a) et celle portant sur des données secondaires de la correspondance (let. b), qui ne permettent pas de connaître le contenu de la correspondance considérée. La définition des données secondaires postales est modifiée par rapport à la notion en vigueur, qui énumère inutilement certaines catégories de données, mais ne change rien au contenu matériel de la notion. Ce changement de définition a pour corollaire ceux opérés à l'art. 273, al. 1 CPP et 70*d*, al. 1 PPM. Afin de satisfaire aux exigences de la légalité, il est précisé à l'al. 1, en s'inspirant par analogie du contenu de l'art. 11, let. b de l'actuelle OSCPT, que les correspondances et données considérées peuvent également être fournies à l'autorité (de poursuite pénale) désignée par l'autorité qui a ordonné la surveillance, et non plus seulement à celle-ci. La police notamment pourra obtenir les données et les correspondances vu qu'elle sera, en principe, chargée de les exploiter. L'obligation des fournisseurs de services postaux de livrer des renseignements supplémentaires, telle qu'elle est prévue à l'art. 12, al. 1 de la LSCPT en vigueur, est supprimée. En effet, ces renseignements, qui ne dépendent pas de connaissances des fournisseurs de services postaux mais de personnes déterminées, comme le facteur, doivent pouvoir être obtenus par un canal normal, c'est-à-dire par le biais d'une audition de la personne considérée en qualité de témoin[39]. Il importe de préciser – ce qui va de soi – que, pour pouvoir satisfaire à leur obligation de fournir les données considérées, les personnes visées doivent disposer desdites données, ce qui suppose qu'elles doivent conserver les données secondaires. Il n'est pas prévu d'enregistrer les données collectées lors d'une surveillance de la correspondance postale dans le système de traitement du service.

L'*al. 2* mentionne simplement deux autres grands types de surveillances, quant au moment où elles sont exécutées, qui existent déjà dans le système actuel: la surveillance en temps réel et la surveillance rétroactive, telles qu'elles sont définies aux ch. 3 et 4 de l'annexe de l'OSCPT.

39 Thomas Hansjakob, op. cit. (note 11), n. 4 ad art. 12 LSCPT.

L'*al. 3* constitue une norme de délégation au Conseil fédéral, lui attribuant la compétence de préciser des points qu'il règle aujourd'hui dans l'OSCPT. Le Conseil fédéral n'impose actuellement que l'obligation de conserver ou de fournir les données secondaires qui sont disponibles; de telles données existent par exemple en cas d'envois postaux avec justificatif de distribution, à la différence de ce qui est le cas lors de l'envoi simple d'une lettre. Il importe ici de préciser que, contrairement à ce qui est le cas pour les fournisseurs de services de télécommunication (voir art. 26, al. 6 et commentaire y relatif), le projet ne prévoit pas la possibilité de dispenser certaines catégories de fournisseurs de services postaux de certaines de leurs obligations légales. Ceci se justifie en particulier par le fait que ces obligations, qui sont citées à l'al. 1, ne sont techniquement pas complexes à remplir (bien moins que celles des fournisseurs de services de télécommunication), que ce ne sont que les types de données secondaires mentionnées ci-dessus qui doivent être livrées par les fournisseurs de services postaux et que ces données ne concernent pas tous les envois postaux. Cette obligation de conservation ne concerne donc pas tous les fournisseurs de services postaux. Afin de déterminer le régime applicable à la surveillance de la correspondance, il y a lieu de déterminer, pour chaque service nouvellement développé, comme les services de poste électronique, si le service en question constitue un service postal ou un service de télécommunication. Une adaptation des dispositions d'exécution peut être nécessaire pour les services d'un genre nouveau présentant des caractéristiques aussi bien postales que de télécommunication.

L'*al. 4*, qui s'inspire de l'art. 12, al. 2 de l'actuelle LSCPT, concerne la durée de conservation des données secondaires dans le domaine de la correspondance par poste. Cette obligation signifie que les fournisseurs de services postaux doivent, à l'instar de ce qui est le cas dans la LSCPT en vigueur, conserver, en «réserve» pour d'éventuelles futures instructions pénales, les données secondaires de toutes les correspondances. Il appartient au Conseil fédéral de désigner ces données secondaires, en application de la compétence que lui octroie l'al. 3. Cette réglementation est nécessaire afin que les fournisseurs précités soient en mesure de satisfaire à l'obligation qui leur incombe en vertu de l'al. 1, let. b dans le cas d'une surveillance rétroactive, étant entendu que les données visées par cette disposition sont absolument indispensables pour lutter contre la criminalité. L'allongement de six mois à douze mois, à compter de la date de la correspondance, de la durée de conservation des données secondaires dans le domaine de la correspondance par poste est notamment à mettre en relation avec la motion Schweiger 06.3170 (Cybercriminalité. Protection des enfants), laquelle demande, entre autres, un allongement égal de la durée de conservation des données secondaires dans le domaine de la correspondance par télécommunication, y compris par Internet (voir commentaire de l'art. 26, al. 5). La problématique soulevée dans la motion, à savoir la perte de données importantes pour des enquêtes pénales, se pose en effet non seulement pour les données secondaires dans le domaine de la correspondance par télécommunication mais également dans celui de la correspondance par poste. Il est donc logique que l'augmentation de la durée de conservation s'applique également aux données secondaires postales. Pour le surplus, nous renvoyons par analogie au commentaire de l'art. 26, al. 5. Le Conseil fédéral estime que le surplus de travail administratif pour les fournisseurs de services postaux lié à l'augmentation de la durée de conservation de données secondaires est acceptable, ce d'autant plus que ceux-ci doivent aujourd'hui déjà conserver de telles données, que cette conservation n'est techniquement pas complexe à effectuer et que ce ne sont que des types limités de données

appartenant à cette catégorie que ces fournisseurs doivent conserver (voir commentaire de l'al. 3). Il n'y a donc pas de raison valable de prévoir une durée de conservation différente (plus courte) pour les données secondaires postales.

Le fait que des correspondances postales fassent l'objet d'une surveillance n'implique pas nécessairement que la personne surveillée ne puisse pas les obtenir. L'*al. 5* s'inscrit dans cette idée. Toutefois, le fournisseur de services postaux considéré ne peut récupérer ces correspondances et les lui livrer qu'après avoir obtenu l'accord de l'autorité qui a ordonné la surveillance ou qui est subséquemment en charge du dossier. Il est évident que celle-ci pourra refuser son accord si les correspondances doivent, par exemple, être séquestrées en vue de leur confiscation ou pour servir de moyens de preuve. Il va également de soi que le fournisseur de services postaux ne pourra pas, sous peine de contrevenir à l'art. 39, al. 1, let. d, divulguer à la personne surveillée le fait que les correspondances postales récupérées qu'il lui remet ont fait l'objet d'une surveillance. Une telle communication aura le cas échéant lieu dans le cadre et aux conditions de l'art. 279 CPP.

Art. 20 Informations préalables à un ordre de surveillance

L'*art. 20* vise des informations à obtenir avant d'ordonner une surveillance. De telles informations peuvent en particulier être utiles lorsqu'on envisage d'ordonner une surveillance spéciale, c'est-à-dire présentant certaines particularités par rapport aux surveillances habituellement ordonnées.

2.5 Section 5 Renseignements relatifs à la surveillance de la correspondance par télécommunication

Un groupe important de participants, issus de la quasi-totalité des différents cercles consultés, a demandé lors de la procédure de consultation que les obligations de collaborer soient précisées, parce qu'elles ne sont pas suffisamment claires dans la loi en vigueur et dans l'AP-LSCPT. Pour les détails, voir le rapport de consultation[40].

Le Conseil fédéral estime également que les diverses obligations de collaborer et de tolérer doivent être clarifiées. Cette clarification a lieu aux art. 21 à 25 (section 5: Renseignements relatifs à la surveillance de la correspondance par télécommunication), aux art. 26 à 30 (section 6: Obligations dans le domaine de la surveillance de la correspondance par télécommunication) et aux art. 31 à 34 (section 7: Garantie de la disponibilité des fournisseurs de services de télécommunication à renseigner et à surveiller). L'étendue de l'obligation de collaborer y est définie de manière échelonnée en fonction de l'activité spécifique considérée.

Il n'y a en revanche pas lieu de régler ces obligations dans le détail dans la loi; les détails y relatifs doivent en effet être réglés par le Conseil fédéral dans une ordonnance (OSCPT). Cette flexibilité est d'autant plus importante que la frontière entre les fournisseurs de services de télécommunication classiques (p.ex. Swisscom) et le phénomène plutôt nouveau des fournisseurs de services de communication dérivés

40 www.admin.ch/ch/f/gg/pc/documents/1719/Rapport_C_surveillance_correspondance_par_poste_et_telecommunication.pdf

(p.ex. Google) s'estompe de plus en plus. Partant, le Conseil fédéral doit obtenir la compétence de soumettre les fournisseurs de services de communication dérivés offrant des services d'une grande importance économique ou à un grand nombre d'utilisateurs à toutes ou à certaines des obligations incombant aux fournisseurs de services de télécommunication (pour les détails, voir le commentaire de l'art. 27, al. 3). En conséquence, le Conseil fédéral doit aussi obtenir la compétence de dispenser des fournisseurs de services de télécommunication de certaines obligations légales, en particulier ceux qui offrent des services de télécommunication de faible importance économique ou dans le domaine de l'éducation (pour les détails, voir le commentaire de l'art. 26, al. 6).

Art. 21 Renseignements sur les services de télécommunication

L'*art. 21* reprend l'essentiel de l'art. 14, al. 2 à 4 de la LSCPTen vigueur et le complète. La notion de «services (de télécommunication)» remplace désormais celle de «raccordements (de télécommunication)», celle-ci s'étant révélée trop restrictive, avec l'évolution technique (voir commentaire de l'art. 15). Les fournisseurs d'accès à Internet sont également obligés par cette disposition (voir commentaire de l'art. 2, let. b) et les services de télécommunication visés concernent également Internet (voir commentaire de l'art. 1, al. 1). Alors que l'obligation d'enregistrement des fournisseurs de services de télécommunication vise aujourd'hui, dans le domaine de la téléphonie mobile, les cartes SIM à prépaiement, elle visera également, dans le domaine d'Internet, les cartes «wireless» (d'accès sans fil) à prépaiement et les autres moyens semblables. Cette extension est exigée par la motion Glanzmann-Hunkeler 07.3627 (Enregistrement des cartes d'accès sans fil à prépaiement), qui demande en substance, à l'instar de ce qui est le cas pour les cartes SIM à prépaiement, d'enregistrer les données permettant d'identifier les usagers de ces moyens, en particulier dans le but d'empêcher le téléchargement anonyme sur Internet d'images ou de vidéos à caractère pédophile. Cette obligation visera en outre les moyens permettant l'accès à un réseau de téléphonie fixe.

Les renseignements mentionnés à l'*art. 21* ne sont pas couverts par le secret des télécommunications, à la différence du contenu des communications et des données secondaires; ces renseignements peuvent donc être communiqués dans le cadre d'une procédure simplifiée[41], comme cela est le cas selon la LSCPT en vigueur, et leur obtention ne constitue pas une mesure de contrainte. Leur communication n'a donc pas à avoir lieu dans le cadre d'une procédure soumise aux conditions restrictives de l'art. 269 CPP, en particulier à la liste des infractions mentionnée à l'al. 2 de l'article précité[42], et n'est pas subordonnée à l'autorisation de l'autorité habilitée à autoriser une surveillance (art. 274 CPP). Ces renseignements sont très importants pour l'avancement des investigations[43], lesquelles sont susceptibles, au vu de leurs résultats, de permettre d'ordonner une surveillance aux conditions strictes de l'art. 269 CPP. Pour pouvoir satisfaire à l'obligation de fournir les renseignements et indications visés à l'*art. 21*, les personnes considérées doivent évidemment disposer des renseignements et indications en question, ce qui suppose qu'elles doivent les conserver. Les personnes auxquelles les renseignements doivent être fournis sont mentionnées à l'art. 15. Il importe de préciser que, en vertu de l'art. 15, al. 1, let. a et

41 Cf. le message du 1er juillet 1998 relatif à la LSCPT en vigueur, FF **1998** 3726.
42 Thomas Hansjakob, op. cit. (note 11), n. 1 à 4 et 23 ad art. 14 LSCPT.
43 Cf. le message du 1er juillet 1998 relatif à la LSCPT en vigueur, FF **1998** 3726.

b, les renseignements visés pourront être directement fournis à la police, sans que le ministère public ne doive rendre un ordre dans le cas de l'art. 15, al. 1, let. b (pour les détails, voir le commentaire de ces dispositions).

Les renseignements faisant l'objet de l'*al. 1*, let. a à d doivent également être fournis par les fournisseurs de services de télécommunication lorsque leurs clients n'ont pas souscrit à un abonnement (voir al. 2); si leurs clients n'ont pas souscrit à un abonnement, les données mentionnées à l'al. 1, let. e doivent en outre être saisies. Les modalités relatives à la saisie des données visées à l'art. 21, al. 1, let. a sont réglées par le Conseil fédéral (pour le détail, voir le commentaire de l'art. 23). Les fournisseurs de services de télécommunication sont ainsi en mesure de rendre accessibles les renseignements visés à *l'al. 1* au moyen du système de commutation des demandes de renseignements sur les services de télécommunication (actuellement nommé CCIS) exploité par le service en collaboration avec eux. Pour les obligations correspondantes des revendeurs de moyens tels que les cartes à prépaiement, nous renvoyons à l'art. 30.

L'*al. 1, let. a* reprend l'art. 14, al. 1, let. a de la LSCPT en vigueur, en y ajoutant le prénom et la date de naissance. Ce sont des éléments d'identification classiques, également pour les autorités et aux fins mentionnées à l'art. 15.

L'*al. 1, let. b* reprend en substance l'art. 14, al. 1, let. b de la LSCPT en vigueur. Etant donné que l'art. 3, let. f, LTC contient l'expression «paramètres de communication» et que celle-ci est définie à l'art. 3, let. g de la loi précitée, le renvoi de la let. b est, pour des raisons de clarté, complété en conséquence.

L'*al. 1, let. c* s'inspire de l'art. 14, al. 1, let. c de l'actuelle LSCPT, en utilisant toutefois la forme plurielle. Lorsque l'on souhaite surveiller une personne, il est en effet utile de connaître l'ensemble des types de services (p.ex. téléphone fixe, mobile et Internet) dont elle dispose. Cela permet de déterminer en connaissance de cause quel type de service doit faire l'objet de la surveillance et d'éviter de devoir interroger les fournisseurs de services de télécommunication autant de fois que la personne visée possède de services de télécommunication.

La norme de délégation prévue à l'*al. 1, let. d* donne la compétence au Conseil fédéral d'obliger les fournisseurs de services de télécommunication à livrer au service d'autres types de renseignements utiles sur les services de télécommunication, comme la date d'activation du service, le statut du service (p.ex. actif, bloqué ou résilié), le numéro PUK, les numéros SIM, IMEI et IMSI, les factures, les modalités de paiement de celles-ci et les contrats. Cette norme lui permet aussi de les obliger à fournir d'autres données utiles que celles visées à la let. a, qui permettent également d'identifier des personnes, par exemple les photocopies de documents d'identité. Le Conseil fédéral pourra prescrire par exemple que l'enregistrement ne peut avoir lieu que sur présentation d'un passeport ou d'une carte d'identité valable ou d'un autre document de voyage reconnu pour entrer ou demeurer en Suisse, que le type et le numéro de la pièce d'identité soient saisis ou qu'une copie soit faite de la pièce présentée. Certains de ces renseignements supplémentaires figurent déjà dans les directives du service et peuvent par conséquent être obtenus aujourd'hui par les autorités de poursuite pénale. Il est donc fort probable que le Conseil fédéral reprenne au moins ces renseignements dans une ordonnance. Les milieux concernés seront consultés sur les dispositions proposées par le Conseil fédéral en vertu de l'*al. 1, let. d*. En vertu de l'art. 15, al. 1, let. a et b, si le Conseil fédéral le prévoit (voir al. 5), les renseignements visés pourront être directement fournis à la police –

sans que le ministère public ne doive rendre un ordre dans le cas de l'art. 15, al. 1, let. b – par le biais d'un système de commutation des demandes de renseignements sur les services de télécommunication (appelé CCIS). Il n'est pas nécessaire de prévoir le traitement de ces données dans une loi au sens formel (art. 17 LPD), comme la LSCPT, étant donné qu'elles ne constituent pas des données personnelles sensibles, au sens de l'art. 3, let. c LPD. Le présent projet ne contient pas de disposition énumérant ces types de renseignements parce que sa densité serait trop importante pour s'insérer dans une loi. L'énumération de ces renseignements a en revanche sa place dans une ordonnance.

L'*al. 1, let. e* prévoit l'obligation des fournisseurs de services de télécommunication de mentionner les nom et prénom de la personne qui a remis, à titre onéreux ou non, le moyen permettant l'accès aux services (cartes SIM à prépaiement ou autres moyens semblables, cartes «wireless» à prépaiement ou autres moyens semblables et les moyens permettant l'accès à un réseau de téléphonie fixe) et quel est le point de remise de celui-ci. Cette obligation est en particulier nécessaire pour que l'on sache à qui incombe un éventuel manquement commis dans l'exécution de l'enregistrement des données faisant l'objet de l'al. 1, let. a à d. Concernant les obligations correspondantes des revendeurs de tels moyens, voir l'art. 27.

L'*al. 2* règle l'obligation de saisir et de maintenir à disposition les données mentionnées à l'al. 1; le fait de savoir si les clients des fournisseurs de services de télécommunication ont ou non souscrit à un abonnement ne joue aucun rôle. L'*al. 2* reprend en partie l'art. 15, al. 5bis de l'actuelle LSCPT et l'adapte. Il étend l'obligation qu'ont les fournisseurs de services de télécommunication de fournir les renseignements requis. Alors que cette obligation vise aujourd'hui, dans le domaine de la téléphonie mobile, les cartes SIM à prépaiement et autres moyens semblables, elle visera également, dans le domaine d'Internet, les cartes «wireless» (d'accès sans fil) à prépaiement et autres moyens semblables. Cette extension est liée à ce que demande la motion 07.3627 Glanzmann-Hunkeler. Seront, de manière logique, désormais également visés les moyens permettant l'accès à un réseau de téléphonie fixe indépendamment de la souscription d'un abonnement. Il est en effet nécessaire de disposer des renseignements considérés relatifs à une relation commerciale avec un client n'ayant pas souscrit d'abonnement. Ceci s'est révélé dans le cadre de la lutte contre le terrorisme, en relation avec les cartes SIM à prépaiement. La LSCPT en vigueur prévoit un délai de deux ans après l'ouverture d'une relation commerciale durant lequel les renseignements en question doivent pouvoir être fournis. Ce délai de deux ans avait été retenu en fonction du fait que, au moment de l'entrée en vigueur de l'art. 15, al. 5bis de la LSCPT actuelle, soit au 1er août 2004, on avait décidé que ce serait aller trop loin que de prévoir l'enregistrement rétroactif des cartes SIM à prépaiement achetées avant le 1er août 2002[44]. Or désormais on n'a plus affaire à un enregistrement rétroactif, ce qui justifie la suppression de ce délai. Cette suppression appelle la création d'une disposition transitoire applicable aux cartes SIM à prépaiement et autres moyens semblables (art. 45, al. 4). Précisons en outre que l'obligation de renseigner ne porte que sur les renseignements saisis lors de l'enregistrement qui doit avoir lieu avant la remise par un fournisseur de services de télécommunication de cartes SIM à prépaiement (ou d'autres moyens semblables), de cartes «wireless» à prépaiement (ou d'autres moyens semblables) ou de moyens permettant l'accès à un réseau de téléphonie fixe au moment de l'ouverture d'une

44 Thomas Hansjakob, op. cit. (note 11), n. 22 ad art. 15 LSCPT.

relation commerciale, et non sur les données concernant des personnes qui pourraient acquérir ces mêmes moyens par la suite. Autrement dit, un fournisseur de services de télécommunication ne doit être en mesure de fournir que les renseignements qu'il a exigés lors de la remise d'un moyen, à l'exclusion des données concernant la personnne qui pourrait acquérir ce moyen par la suite. Tout autre régime impliquerait des formalités et un travail administratif excessifs (voir aussi commentaire de l'art. 6*a* LTC).

Il y a lieu de noter que l'*al. 2* ne limite pas la portée de l'art. 22.

La violation des obligations d'enregistrement est sanctionnée par l'art. 39, al. 1, let. c.

Art. 22 Renseignements visant à identifier les auteurs d'infractions sur Internet

L'*art. 22* reprend pour l'essentiel l'art. 14, al. 4 de la LSCPT en vigueur et prévoit un devoir de collaboration des fournisseurs de services de télécommunication, qui doivent faire tout leur possible pour permettre cette identification. Cet article n'a toutefois pas pour conséquence l'obligation pour les fournisseurs de services de télécommunication de livrer le nom de la personne qui utilise effectivement un ordinateur, dès lors qu'ils n'ont aucun contrôle sur cela; en revanche, ils devront, par exemple, – dans la mesure où le Conseil fédéral leur en donne l'obligation – livrer le nom de la personne à qui l'adresse IP considérée a été attribuée. Comme cela est le cas en vertu de la LSCPT en vigueur, la communication des renseignements visés à l'*art. 22* peut avoir lieu par une voie simplifiée (voir commentaire relatif à l'art. 21).

L'art. 22 concerne l'identification des auteurs d'infractions sur Internet; l'*al. 1* vise toutes les données qui permettent une telle identification[45]. Dans un objectif d'identification, des données secondaires comme l'attribution d'une adresse IP dynamique (c'est-à-dire qui n'est pas attribuée à l'avance), peuvent aussi être obtenues par la voie simplifié[46]. Pour des raisons de cohérence avec le rôle d'interface du service, il est mentionné que les indications visées doivent être fournies au service, et non pas, comme dans le droit actuel, à l'autorité compétente[47].

A la différence de l'art. 14, al. 4 de la LSCPT actuelle, qui est formulé de manière large, l'*al. 2* contient une norme de délégation qui donne expressément mandat au Conseil fédéral de mentionner, sur le modèle de l'art. 27 de l'actuelle OSCPT, les données que les fournisseurs de services de télécommunication doivent fournir. Les milieux concernés seront consultés sur les propositions que fera le Conseil fédéral en vertu de l'*al. 2*.

Les personnes visées à l'art. 2, let. c et d détiennent également des indications susceptibles d'être utiles dans le contexte visé par l'*art. 22*. L'*al. 3* exige toutefois, comme corollaire de ce que prévoient les art. 27, al. 2 et 28, al. 2, qu'elles ne fournissent que les indications à leur disposition (au moins celles disponibles au moment où la demande leur est faite).

45 Thomas Hansjakob, op. cit. (note 11), n. 25 ad art. 14 LSCPT.
46 Thomas Hansjakob, op. cit. (note 11), n. 26 ad art. 14 LSCPT.
47 Thomas Hansjakob, op. cit. (note 11), n. 24 ad art. 14 LSCPT.

Le Conseil fédéral peut cependant se rendre compte que cette réglementation n'est pas suffisante pour permettre une identification efficace des auteurs d'actes punissables commis par Internet. C'est pourquoi la norme de délégation faisant l'objet de l'*al. 4* lui permet d'obliger, comme corollaire de l'art. 27, al. 3, à des conditions restrictives (voir, par analogie, commentaire de l'art. 27, al. 3), les personnes visées à l'art. 2, let. c de fournir des indications supplémentaires, sur le modèle de celles que les fournisseurs de services de télécommunication doivent fournir.

Art. 23 Modalités relatives à la saisie des données et octroi des renseignements

Aux termes de l'*al. 1*, les modalités d'enregistrement des données visées aux art. 21, al. 1, let. a et 22, al. 2, phr. 1 seront déterminées par le Conseil fédéral. Celui-ci pourra prévoir par exemple que cet enregistrement ne pourra avoir lieu que sur présentation d'un passeport ou d'une carte d'identité valable ou d'un autre document de voyage reconnu pour entrer ou demeurer en Suisse, que le type et le numéro de la pièce d'identité devront être saisis et qu'une copie de la pièce présentée devra en outre être effectuée.

L'*al. 2* reprend l'art. 14, al. 3, phr. 1 de la LSCPT en vigueur.

Sous l'empire de la LSCPT en vigueur, le Conseil fédéral avait choisi de rendre des données mentionnées à l'art. 21, al. 1 accessibles aux autorités mentionnées à l'art. 15 par une consultation en ligne, au moyen d'un système de commutation des demandes de renseignements sur les raccordements de télécommunication (appelé CCIS), mis sur pied et exploité par le service, en collaboration avec les fournisseurs de services de télécommunication (art. 19 ss de l'actuelle OSCPT). Les renseignements qui ne peuvent être obtenus de la sorte le sont par une demande (en principe par fax) adressée au service, qui la transfère ensuite aux fournisseurs de services de télécommunication. Le Conseil fédéral n'avait donc pas choisi de permettre aux autorités mentionnées à l'art. 15 d'accéder directement aux répertoires existants et non accessibles au public. L'*al. 3* permet au Conseil fédéral de modifier le système actuel. S'il le juge souhaitable, il pourra par exemple prévoir que toutes les données faisant l'objet des art. 21 et 22 devront être rendues accessibles par un accès en ligne au système de commutation des demandes de renseignements sur les services de télécommunication. Rappelons que les instances policières citées à l'art. 15, al. 1, let. b pourront de leur propre chef demander auprès du service et obtenir de celui-ci les renseignements visés aux art. 21 et 22, sans qu'un ordre du ministère public soit nécessaire pour ce faire (pour les détails, voir le commentaire de l'art. 15, al. 1, let. b).

Art. 24 Informations préalables à un ordre de surveillance

L'art. 24 vise, à la différence de ce qui est le cas de l'art. 26, al. 2, des informations à obtenir avant d'ordonner une surveillance. De telles informations (p. ex. position d'une antenne de téléphonie mobile) peuvent en particulier être utiles lorsqu'on envisage d'ordonner une surveillance spéciale, c'est-à-dire présentant certaines particularités par rapport aux surveillances habituellement ordonnées.

Art. 25 Information sur les services

L'*art. 25* vise, tout comme les art. 32 à 34, à garantir que les surveillances ordonnées puissent être exécutées correctement, notamment à éviter des lacunes dans la surveillance. Il s'agit en particulier de permettre au service d'anticiper les difficultés qui pourraient survenir dans le cadre de surveillances futures, et non de se contenter de réagir suite à des problèmes qui auraient eu lieu lors de l'exécution de ces surveillances. Il importe de préciser que l'*art. 25* prévoit uniquement d'informer le service sur la nature et les caractéristiques des services considérés et non, en plus, sur les caractéristiques de la technologie sur laquelle les services considérés se fondent. Il n'est pas nécessaire, en effet, de connaître les caractéristiques de cette technologie, l'important étant que les surveillances ordonnées puissent être exécutées de manière conforme à ce que les art. 18 et 32 à 34 sont censés permettre. Dans les faits, les fournisseurs de services de télécommunication devront, à la demande du service, expliquer à celui-ci quels sont les services considérés et en quoi ils consistent, c'est-à-dire ce qu'ils permettent de faire. Ceci, indépendamment du fait de savoir si le service en question a été développé par une autre personne que le fournisseur de services de télécommunication et s'il fait appel à une technologie qui a été développée par un tiers. L'organe consultatif faisant l'objet de l'art. 5 constitue un cadre susceptible de favoriser l'obtention par le service des informations précitées. Il apparaît que l'on peut donc renoncer à prévoir l'obligation des fournisseurs de services de télécommunication d'informer spontanément le service, sans avoir au préalable été abordés par celui-ci.

Il est possible que des collaborateurs du service aient de la sorte connaissance de secrets d'affaires de ces fournisseurs de services de télécommunication. Ces collaborateurs sont toutefois soumis au secret de fonction et si l'un d'entre eux devait révéler de tels secrets il se rendrait coupable de violation du secret de fonction (art. 320 CP).

Le délai de six mois mentionné à l'*art. 25* vise à éviter que les fournisseurs de services de télécommunication ne doivent fournir les informations visées à un stade où ils sont susceptibles de ne pas encore être au clair sur le fait de savoir s'il vont mettre sur le marché le service considéré. Ceci, même si les fournisseurs de services de télécommunication planifient en principe 12 mois à l'avance leur budget et souhaitent en principe un délai transitoire de 12 mois lors de l'introduction d'un nouveau système de surveillance. Le délai de six mois vise donc à éviter de donner du travail superflu non seulement aux fournisseurs de services de télécommunication mais aussi au service. Selon les cas, le service aura besoin de plus de temps pour entreprendre toutes les démarches nécessaires afin de rendre possible une exécution correcte des surveillances. Nonobstant ce qui précède, un délai plus long que six mois n'a pas été retenu, car cela irait trop loin pour les fournisseurs de services de télécommunication. Dans l'intervalle, il faudra donc tolérer le risque que l'on ne puisse pas effectuer une surveillance. Il importe de noter que la réglementation proposée n'empêche bien entendu pas les fournisseurs de services de télécommunication de changer et d'adapter leur planification concernant les services qu'ils souhaitent à l'avenir mettre sur le marché; un autre régime reviendrait à limiter la possibilité de ces entreprises de s'affirmer sur le marché des télécommunications, qui est en constante mutation.

2.6 Section 6 Obligations dans le domaine de la surveillance de la correspondance par télécommunication

Concernant les remarques générales relatives aux obligations de renseignement et de surveillance et relatives aux résultats de la procédure de consultation, nous renvoyons aux explications introductives concernant la section 5.

Art. 26 Obligations des fournisseurs de services de télécommunication

L'*art. 26* remplace l'art. 15 de la LSCPT en vigueur concernant les obligations des fournisseurs de services de télécommunication. Il répond en particulier au vœu légitime exprimé lors de la procédure de consultation de préciser les obligations de collaborer, notamment des fournisseurs de services de télécommunication, ces obligations n'étant pas jugées suffisamment claires dans la loi en vigueur et dans l'AP-LSCPT. Pour les détails, voir le rapport de consultation[48]. Le présent projet supprime en outre les tâches spécifiques confiées aux fournisseurs de services de télécommunication dans l'AP-LSCPT en relation avec le recours à des Government Software (GovWare), dès lors qu'il apparaît, après une analyse plus approfondie, qu'une aide ou un concours particulier des fournisseurs de services de télécommunication n'est pas nécessaire pour permettre aux autorités de poursuite pénale de recourir à des GovWare (voir aussi commentaire de l'art. 280, let. d CPP).

L'*al. 1* mentionne deux grands types de surveillances, quant aux données concernées, lesquels existent déjà dans la LSCPT en vigueur. Il s'agit de la surveillance portant sur le contenu de la correspondance par télécommunication émise et reçue (données de contenu) (*let. a*) et de celle portant uniquement sur des données secondaires de la correspondance (*let. b*), qui ne permettent pas de connaître le contenu de la correspondance considérée. Comme cela ressort de l'art. 8, let. b, la définition des données secondaires de télécommunication est simplifiée par rapport à celle en vigueur sans que cela ne change le contenu matériel de la notion. Ainsi, la mention «données relatives au trafic et à la facturation» est supprimée, puisque la catégorie de données en question est couverte par la nouvelle définition des données secondaires. Les expressions «personne surveillée» et «données indiquant avec qui» visent en somme, plus que des personnes, le service (p.ex. le raccordement) utilisé par celles-ci. En effet, ce que l'on surveille, en fin de compte, c'est par exemple le raccordement de la personne surveillée (qui peut d'ailleurs être un inconnu), lequel peut être en communication avec un autre raccordement, attribué à une personne donnée, qui n'est pas forcément celle qui a utilisé ou utilise cet autre raccordement au moment considéré. Le changement de définition des données secondaires entraîne une modification des art. 273, al. 1, CPP et 70*d*, al. 1, PPM. L'*al. 1* couvre bien entendu les données concernant les accès à Internet, dès lors que l'accès à Internet est un mode de correspondance par télécommunication (voir commentaire de l'art. 1, al. 1). La formulation de l'*al. 1* permet en particulier de saisir le contenu d'un SMS (*let. a*), les données secondaires d'un SMS (*let. b*), tout comme les simples tentatives d'établissement d'une correspondance (p.ex. cas où la personne que cherche à atteindre la personne surveillée ne décroche pas) (*let. b*). Il va de soi que, pour pouvoir satisfaire à leur obligation de fournir les données considérées, les personnes

48 www.admin.ch/ch/f/gg/pc/documents/1719/Rapport_C_surveillance_correspondance_par_poste_et_telecommunication.pdf

visées doivent disposer desdites données, ce qui suppose qu'elles doivent conserver les données secondaires. Pour plus d'explications en relation avec la notion de données secondaires, voir le commentaire de l'al. 5. Le renvoi à l'art. 17 let. c ne fait que rappeler le fait que, dans le cas d'une surveillance exécutée par branchement direct, les données collectées sont, exceptionnellement, directement transmises à l'autorité qui a ordonné la surveillance ou à l'autorité (en principe de poursuite pénale) désignée par celle-ci, et non pas d'abord au service, qui joue en principe le rôle d'intermédiaire. Il appartiendra au Conseil fédéral de déterminer dans quel délai on peut exiger des fournisseurs de services de télécommunication l'obtention des données. Les fournisseurs de services de télécommunication doivent fournir les données demandées par l'autorité qui a ordonné la surveillance. Si celle-ci le souhaite, ils doivent donc, pour autant que cela puisse dans le cas concret raisonnablement être exigé de leur part, effectuer un tri permettant d'isoler certains types de données composant le flux de données considéré pour ne fournir que le type de données souhaitées (p.ex. données Internet, à l'exclusion de la TV par Internet). Pour le surplus, voir aussi le commentaire de l'art. 17, let. f.

L'*al. 2* reprend des obligations existantes dans la LSCPT actuelle (art. 15, al. 1, phr. 2 et al. 4, phr. 2) nécessaires pour l'exécution de la surveillance. On vise ici, à la différence de ce qui est le cas de l'art. 24, les informations nécessaires lorsqu'une surveillance a déjà été ordonnée. Constituent en particulier des informations visées par cette disposition celles relatives à la technique de communication dont il est fait usage et aux appareils de particuliers utilisés[49]. L'*al. 2* vise à combler dans une certaine mesure la lacune dans la surveillance créée par l'al. 6, en imposant aux personnes visées l'obligation minimale de tolérer une surveillance ainsi que des obligations accessoires nécessaires pour permettre l'exécution de celle-ci. S'inspirant en partie de la réglementation contenue dans la LSCPT actuelle en relation avec la surveillance au sein d'un réseau de télécommunication interne ou d'un central domestique, il est prévu que ce soit le service ou une personne mandatée par celui-ci, en particulier la police, qui exécute la surveillance considérée. Ceci ne signifie pas que le service peut transférer des tâches administratives à des privés, au sens de l'art. 178, al. 3 de la Constitution (Cst.)[50]. Le service demeure en effet responsable de l'exécution de la tâche déléguée. Concernant l'obligation de dépôt, portant sur des données secondaires, des fournisseurs dispensés en vertu de l'al. 6, voir le commentaire relatif à celui-ci.

L'*al. 3*, qui est à lire en relation avec l'art. 17, let. a, reprend aussi une obligation existante dans la LSCPT actuelle (art. 15, al. 2, phr. 2) et nécessaire pour l'exécution de la surveillance. A la demande de l'autorité qui a ordonné la surveillance relayée par le service, la possibilité est également prévue de fournir les données directement au service, ce, en particulier, pour des raisons de confidentialité.

L'*al. 4* mentionne quant à lui deux autres – par rapport à l'al. 1 – grands types de surveillances, quant au moment où elles sont exécutées, lesquels existent déjà dans le système de la LSCPT en vigueur: la surveillance en temps réel et la surveillance rétroactive, telles qu'elles sont définies aux ch. 3 et 4 de l'annexe de l'actuelle OSCPT. Les données pouvant être obtenues dans le cadre d'une surveillance rétroactive sont des données secondaires dénommées dans le langage technique «données retenues» («retained data»).

49 Thomas Hansjakob, op. cit. (note 11), n. 5 ad art. 15 LSCPT.
50 RS **101**

L'obligation visée à l'*al. 5* signifie que les fournisseurs de services de télécommunication doivent, à l'instar de ce qui est le cas aujourd'hui (art. 15, al. 3), conserver, en «réserve» pour d'éventuelles futures enquêtes pénales, les données secondaires de toutes les communications. Il appartient au Conseil fédéral de désigner ces données secondaires, en application de la compétence que lui octroie l'art. 31. Ceci implique évidemment que devront être conservées les données concernant les communications de toutes les personnes à l'encontre desquelles aucune instruction n'est et ne sera ouverte pendant la durée de conservation des données, étant précisé que ces personnes représentent l'énorme majorité de la population. Cette réglementation est toutefois nécessaire afin que les fournisseurs de services de télécommunication soient en mesure de satisfaire à l'obligation qui leur incombe en vertu de l'al. 1, let. b dans le cadre d'une surveillance rétroactive, sachant que les données visées par cette disposition sont absolument indispensables pour lutter contre la criminalité. Ces données, à la différence de celles visées à l'al. 1, let. a (données dites de contenu), ne fournissent au demeurant pas d'information sur le contenu de la communication. Il importe en outre de préciser que lesdites données ne peuvent être obtenues que dans le respect des art. 269 ss CPP, c'est-à-dire, en particulier, qu'avec l'autorisation de l'autorité compétente pour autoriser les surveillances ordonnées (tribunal des mesures de contrainte) dans le cadre d'une procédure pénale, et non à titre préventif. Ceci constitue une forte garantie légale permettant de protéger toute personne concernée contre d'éventuels abus. La personne concernée pourra de plus interjeter recours contre la surveillance ordonnée (art. 279 CPP). Notons que les fournisseurs de services de télécommunication conservent aujourd'hui déjà tout ou partie des données en question pendant au moins un an, en particulier pour des raisons commerciales et liées à la facturation.

L'*al. 5* indique la durée de conservation des données secondaires de télécommunication, qui passe de six à douze mois à compter de la date de la correspondance. Cet allongement est exigé par le ch. 2 de la motion Schweiger 06.3170 (Cybercriminalité. Protection des enfants) et la motion Barthassat 10.4133 (Relever la durée de conservation des journaux d'attribution d'adresses IP). Les raisons qui justifient l'augmentation de six à douze mois de la durée de conservation des données précitées, qui comprennent celles permettant de connaître l'attribution des adresses IP, visées par la motion Barthassat 10.4133, tiennent à l'efficacité de la poursuite pénale, notamment dans les domaines de la lutte contre la pédopornographie, le crime organisé et le terrorisme. En effet, il ressort des expériences acquises par les autorités de poursuite pénale que la durée pendant laquelle les données secondaires doivent actuellement être conservées, soit six mois, est trop courte, puisque ce délai est souvent, totalement ou en grande partie, échu lorsque l'autorité est en mesure, au vu de l'avancement de la procédure considérée, d'ordonner une surveillance. Ceci peut en particulier avoir pour conséquence qu'il n'est pas possible de donner suite à une demande d'entraide judiciaire internationale ou d'identifier un prévenu ou, pire encore, une victime, par exemple un enfant victime d'actes pédophiles. Eu égard aux intérêts publics en jeu, il y a lieu de considérer l'extension de six à douze mois de la durée de conservation des données est compatible avec les droits fondamentaux des personnes dont les données sont conservées. Le Conseil fédéral a déjà soutenu cette position dans son rapport du 9 juin 2006 donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats 05.3006 (Lutter plus efficacement contre le terrorisme et le crime organisé)[51]. Cette durée est

51 www.admin.ch/ch/f/ff/2006/5421.pdf

en particulier à considérer en relation avec la directive de l'Union européenne 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006. Cette directive autorise, pour les données correspondant aux données secondaires en Suisse, une durée de conservation de six mois au minimum à, en principe, deux ans au maximum à compter de la date de la communication[52]. L'augmentation de la durée de conservation en question a obtenu un soutien important dans le cadre de la procédure de consultation. Elle est toutefois remise en question en particulier par les milieux des fournisseurs de services de télécommunication. Ceux-ci invoquent des coûts supplémentaires. De l'avis du Conseil fédéral, l'extension de la durée de conservation telle qu'elle est proposée n'engendrera pas de surcoûts disproportionnés pour les personnes qui devront satisfaire à cette obligation de conservation. Rappelons, en outre, que les fournisseurs de services de télécommunication conservent déjà aujourd'hui tout ou partie des données considérées pendant au moins un an. Quant à l'allongement de six à douze mois de la période durant laquelle les données secondaires peuvent être demandées rétroactivement (art. 273, al. 3 CPP et art. 70*d*, al. 3 PPM), il est le corollaire de l'allongement de la durée de conservation de ces données et découle du même constat et du même souci d'efficacité.

L'*al. 6* prévoit la possibilité pour le Conseil fédéral de dispenser certaines personnes répondant à la définition de fournisseur de services de télécommunication de certaines obligations impliquant une préparation active de leur part (par opposition à la simple obligation de tolérer une surveillance ou de livrer des données disponibles), en fonction de certaines caractéristiques. Ces caractéristiques donnent à penser, par exemple, que ces personnes ne seront *a priori* pas en possession de données intéressantes pour une surveillance de la correspondance par télécommunication. Ce peut être le cas des personnes qui offrent des services de télécommunication dans le domaine de l'éducation ou à un nombre de clients très réduits. De fait, cette possibilité de dispense se rapproche de ce que prévoit le système en vigueur, étant donné que ne tombent dans le champ d'application à raison des personnes et n'ont par conséquent des obligations en vertu de la LSCPT en vigueur que les fournisseurs de services de télécommunication soumis à concession ou à l'obligation d'annoncer (art. 1, al. 2 de la LSCPT en vigueur, en relation avec art. 4, al. 2 LTC et 3 OST). L'*al. 6* impose à ces personnes l'obligation de livrer les données secondaires dont elles disposent, sans toutefois – à la différence de ce qui est la règle (voir al. 5) – les contraindre à conserver ces données. Ces personnes ont toutefois l'obligation minimale de tolérer une surveillance ainsi que des obligations accessoires nécessaires pour permettre l'exécution de celle-ci (voir al. 2). Force est toutefois de constater que ces obligations ne permettent pas de combler entièrement la lacune créée par l'*al. 6*. Le régime proposé est en effet susceptible d'impliquer la perte de données secondaires pouvant normalement être obtenues dans le cadre d'une surveillance rétroactive et la perte de données normalement obtenues dans le cadre d'une surveillance en temps réel, étant donné que le temps de réaction pour initier la surveillance est augmenté, le service ou la personne mandatée par celui-ci ayant besoin de temps pour ce faire.

Il importe de signaler que le présent projet propose – en dépit de ce que demande la motion Glanzmann-Hunkeler 07.3627 (Enregistrement des cartes d'accès sans fil à prépaiement) et du fait que l'on tolère ainsi une lacune dans la surveillance – de

52 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:FR:PDF

renoncer à prescrire aux fournisseurs de services de télécommunication une obligation d'identification des usagers (et non pas seulement des ordinateurs de ceux-ci) d'un réseau fourni par leur soin à une personne qui le laisse à la disposition de ces usagers. Pour le surplus, voir le commentaire de l'art. 29.

Art. 27 Obligations des fournisseurs de services de communication dérivés

Il faut préciser d'emblée que l'*art. 27* ne saurait susciter trop d'attentes, étant donné que beaucoup de fournisseurs importants de services Internet ont leur siège et leur infrastructure à l'étranger. Pour le surplus, voir le commentaire de l'art. 2, let. c.

L'*al. 1* impose aux fournisseurs visés l'obligation minimale de tolérer une surveillance ainsi que des obligations accessoires nécessaires pour permettre l'exécution de celle-ci. La surveillance concerne des données que la personne surveillée envoie par le truchement d'un tel fournisseur (p.ex. dans le cas de services e-mail) ou enregistre chez celui-ci (p.ex. dans le cas de services de cloud storage). Il est prévu que ce soit le service ou une personne mandatée par celui-ci, en particulier la police, qui exécutera la surveillance considérée. Ceci ne signifie pas que le service pourra transférer des tâches administratives à des privés, au sens de l'art.178, al. 3, Cst. Le service demeure en effet responsable de l'exécution de la tâche.

L'*al. 2* impose à ces personnes l'obligation de livrer les données secondaires dont elles disposent (au moins celles disponibles au moment où la décision de surveillance est rendue), sans toutefois – à la différence de ce qui vaut en principe pour les fournisseurs de services de télécommunication (art. 26, al. 5) – les contraindre à conserver ces données. Ce régime est susceptible d'entraîner – par rapport à la réglementation normale applicable aux fournisseurs de services de télécommunication – la perte de données secondaires pouvant être obtenues dans le cadre d'une surveillance rétroactive et la perte de données obtenues dans le cadre d'une surveillance en temps réel, étant donné que le temps de réaction pour initier la surveillance est augmenté, le service ou la personne mandatée par celui-ci ayant besoin de temps pour entrer en action.

Le dépôt de données secondaires correspond en principe à une surveillance rétroactive et constitue un cas particulier du séquestre procédural (art. 263 ss CPP); en effet, à la différence d'une surveillance en temps réel, on séquestre dans ce cas auprès d'un fournisseur des données de télécommunication déjà existantes concernant une personne surveillée. Un tel dépôt constitue un cas spécial, étant donné que ces données font partie du contenu de la communication: Afin que l'information interceptée (en temps réel) puisse être attribuée correctement matériellement et juridiquement, de plus amples informations sont nécessaires, comme des données secondaires (combien de fois la personne a consulté un site Internet déterminé, à quels moments, etc.). Il n'est pas seulement important de savoir ce qu'a dit une personne, mais aussi quand et à qui. De par leur nature, ces informations sont en possession des fournisseurs de services considérés, raison pour laquelle ceux-ci peuvent être obligés – suivant leur type (voir art. 2) – de les conserver ou de les fournir dans la mesure où elles sont disponibles; d'autres informations encore doivent être fournies si elles sont nécessaires à la poursuite pénale.

Cette obligation de dépôt ne constitue pas quelque chose de nouveau, mais se trouve déjà dans les règles de procédure pénale classiques (art. 263 ss CPP). Compte tenu du lien de connexité étroit qui lie ces données et le contenu d'une communication, du fait que lesdites données sont obtenues des fournisseurs visés à l'art. 2 et du fait

que ceux-ci ont en partie une obligation de conserver les données secondaires, il est matériellement juste de régler dans la LSCPT – donc au moyen d'une base légale prévue dans la législation spéciale – ce mode particulier de séquestre (p.ex. art. 21, 22, 27, al. 2, 28, al. 2, etc.).

Les explications qui précèdent valent de manière générale pour le dépôt de données secondaires (voir art. 8, let. b, art. 19, al. 1, let. b et art. 26, al. 1, let. b); elles valent par exemple également pour les renseignements visant à identifier les auteurs d'infractions sur Internet, qui pourraient par exemple être obtenus chez un fournisseur de services «cloud» (voir art. 22). Le fait de régler ces obligations de dépôt spéciales dans la LSCPT présente en outre d'un point de vue juridique l'avantage de poser des exigences supérieures à la poursuite pénale pour obtenir les informations désirées: un ordre de séquestre (c'est-à-dire un ordre de surveillance) doit impérativement faire l'objet d'une autorisation du tribunal des mesures de contrainte (art. 269 en relation avec l'art. 272 CPP), ce qui renforce la protection juridique du prévenu. Dans le cas d'un séquestre classique au sens de l'art. 263 CPP, cela n'est pas nécessaire et le tribunal (des mesures de contrainte) n'intervient que dans le cadre d'une mise sous scellés (ou d'une demande de levée des scellés [voir art. 248 CPP])[53].

Le Conseil fédéral peut se rendre compte que la réglementation prévue aux al. 1 et 2 n'est pas suffisante pour permettre une surveillance adéquate. C'est pourquoi l'*al. 3* lui permet de conférer aux personnes visées des obligations supplémentaires par rapport à celles prévues dans la disposition précitée, sur le modèle de celles que les fournisseurs de services de télécommunication doivent en principe respecter. Le Conseil fédéral pourra de la sorte prescrire à ces personnes des obligations impliquant une préparation active de leur part, par opposition aux simples obligations mentionnées aux al. 1 et 2. Dans un contexte aussi technique et en constante évolution, on ne peut pas instaurer une norme de délégation sensée avec un degré de précision plus grand. Cette norme contient en outre des critères restrictifs qui peuvent être concrétisés. Elle est donc admissible. Elle se justifie en particulier par le fait qu'elle vise un domaine technique qui évolue très vite, notamment pour ce qui a trait aux acteurs en présence et aux services proposés. Ceci nécessite de pouvoir adapter la législation rapidement, en fonction des nouveaux besoins en matière de surveillance. La notion de nécessité contenue dans cette norme fait référence à des situations qui se sont répétées ou qui vont se répéter, dans lesquelles les obligations selon les al. 1 et 2 ne permettent pas d'obtenir des données souhaitées (voir les explications contenues dans le commentaire des al. 1 et 2) et pour lesquelles il est donc raisonnable de soumettre les fournisseurs en question à des obligations de surveillance plus étendues que la simple obligation de tolérer celle-ci ou de livrer des données disponibles. La nécessité du caractère raisonnable de soumettre ces fournisseurs à des obligations plus étendues s'exprime aussi au travers des autres critères mentionnés dans l'*al. 3*, à savoir la grande importance économique des services fournis et le grand nombre d'utilisateurs de ces services. Il appartient au Conseil fédéral de concrétiser ces critères et de déterminer si ceux-ci sont dans le cas d'espèce remplis. Sur la base de cette norme de délégation, le Conseil fédéral fera en sorte que les possibilités de surveillance qui existent déjà soient maintenues. Il fera en particulier en sorte que les obligations supplémentaires visées par ladite norme

53 Voir aussi Marc Jean-Richard-dit-Bressel in: Niggli/Heer/Wiprächtiger (éd.), Basler Kommentar, Schweizerische Strafprozessordnung, Bâle 2011, n. 20 ad art. 269 CPP.

s'appliquent aux services e-mail fournis par de grandes entreprises, étant entendu que l'OSCPT actuelle prévoit déjà cela pour les fournisseurs de services de télécommunication fournissant de tels services. A défaut, les possibilités de surveillance pouvant avoir lieu sous l'empire de la nouvelle LSCPT seront alors plus limitées qu'avec la LSCPT actuelle, ce qui n'est pas conforme au but premier visé par la révision totale de la loi.

Dans la mesure où le Conseil fédéral fait usage de la compétence que lui attribue l'*al. 3*, les dispositions du présent projet concernant les surveillances à effectuer par les fournisseurs de services de télécommunication sont applicables par analogie, étant donné que le Conseil fédéral soumet ainsi les personnes visées à l'art. 2, let. c, à tout ou partie des obligations des fournisseurs de services de télécommunication. Dans ce cas, sont aussi applicables aux fournisseurs de services de communication dérivés les dispositions qui ne mentionnent expressément que les fournisseurs de services de télécommunication (p.ex. art. 4, 17, let. a à d, 18, 24s. et 32).

Art. 28 Obligations des exploitants de réseaux de télécommunication internes

L'*art. 28, al. 1* impose aux personnes visées l'obligation minimale mais suffisante de tolérer une surveillance ainsi que des obligations accessoires nécessaires pour permettre l'exécution de celle-ci. Elle correspond aux obligations incombant selon la LSCPT actuelle aux exploitants de réseaux de télécommunication internes et de centraux domestiques. S'inspirant en partie de la réglementation en vigueur applicable à la surveillance au sein d'un réseau de télécommunication interne ou d'un central domestique, il est prévu que ce soit le service ou une personne mandatée par celui-ci, en particulier la police, qui exécute la surveillance considérée. Ceci ne signifie pas que le service peut transférer des tâches administratives à des privés, au sens de l'art.178, al. 3, Cst. Le service demeure en effet responsable de l'exécution de la tâche.

L'*al. 2* impose en outre à ces personnes l'obligation de livrer les données secondaires dont elles disposent (au moins celles disponibles au moment où la décision de surveillance est rendue), sans toutefois les contraindre à conserver ces données. Ce régime est susceptible d'entraîner – par rapport à la réglementation normale applicable aux fournisseurs de services de télécommunication – la perte de données secondaires pouvant être obtenues dans le cadre d'une surveillance rétroactive et la perte de données obtenues dans le cadre d'une surveillance en temps réel, étant donné que le temps de réaction pour initier la surveillance est augmenté, le service ou la personne mandatée par celui-ci ayant besoin de temps pour entrer en action. Il y a toutefois lieu de renoncer à imposer des obligations supplémentaires, impliquant une préparation active, aux personnes visées, car ce serait leur demander des efforts disproportionnés, même s'il est possible que la motion Glanzmann-Hunkeler 07.3627 (Enregistrement des cartes d'accès sans fil à prépaiement), qui n'est pas claire sur ce point, poursuive cet objectif.

Art. 29 Obligations des personnes qui laissent leur accès à un réseau public de télécommunication à la disposition de tiers

L'*art. 29, al. 1* impose aux personnes visées l'obligation minimale mais suffisante de tolérer une surveillance ainsi que des obligations accessoires nécessaires pour permettre l'exécution de celle-ci. Il est prévu que ce soit le service ou une personne

mandatée par celui-ci, en particulier la police, qui exécute la surveillance considérée. Ceci ne signifie pas que le service peut transférer des tâches administratives à des privés, au sens de l'art.178, al. 3, Cst. Le service demeure en effet responsable de l'exécution de la tâche considérée.

L'*al. 2* impose en outre à ces personnes l'obligation de livrer les données secondaires dont elles disposent (au moins celles disponibles au moment où la décision de surveillance est rendue), sans toutefois les contraindre à conserver ces données. Ce régime est susceptible d'entraîner – par rapport à la réglementation normale applicable aux fournisseurs de services de télécommunication – la perte de données secondaires pouvant être obtenues dans le cadre d'une surveillance rétroactive et la perte de données obtenues dans le cadre d'une surveillance en temps réel, étant donné que le temps de réaction pour initier la surveillance est augmenté, le service ou la personne mandatée par celui-ci ayant besoin de temps pour entrer en action.

Il y a toutefois lieu de renoncer à imposer aux personnes visées des obligations supplémentaires impliquant une préparation active car ce serait leur demander des efforts disproportionnés. Il en va ainsi de l'obligation d'identification des usagers que semble demander la motion Glanzmann-Hunkeler 07.3627 (Enregistrement des cartes d'accès sans fil à prépaiement). Une telle obligation d'identification par les personnes visées dans cet article se heurterait en outre à des problèmes pratiques. En effet, il appartiendrait à celles-ci, que ce soit un particulier ou un hôtel, un restaurant, un café, un hôpital, une école, un commerce, une commune, etc., qui laisse son accès à la disposition de tiers, de tenir un registre afin de noter, sur présentation d'une pièce de légitimation de ces tiers, qui a accès et quand à son réseau, ce qui engendre un travail relativement important, dont la fiabilité n'est pas garantie et qui n'est pas forcément compatible avec l'activité du tiers (p.ex. consommer un café rapidement dans un établissement qui offre l'accès à son réseau Wi-Fi).

La motion précitée paraît exiger une obligation d'identification des usagers (et pas seulement des ordinateurs de ceux-ci) de réseaux laissés à la disposition de tiers.

Si une telle obligation devait effectivement être prévue, elle ne devrait incomber qu'au fournisseur de services de télécommunication qui fournit le réseau à la personne qui le laisse à la disposition des tiers, et non à celle-ci. Il apparaît que l'identification des usagers de ces réseaux et des ordinateurs de ceux-ci, prévue dans l'art. 22 AP-LSCPT ayant reçu un accueil mitigé dans le cadre de la procédure de consultation, soit techniquement possible pour les fournisseurs de services de télécommunication. D'après les tenants de cette identification, il est facile pour un hôtel ou un commerce de mettre Internet à la disposition d'un client moyennant l'accès via un code, via un SMS ou encore via son adresse e-mail personnelle. La majorité des grands fournisseurs de services de télécommunication offrent déjà cette possibilité en Suisse. Concrètement, cela peut par exemple se faire en exigeant de l'usager qu'il s'identifie préalablement (p.ex. au moyen de son téléphone portable ou de sa carte de crédit), avant de pouvoir accéder à Internet, auprès du fournisseur de services de télécommunication qui fournit le réseau à la personne qui le laisse à la disposition de tiers. Les tenants de cette identification invoquent en outre le fait que l'accès anonyme à Internet n'est pas possible dans certains pays voisins de la Suisse et en Suède. Une telle réglementation peut certes se justifier sous l'angle de la lutte contre la criminalité. Nonobstant ce qui précède, il ne faut pas perdre de vue qu'elle impliquerait une charge supplémentaire pour les fournisseurs de services de télécommunication et, surtout, irait très loin, puisqu'elle causerait la fin de la liberté qu'offre le fonctionnement actuel des réseaux Wi-Fi, sans pour autant signifier la fin

de ces réseaux. Il se pourrait également que l'obligation d'identification ne constitue pas la panacée, puisqu'elle pourrait techniquement être éludée. Il est donc proposé dans le présent projet, en dépit de ce que demande la motion Glanzmann-Hunkeler 07.3627 (Enregistrement des cartes d'accès sans fil à prépaiement) et du fait que l'on tolère ainsi une lacune dans la surveillance, de renoncer à cette obligation d'identification.

Art. 30 Obligations des revendeurs professionnels de cartes ou de moyens semblables

L'*art. 30* vise à combler une lacune de la législation en vigueur. Cette lacune concerne l'enregistrement, par les personnes visées par cet article, des données sur l'identité de leurs clients, auxquels elles fournissent des moyens permettant d'accéder à un réseau public de télécommunication sans souscrire à un abonnement. En effet, en vertu de la législation actuelle, l'obligation d'enregistrer ces données n'incombe qu'aux fournisseurs de services de télécommunication. La conséquence en est que les revendeurs visés par cette disposition (p.ex. Interdiscount, Media Markt et Mobilezone), qui obtiennent de la part de fournisseurs de services de télécommunication (p.ex. Swisscom, Orange et Sunrise) de tels moyens – en particulier des cartes SIM à prépaiement, des cartes d'accès sans fil à Internet à prépaiement – non encore enregistrés au nom d'un client, n'ont pas à enregistrer ces données. Ceci implique l'anonymat du client et constitue une lacune injustifiée dans la surveillance. Il est, en outre, prévu que les personnes visées doivent ensuite communiquer les données enregistrées au fournisseur de services de télécommunication au réseau duquel le moyen considéré donne accès (p.ex. Swisscom, Orange et Sunrise), afin que celui-ci puisse les enregistrer à son tour; ceci, de manière à ce que le fournisseur puisse, conformément aux art. 21 et 23, les fournir au moyen du système de commutation des demandes de renseignements sur les services de télécommunication (appelé CCIS) exploité par le service en collaboration avec les fournisseurs de services de télécommunication. Voir également le commentaire de l'art. 21, al. 2. La violation des obligations prévues à l'*art. 30* est sanctionnée par l'art. 39, al. 1, let. c. Il importe de préciser que les simples cartes téléphoniques permettant, en lieu et place de l'argent, de téléphoner dans des cabines téléphoniques (p.ex. «taxcards», contenant un crédit, vendues dans les kiosques) ne sont pas visées par l'obligation faisant l'objet de l'*art. 30*.

2.7 Section 7 Garantie de la disponibilité des fournisseurs de services de télécommunication à renseigner et à surveiller

Les art. 31 à 34 visent en particulier, comme l'art. 18, à garantir une bonne exécution des surveillances de la correspondance par télécommunication ordonnées. Il s'agit notamment de pouvoir examiner la possibilité des fournisseurs de services de télécommunication de fournir les renseignements et de surveiller les services de télécommunication désignés, ce conformément au droit applicable. Il s'agit donc d'une question de conformité («compliance») aux obligations y relatives. On ne peut pas parler d'une activité de «certification», comme ce fut le cas aux art. 18 et 24

AP-LSCPT, étant donné que la procédure mise en place n'a pas pour but de vérifier le respect de certains standards pour des produits ou des services.

Art. 31 Dispositions d'exécution applicables aux types de renseignements et de surveillance

L'art. 31 constitue une norme de délégation au Conseil fédéral (al. 1 et 2) et au DFJP (al. 3). Ces deux autorités doivent pouvoir fixer les détails concernant la surveillance de la correspondance par poste et télécommunication. Se pose à cet égard la question de savoir quels détails doivent être réglés.

La séparation entre les aspects de droit administratif (LSCPT) et de procédure pénale (CPP) répond à l'exigence exprimée au ch. 2 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT). Cet examen séparé est sensé, au vu du fait que la LSCPT, d'une part, et le CPP, d'autre part, ont des destinataires différents et cherchent à réglementer des choses différentes. Dit de manière simplifiée: alors que dans le CPP, c'est la personne prévenue qui est au centre de l'attention, la LSCPT vise le fournisseur dans le domaine de la correspondance par poste et télécommunication qui doit collaborer à la surveillance, relevant de la procédure pénale, de la personne prévenue. La LSCPT suit en quelque sorte le CPP.

En examinant la situation de manière superficielle, on peut avoir l'impression qu'on peut ordonner des types de surveillance non autorisés, parce que non couverts par une base légale (voir art. 8, al. 2 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales [CEDH][54] et art. 13, al. 1 et 36, al. 1 Cst.) suffisamment précise. Tel n'est toutefois pas le cas, étant donné que les art. 269 à 279 CPP (en particulier les art. 269 à 269ter dans leur version modifiée) règlent de manière adéquate l'admissibilité du point de vue de la procédure pénale des types de surveillance. La LSCPT n'a pas à se prononcer sur ces aspects de procédure pénale, mais doit le plus possible garantir la mise en œuvre technique des surveillances admissibles du point de vue de la procédure pénale (sous réserve de la recherche en cas d'urgence et de la recherche de personnes condamnées). Ce n'est qu'en relation avec cet aspect technique et de droit administratif qu'il est nécessaire de régler précisément dans le sens technique les types de surveillance dans la LSCPT et dans l'OSCPT.

A l'encontre des personnes surveillées, toute surveillance de la correspondance par poste et télécommunication peut, selon le cas d'espèce, être admissible. La garantie juridique des droits fondamentaux n'est dans ce contexte pas assurée au moyen de dispositions détaillées d'une ordonnance mais par le biais de la procédure pénale. Les résultats d'une surveillance (en temps réel ou rétroactive; contenus de communications ou données secondaires) ne peuvent en effet pas être exploités sans autorisation judiciaire; il est tout de suite mis fin à une surveillance non autorisée et les données recueillies sont détruites (art. 277 CPP).

Par conséquent, la base légale permettant des mesures comme le recours à des GovWare ou IMSI-catchers et des types de surveillance comme la surveillance en rapport avec une ressource d'adressage étrangère et la recherche par champ

54 RS **0.101**

d'antennes doit figurer dans le CPP et celle pour la collaboration des fournisseurs de services de télécommunication dans la LSCPT[55]:

- Sous l'angle de la LSCPT, le recours à des GovWare ou des IMSI-catchers n'a pas d'importance, étant donné qu'il n'exige pas la collaboration des fournisseurs de services de télécommunication. Du point de vue de la procédure pénale, une nouvelle base légale doit toutefois être créée, étant donné qu'il va au-delà du cadre des types de surveillance réglés jusqu'à maintenant (voir le commentaire des art. 269bis et 269ter CPP).
- Du point de vue de la procédure pénale, la recherche par champ d'antennes[56] est, selon la doctrine et la jurisprudence[57], admissible à certaines conditions (obtention de données secondaires, au sens de l'art. 273 CPP, les conditions de l'art. 269, al. 1, let. b et c CPP devant toutefois être remplies). Une base légale particulière n'est pas nécessaire. Selon le Tribunal fédéral, la recherche par champ d'antennes ne constitue pas une atteinte grave aux droits fondamentaux, pour autant que ce mode d'identification des usagers constitue l'ultima ratio pour les investigations considérées, que l'on soit en présence de graves soupçons, qu'il s'agisse d'élucider un crime, que l'auteur soit suffisamment individualisable et qu'on n'obtienne pas de contenus de communications[58]. Il importe de ne pas perdre de vue que la recherche par champ d'antennes doit être autorisée par le tribunal des mesures de contrainte (art. 273, al. 2 CPP) et que le ministère public doit à cet effet soumettre l'ordre de surveillance et les motifs y relatifs (y compris les pièces du dossier déterminantes) à ce tribunal (art. 274, al. 1 CPP). La recherche par champ d'antennes ne présente du point de vue de la LSCPT pas de particularité qui nécessiterait une adaptation de cette loi, étant donné que ce mode de surveillance ne constitue qu'une forme d'acquisition de données secondaires et est déjà réglé dans l'actuelle OSCPT (art. 16, let. e OSCPT).
- Une mesure de surveillance en rapport avec une ressource d'adressage étrangère (surveillance d'un raccordement téléphonique avec un numéro d'appel étranger) ne constitue pas une nouveauté du point de vue de la procédure pénale, étant donné qu'elle consiste à surveiller un numéro d'appel étranger connu, pour savoir s'il est appelé par un participant se trouvant en Suisse. Le point de rattachement pour cette surveillance est – exactement comme lors d'une surveillance d'un raccordement national – un numéro d'appel déterminé. Il ne s'agit pas de la surveillance d'un raccordement tiers,

55 Voir aussi ATF **130** II 249, 253 ss et ATAF 2009/46, consid. 3.1.3, 3.2, 3.3.

56 La recherche par champ d'antennes permet dans un premier temps d'obtenir rétroactivement les données secondaires ne se référant pas à des personnes de l'ensemble des communications par téléphonie mobile qui ont lieu pendant un certain laps de temps en passant par une cellule déterminée d'une antenne. Dans un deuxième temps, on forme à l'aide de divers paramètres prédéfinis une intersection des connexions obtenues de deux (ou plusieurs) antennes; voir à ce sujet l'exemple chez Thomas Hansjakob, op. cit. (note 11), n. 18 ad art. 16 OSCPT et l'état de fait dans l'ATF **137** IV 340, 341s. Cette de surveillance sert à l'individualisation et à l'identification de l'auteur lorsque l'on est déjà en présence de graves soupçons objectivement concrétisés de commission d'un crime.

57 ATF **130** II 249 et **137** IV 340, 346 ss (avec les références à la doctrine)

58 ATF **137** IV 340, 349 ss

qui n'est admissible qu'aux conditions de l'art. 270, let. b CPP[59]. La LSCPT ne règle que la faisabilité technique et organisationnelle ainsi que le fait de savoir qui doit supporter les frais de la surveillance[60].

– Pour être complet, il importe de mentionner que les surveillances d'Internet ne nécessitent aucune base légale particulière, étant donné qu'elles sont saisies de manière incontestée[61] par la définition de la correspondance par télécommunication des art. 269 CPP et 1 LSCPT.

En résumé, on peut retenir que la base légale concernant la question de savoir *si* une surveillance est admissible doit être cherchée dans les art. 269 ss CPP (aspect de procédure pénale). En revanche, la question de savoir *comment* les acteurs actifs dans le domaine de la correspondance par poste et télécommunication peuvent être obligés de collaborer dans le cadre d'une telle surveillance est réglée dans la LSCPT (aspect de droit administratif). Voir à ce sujet également le commentaire de l'art. 42.

Les *al. 1 et 2* constituent une norme de délégation au Conseil fédéral lui attribuant la compétence de régler des questions qu'il règle aujourd'hui déjà dans l'OSCPT. Cette règlementation permet par exemple de tenir compte du fait que les données secondaires que l'on doit pouvoir exiger d'un fournisseur de services de télécommunication dans le cadre d'une surveillance rétroactive d'une correspondance téléphonique, y compris par Internet, ne doivent pas forcément être les mêmes que celles que l'on doit pouvoir exiger dans le cadre d'une surveillance rétroactive d'Internet (portant sur autre chose qu'une correspondance téléphonique). Une surveillance rétroactive d'Internet ne doit par exemple pas forcément permettre de savoir quelles pages Internet ont été consultées, dès lors qu'un tel type de surveillance, bien que portant sur des données secondaires, revient en somme à permettre une certaine surveillance du contenu de la correspondance. Les milieux concernés seront consultés sur les propositions que fera le Conseil fédéral en vertu des *al. 1 et 2*. Il importe de mentionner que des surveillances d'un nouveau type, qui ne figure pas encore dans les dispositions d'exécution mais est couvert par le CPP, peuvent tout de même être exécutées. Le fournisseur de services de télécommunication n'aura pas l'obligation dans un tel cas – comme c'est en principe également le cas des fournisseurs de services de communication dérivés (art. 27) ou des exploitants de réseaux de télécommunication internes (art. 28) – d'exécuter lui-même la surveillance mais ne devra que permettre et tolérer l'exécution de cette surveillance par le service ou par un tiers mandaté par celui-ci (voir art. 26, al. 2 et 32, al. 2).

L'*al. 3* prévoit que les détails techniques et administratifs qui ont pour objectif la bonne exécution au moindre coût des types de surveillances admissibles usuels ne sont plus, comme aujourd'hui, réglés dans des directives du service mais dans des dispositions d'ordonnances du DFJP. Il est prévu de ne publier les textes d'ordon-

59 Concernant la formulation prêtant à confusion de l'art. 270, let. b CPP («tiers» au lieu de «raccordement tiers»), voir Thomas Hansjakob, op. cit. (note 11), n. 10 ad remarques préliminaires.

60 Voir ATAF 2009/46, consid. 3.2, 7.4 et 8.3. Le TAF ne constate ici pas de violation de l'art. 13, al. 1 Cst. Cette constatation intervient de manière un peu surprenante, étant donné que dans le consid. 3.2 le TAF fonde sa non-entrée en matière sur le grief du fournisseur de services de télécommunication, selon lequel les droits de la personne surveillée seraient violés sans base légale.

61 Voir simplement Marc Jean-Richard-dit-Bressel in: Niggli/Heer/Wiprächtiger (éd.), Basler Kommentar, Schweizerische Strafprozessordnung, Bâle 2011, n. 15 s. ad art. 269 CPP.

nances, très techniques et volumineux de niveau départemental, dans le Recueil officiel du droit fédéral qu'au moyen d'un renvoi (art. 5 de la loi fédérale du 18 juin 2004 sur les recueils du droit fédéral et la Feuille fédérale[62]). Dans ce cas, le texte complet pourra se trouver sur une page Internet du DFJP.

La réglementation des détails techniques et administratifs dans une ordonnance implique que l'exécution des surveillances considérées est standardisée. Des standards internationaux existent en la matière et il y a donc lieu d'en tenir compte. Il importe de préciser que tous les types de surveillances admissibles au sens de l'al. 1, c'est-à-dire couverts par la législation, ne sont pas forcément standardisés. Ceux qui sont admissibles mais pas (encore) standardisés sont des mesures de surveillance dites spéciales, des cas dits spéciaux. Le changement de compétence qui précède est conforme à l'esprit du ch. 1 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT), selon lequel les tâches normatives et réglementaires du service doivent en substance être distinguées de ses tâches d'exécution des surveillances. Ledit changement donnera aussi plus de légitimité aux dispositions considérées, lesquelles pourront notamment être élaborées dans le cadre de l'organe consultatif selon l'art. 5.

Art. 32 Disponibilité à renseigner et à surveiller

Sont bien entendu visés par l'*art. 32* les types de surveillances dont le fournisseur de services de télécommunication n'est pas dispensé en vertu de l'art. 26, al. 6.

C'est conformément au droit applicable, en particulier dans le respect des modalités fixées dans la LSCPT, l'OSCPT et les ordonnances contenant les détails techniques et administratifs, que les renseignements visés doivent être fournis et les surveillances exécutées, d'après l'*al. 1*. Pour pouvoir satisfaire à leur obligation de fournir les renseignements et les données considérés, les fournisseurs de services de télécommunication doivent être en leur possession, ce qui suppose qu'ils doivent conserver ces renseignements et les données secondaires.

L'obligation visée à l'*al. 2* des fournisseurs de services de télécommunication implique un comportement actif de leur part, conformément aux directives données par le service (art. 16, let. d). Ils doivent par conséquent fournir notamment les renseignements nécessaires à l'exécution de la surveillance et, au besoin, garantir l'accès à leurs installations.

L'*al. 3* prévoit que les fournisseurs de services de télécommunication peuvent confier à leurs frais l'exécution de tout ou partie des obligations de renseignement et de surveillance leur incombant à des tiers, principalement à des entreprises qui se sont spécialisées dans l'offre de services de surveillance de la correspondance par télécommunication sur ordre des autorités (*lawful interception*). Cette réglementation permet une grande flexibilité. Elle implique en particulier que les fournisseurs de services de télécommunication ne sont pas contraints d'acquérir les infrastructures pour satisfaire à ces obligations. Cette réglementation leur permettra par exemple également de mettre leurs efforts en commun pour satisfaire à ces obligations, peu importe d'ailleurs que ce soit au moyen d'infrastructures qu'ils auront achetées ou louées. Pour satisfaire aux exigences de l'al. 1, il suffit donc, selon l'*al. 3*, que le fournisseur de services de télécommunication soit en mesure de fournir les rensei-

62 RS **170.512**

gnements visés et d'exécuter les surveillances considérées par le truchement d'un tiers ou en collaboration avec celui-ci. C'est toutefois aux seuls fournisseurs de services de télécommunication qu'incombent les obligations de renseigner et de surveiller, et non aux entreprises tierces auxquelles ils feront éventuellement appel. Pour le surplus, voir le commentaire de l'art. 33, al. 1. La *phr. 2 de l'al. 3* régit la relation de droit privé entre le fournisseur de services de télécommunication et le tiers auquel il choisit de confier l'exécution des obligations précitées. Quant à la *phr. 3 de l'al. 3,* elle concerne la relation de droit administratif entre le service et le tiers et a, en particulier, pour objectif de permettre un bon déroulement des surveillances, y compris pour ce qui concerne la protection et la qualité des données.

Art. 33 Preuve de la disponibilité à renseigner et à surveiller

Les fournisseurs de services de télécommunication doivent dans l'hypothèse visée démontrer qu'ils peuvent fournir les renseignements en question et exécuter les surveillances considérées conformément au droit applicable, en particulier dans le respect des modalités fixées dans la LSCPT, l'OSCPT et les ordonnances contenant les détails techniques et administratifs. Les fournisseurs de services de télécommunication supportent les frais liés à la démonstration selon l'*al. 1*, partant aussi ceux qui découleraient de leur recours à des entreprises tierces pour apporter ladite démonstration. Un fournisseur de services de télécommunication ne doit bien entendu fournir la preuve considérée que pour les types de surveillance dont il n'est pas dispensé de l'exécution en vertu de l'art. 26, al. 6. Cette obligation implique un comportement actif de sa part; par conséquent, il doit fournir en particulier les renseignements nécessaires à la démonstration et, au besoin, garantir l'accès à ses installations. Il est possible – ce qui est admissible aux termes de l'art. 32, al. 3 – que le fournisseur de services de télécommunication ne soit en mesure de satisfaire aux obligations de renseignement et de surveillance lui incombant que par le truchement d'un tiers ou en collaboration avec celui-ci, auquel il a confié l'exécution de tout ou partie de ces obligations. Si tel est le cas, ce tiers pourra également être amené à entreprendre les démarches nécessaires – soutenant ainsi le fournisseur de services de télécommunication en question dans l'exécution de l'obligation de démonstration qui lui incombe en vertu de l'*al. 1* – pour démontrer au service qu'il est en mesure de remplir les obligations de renseignement et de surveillance susmentionnées à la place de ce fournisseur de services de télécommunication ou en collaboration avec celui-ci. Si le tiers ne parvient pas à faire cette démonstration, cet échec est à mettre sur le compte du fournisseur de services de télécommunication. Pour le surplus, voir le commentaire de l'art. 32, al. 3.

La possibilité qu'a le service de confier, en vertu de l'*al. 2*, à une tierce personne la tâche de contrôler si le fournisseur de services de télécommunication a fourni la preuve de sa disponibilité à renseigner et à surveiller se justifie par le fait que ce contrôle est susceptible d'impliquer un long travail, qui peut être incompatible avec les ressources en personnel du service. Cette possibilité du service ne signifie pas qu'il peut transférer des tâches administratives à des privés, au sens de l'art. 178, al. 3, Cst. Le service demeure en effet responsable de l'exécution de la tâche. Si le service fait usage de cette possibilité, il conserve toutefois, conformément à l'al. 6, la tâche de délivrer aux fournisseurs de services de télécommunication une confirmation lorsque ceux-ci ont fourni la démonstration susmentionnée. Ceci suppose qu'il contrôle que la tierce personne qu'il a mandatée a respecté les modalités fixées pour l'examen effectué.

Sur la base de l'*al. 3*, le service et le fournisseur de services de télécommunication pourront par exemple effectuer des contrôles de qualité, portant notamment sur des «cibles» test fictives (voir art. 18 et commentaire y relatif).

En vertu de l'*al. 4*, le fournisseur de services de télécommunication examiné doit verser au service un émolument en guise de contrepartie de la prestation fournie par celui-ci. Il appartient au Conseil fédéral de fixer cet émolument, selon la nature de la prestation fournie par le service.

L'*al. 5* se rapproche de l'art. 16, let. d, lequel ne s'inscrit toutefois pas dans une procédure de preuve de la disponibilité à renseigner et à surveiller, y compris suite à une surveillance qui ne s'est pas déroulée de manière optimale, mais dans une procédure d'exécution d'une surveillance. Les fournisseurs de services de télécommunication supportent les coûts des mesures qu'ils doivent prendre pour pallier les manquements concernant leur disponibilité à renseigner et à surveiller, étant donné que ces mesures sont nécessaires pour leur permettre de remplir leurs obligations légales. S'ils ne donnent pas suite aux injonctions du service de prendre les mesures techniques et organisationnelles pour pallier les manquements concernant leur disponibilité à renseigner et à surveiller, il pourront être poursuivis en vertu de l'art. 39, al. 1, let. a.

Le contenu de la confirmation et les détails de sa validité dans le temps seront, conformément à l'*al. 6*, fixés par le Conseil fédéral par voie d'ordonnance. La confirmation devra en particulier mentionner son champ d'application matériel, c'est-à-dire quels renseignements et types de surveillances ont fait l'objet de la démonstration considérée, et son champ d'application temporel, à savoir jusqu'à quand elle déploie ses effets, notamment en cas de développements techniques. Cette confirmation permet de considérer que le fournisseur de services de télécommunication est en mesure de fournir les types de renseignements et d'exécuter les types de surveillances sur lesquels elle porte. Elle permet donc de retenir que le fournisseur de services de télécommunication satisfait pour ces renseignements et surveillances à l'obligation qui lui incombe en vertu de l'al. 1. Cette confirmation a également des conséquences financières pour un fournisseur de services de télécommunication, lorsque, dans un cas concret, il s'avère qu'il n'est pas en mesure d'exécuter une surveillance (voir art. 34, en particulier al. 2, let. a).

Art. 34 Prise en charge des coûts en cas de manquement à la collaboration

L'*art. 34* s'applique à deux types de manquements dans la disponibilité à surveiller. Il vise d'abord le cas où un fournisseur de services de télécommunication, bien que disposé à le faire, n'est pas en mesure d'exécuter une surveillance. Il vise ensuite le cas où le fournisseur refuse de donner suite à l'injonction de surveillance du service.

Est visé par l'*al. 1* le fait que les fournisseurs de services de télécommunication ne sont pas, dans un cas concret, en mesure d'exécuter ou ne veulent pas exécuter les surveillances requises conformément au droit applicable, c'est-à-dire, en particulier, dans le respect des modalités fixées dans la LSCPT, l'OSCPT et les ordonnances contenant les détails techniques et administratifs. Ne sont bien entendu visés par cette disposition que les types de surveillances dont le fournisseur de services de télécommunication n'est pas dispensé de l'exécution en vertu de l'art. 26, al. 6. Si l'entreprise tierce à laquelle un fournisseur de services de télécommunication a confié l'exécution de tout ou partie des obligations de surveillance qui lui incombent ne parvient pas à remplir la tâche prescrite, cet échec sera imputable au fournisseur

de services de télécommunication. Ce dernier devra partant dans ce cas également subir les conséquences mentionnées à l'*al. 1*. Pour le surplus, voir le commentaire des art. 31 et 32.

L'*al. 2* porte sur les exceptions concernant la prise en charge des coûts au sens de l'al. 1 et doit être une incitation pour les fournisseurs de services de télécommunication à se faire certifier. La libération de la prise en charge des coûts n'entre bien évidemment en considération que si un fournisseur de services de télécommunication, bien que voulant le faire, n'est pas en mesure d'exécuter la surveillance considérée. Le contenu de l'*al. 2, let. a* va de soi. En effet, un fournisseur de services de télécommunication qui dispose d'une confirmation visée à l'art. 33, al. 6 ne doit pas supporter les coûts en question, étant donné que cette confirmation permet précisément de considérer qu'il est en mesure d'exécuter les types de surveillances sur lesquels elle porte. Il est également justifié que dans l'hypothèse de l'*al. 2, let. b* le fournisseur de services de télécommunication n'ait pas à subir de conséquences financières liées à l'échec de la surveillance ordonnée. Est notamment visé le cas où le service n'a pas encore eu la possibilité, en particulier pour des raisons de ressources, de procéder à l'examen du fournisseur.

2.8 Section 8 Recherche en cas d'urgence et de personnes condamnées

Art. 35 Recherche en cas d'urgence

L'*art. 35* n'a pas sa place dans le CPP, vu qu'il ne s'applique pas à une procédure pénale en cours. Cet article ne trouve pas application en cas d'enlèvement ou de séquestration d'une personne dans un endroit inconnu parce que cela relève d'une procédure pénale et que les moyens de surveillance de la correspondance par poste et télécommunication nécessaires pour localiser l'auteur d'un tel acte pourront, partant, être ordonnés immédiatement par le ministère public. L'*art. 35* est en revanche applicable, par exemple, lorsque des personnes sont recherchées suite à une catastrophe (inondation, tremblement de terre, etc.), dans la mesure où les conditions prévues sont remplies.

L'*al. 1* prévoit que la surveillance de la correspondance par poste et télécommunication mise en œuvre dans un cas d'urgence n'est plus, contrairement à l'art. 3 de la LSCPT actuelle et à ce que prévoyait l'art. 27 AP-LSCPT, limitée à l'identification des usagers et aux données relatives au trafic, c'est-à-dire à des données secondaires. Elle permettra également d'obtenir le contenu des envois, dans le domaine de la correspondance postale, et celui des communications, dans le domaine de la correspondance par télécommunication. Ceci se justifie, étant donné que le contenu des correspondances et des communications est susceptible de donner des renseignements sur le lieu où se trouve la personne disparue et, dans le domaine de la correspondance par télécommunication, de permettre de vérifier si c'est vraiment elle qui utilise le raccordement surveillé. Ce sont les art. 19 à 32 et les dispositions d'exécution contenues dans l'OSCPT qui précisent les types de surveillance de la correspondance par poste et télécommunication au sens de l'art. 269 CPP qui peuvent être ordonnés et à qui incombent les obligations prescrites dans l'exécution de la surveillance considérée.

La condition de l'impossibilité de localiser la personne disparue, contenue à l'art. 3, al. 2 de la LSCPT actuelle, est complétée, à l'*al. 2*, par celle de la difficulté excessive. Cette adjonction se justifie, étant donné que la condition de l'impossibilité, prise à la lettre, pose des exigences exorbitantes et disproportionnées par rapport au bien juridique de la personne disparue qui est en jeu. La surveillance sera donc possible, à l'instar de ce que prévoient les art. 269, al. 1, let. c, CPP et 36, al. 1, lorsque les autres mesures prises jusqu'alors pour retrouver la personne disparue sont restées sans succès ou lorsque les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance.

Le recours aux dispositifs techniques de surveillance visés à l'art. 269bis CPP pour retrouver une personne disparue est également autorisé aux termes de l'*al. 3*. Ceci permet concrètement d'utiliser à cette fin des dispositifs tels que les IMSI-catchers. Ce mode de surveillance, efficace, est en particulier susceptible de permettre de retrouver une personne disparue même lorsque les mesures de surveillance de la correspondance par télécommunication dites classiques se sont révélées inopérantes. L'utilisation de ces dispositifs est toutefois subsidiaire au recours à ces mesures de surveillance (voir, par analogie, le commentaire de l'art. 269bis, let. b, CPP). Le recours à ce procédé (dispositifs tels que les IMSI-catchers) ne requiert en l'état actuel pas l'intervention d'un fournisseur de services de télécommunication ni un comportement de celui-ci typiquement contraire à l'art. 321ter, al. 1, CP et le service n'a pas à apporter son concours pour ce faire (aucun ordre de surveillance n'a donc à lui parvenir). Pour le surplus, voir le commentaire de l'art. 269bis CPP.

En cas de nécessité, en conformité avec le principe constitutionnel de la proportionnalité, l'*al. 4* permet, à l'instar de ce que prévoit l'art. 3, al. 1 de la LSCPT en vigueur, de surveiller la correspondance par poste et télécommunication qui n'est pas celle de la personne recherchée mais celle d'un tiers non impliqué. Ceci est en particulier indiqué lorsqu'on a des raisons de penser que la personne disparue utilise le raccordement de ce tiers ou appelle ce raccordement. Cette possibilité constitue une limitation du droit à la protection de la sphère privée de ce tiers, consacré par la constitution fédérale et par le droit international (voir infra, ch. 5); il y a lieu d'en tenir compte dans le cadre du pouvoir d'appréciation dans chaque cas d'espèce.

Art. 36 Recherche de personnes condamnées

L'*art. 36* prévoit la possibilité, nouvelle, d'avoir recours à une surveillance de la correspondance par poste et télécommunication pour rechercher une personne condamnée à une peine privative de liberté ou qui fait l'objet d'une mesure entraînant une privation de liberté, sur la base d'un jugement définitif et exécutoire. Cette surveillance, qui est possible dans le cadre d'une procédure pénale en cours, doit d'autant plus être admissible pour poursuivre l'objectif précité; en effet, dans ce cas de figure, on est, aux termes de l'*al. 1,* en présence d'un jugement définitif et exécutoire, et non uniquement de soupçons, mêmes graves (art. 269, al. 1, let. a CPP). Cette possibilité s'impose aussi du fait qu'elle est déjà prévue dans le domaine de l'entraide pénale internationale[63], selon l'art. 18*a,* al. 1 EIMP.

On renonce à mentionner à l'*al. 1* une durée minimale concernant la peine privative de liberté prononcée à partir de laquelle une surveillance peut être ordonnée. Ce qui devra guider le choix de l'autorité compétente d'ordonner ou non une surveillance

63 Thomas Hansjakob, op. cit. (note 11), n. 8 ad art. 1 LSCPT.

c'est le principe de la proportionnalité; l'autorité compétente devra tenir compte en particulier des éléments suivants: la durée de la peine privative de liberté ferme prononcée, l'infraction ayant donné lieu à cette peine, l'éventuelle dangerosité de la personne condamnée et le coût de la surveillance envisagée.

Cette réglementation, à l'instar de l'art. 35, n'a pas sa place dans le CPP, dès lors, qu'elle aussi, ne s'applique pas à une procédure pénale en cours, celle-ci étant à ce stade terminée. Contrairement à ce qui est en principe le cas des surveillances ordonnées dans le cadre de procédures pénales, la condition de l'art. 269, al. 2, CPP (catalogue d'infractions) n'est pas applicable aux surveillances ayant pour but de retrouver une personne condamnée à une peine privative de liberté ou qui fait l'objet d'une mesure entraînant une privation de liberté (voir le renvoi effectué à l'art. 37, al. 1). Ceci se justifie en particulier par le fait que, dans ce cas, on a affaire à un jugement définitif et exécutoire, et non simplement à des soupçons, mêmes graves (art. 269, al. 1, let. a, CPP). A l'instar de ce que prévoient en substance les art. 269 al. 1, let. c, CPP et 35, al. 2, let. a, cette mesure de surveillance est subsidiaire aux autres mesures qui peuvent être prises pour trouver la personne recherchée. La surveillance de la correspondance par poste et télécommunication visée à l'art. 36 permet non seulement d'obtenir les données permettant d'identifier les usagers et les données relatives au trafic, c'est-à-dire des données secondaires, mais également le contenu des envois, dans la domaine de la correspondance par poste, et celui des communications, dans le domaine de la correspondance par télécommunication. Ceci se justifie, étant donné que le contenu des correspondances et des communications est susceptible de donner des renseignements sur le lieu où se trouve la personne disparue et, dans le domaine de la correspondance par télécommunication, de permettre de vérifier si c'est vraiment elle qui utilise le raccordement surveillé. Ce sont les art. 19 à 32 et les dispositions d'exécution contenues dans l'OSCPT qui précisent les types de surveillance de la correspondance par poste et télécommunication au sens de l'art. 269 CPP qui peuvent être ordonnés et à qui incombent les obligations prescrites dans l'exécution de la surveillance considérée.

Le recours aux dispositifs techniques de surveillance visés à l'art. 269bis CPP pour retrouver une personne condamnée disparue est également autorisé aux termes de l'*al. 2*. Ceci permet concrètement d'utiliser à cette fin des dispositifs tels que les IMSI-catchers. Ce mode de surveillance, efficace, est en particulier susceptible de permettre de retrouver une personne disparue même lorsque les mesures de surveillance de la correspondance par télécommunication classiques se sont révélées inopérantes. L'utilisation de ces dispositifs est toutefois subsidiaire au recours à ces mesures de surveillance (voir, par analogie, le commentaire de l'art. 269bis, let. b, CPP). Le recours à ce procédé (dispositifs tels que les IMSI-catchers) ne requiert en l'état actuel pas l'intervention d'un fournisseur de services de télécommunication ni un comportement de celui-ci typiquement contraire à l'art. 321ter, al. 1 CP et le service n'a pas à apporter son concours pour ce faire (aucun ordre de surveillance n'a donc à lui parvenir). Pour le surplus, voir le commentaire de l'art. 269bis CPP.

L'*al. 3* permet, lorsque les conditions de l'art. 270 CPP sont par analogie remplies, de surveiller la correspondance par poste et télécommunication qui n'est pas celle de la personne recherchée mais celle d'un tiers non impliqué. Tel est par exemple le cas lorsqu'on a des raisons de penser que la personne recherchée utilise le raccordement de ce tiers ou appelle ce raccordement. Pour le surplus, voir le commentaire de l'art. 35, al. 4.

Art. 37 Procédure

L'*art. 37* mentionne la procédure applicable dans les cas visés aux art. 35 et 36.

L'*al. 1*, applicable aussi bien à l'art. 36 qu'à l'art. 35, reprend, à la différence de sa version dans l'AP-LSCPT, le contenu de l'art. 3, al. 3 de la LSCPT en vigueur, qui concerne cependant uniquement la recherche de personnes disparues. Il ne renvoie pas, en particulier, à la liste faisant l'objet de l'art. 269, al. 2, CPP pour ce qui concerne la surveillance visée à l'art. 36 (voir le commentaire de l'art. 36). Les articles cités ne doivent être appliqués que par analogie, étant donné que le CPP régit les procédures pénales en cours et que les surveillances visées par les art. 35 s. ont précisément lieu en dehors d'une procédure pénale.

L'*al. 2* prévoit que, dans le cas d'une surveillance effectuée dans le cadre d'une recherche en cas d'urgence, les personnes surveillées doivent, en dérogation à ce que prévoit l'art. 279 CPP, être informées de la surveillance dans les meilleurs délais. Dans le cadre d'une recherche de personnes condamnées, il peut y avoir un intérêt à garder la surveillance secrète plus longtemps, ou à omettre totalement cette information, par exemple pour permettre d'instruire une enquête à l'encontre d'une personne qui aurait favorisé la fuite de la personne recherchée (art. 279, al. 2 CPP par analogie). Un tel intérêt n'existe pas lors d'une recherche dans un cas d'urgence, ce qui justifie la dérogation précitée.

L'*al. 3* s'inspire du contenu de l'art. 3, al. 4 de l'actuelle LSCPT. Il règle la compétence pour ordonner et autoriser une surveillance faisant l'objet des art. 35 et 36, étant entendu que cette compétence peut aussi bien relever de la Confédération que des cantons. Dans le domaine de l'entraide pénale internationale, ces questions sont réglées à l'art. 18*a* EIMP. Dans ce domaine, la compétence d'ordonner la surveillance pour déterminer le lieu de séjour d'une personne poursuivie revient à l'Office fédéral de la justice, en vertu de l'art. 18*a*, al. 1 de la loi précitée. Le fait que la surveillance soit soumise à autorisation, plus précisément d'une autorité judiciaire, ne saurait – contrairement à certaines craintes exprimées pendant la procédure de consultation – causer une perte de temps dans la mise en œuvre de la surveillance. En effet, comme cela est le cas pour une surveillance ordonnée dans le cadre d'une procédure pénale et conformément à l'interprétation qui doit être faite de l'art. 274, al. 1 à 3, CPP, la surveillance ordonnée peut débuter avant même que le tribunal des mesures de contrainte l'ait autorisée.

2.9 Section 9 Frais et émoluments

Art. 38

En vertu du droit en vigueur, les équipements nécessaires à la mise en œuvre de la surveillance sont à la charge des fournisseurs de services postaux et de télécommunication. Ceux-ci reçoivent toutefois une indemnité équitable pour les frais occasionnés par chaque surveillance exécutée. En plus de cette indemnité, les autorités ordonnant une surveillance doivent verser un émolument pour les prestations du service (art. 16 de l'actuelle LSCPT). L'art. 2 de l'ordonnance du Conseil fédéral du 7 avril 2004 sur les émoluments et les indemnités en matière de surveillance de la

correspondance par poste et télécommunication (OEI-SCPT)[64] fixe pour chaque type de surveillance un émolument global et l'indemnité qui en fait partie et prévoit que, contrairement à ce que prévoit l'art. 16, al. 1 de l'actuelle LSCPT, cet émolument global doit être versé au service; celui-ci transmet l'indemnité aux fournisseurs. L'avant-projet envoyé en consultation (art. 30 AP-LSCPT) prévoyait de supprimer l'indemnisation des fournisseurs en relation avec le programme de consolidation 2011–2013.

Le relevé et l'analyse des coûts de la surveillance de la correspondance par poste et télécommunication ont fait l'objet d'un rapport externe, daté du 12 juin 2012, commandé par le service[65]. Ce rapport devait en particulier contribuer à déterminer la réglementation à prévoir dans le présent projet quant au financement de l'infrastructure nécessaire à la mise en œuvre des surveillances, au versement d'une éventuelle indemnisation des fournisseurs et au paiement d'un éventuel émolument au service.

Suite à ce rapport, une analyse minutieuse de son contenu et des diverses variantes a été menée, également par rapport à la réduction de tarifs que demande le postulat Recordon 11.4210 (Coût de la surveillance pénale des télécommunications). La variante consistant à verser une indemnité équitable aux fournisseurs aussi bien pour les coûts des équipements que pour ceux occasionnés par une mesure de surveillance a été envisagée. Cette variante est susceptible de mieux tenir compte du cas dans lequel pourraient se trouver en particulier de petits fournisseurs de services de télécommunication qui devraient supporter les coûts d'investissements nécessaires pour être aptes a exécuter des surveillances mais qui ne recevraient, en fin de compte, jamais d'ordre de surveillance à exécuter. Il importe à cet égard de préciser que ces fournisseurs sont susceptibles d'être dispensés d'obligations légales incombant en principe aux fournisseurs de services de télécommunication (voir commentaire de l'art. 26, al. 6), dispense qui aura une influence à la baisse sur les coûts d'investissements susmentionnés. Suite à l'analyse globale précitée, il a été décidé – contrairement à ce qui avait été proposé lors de la consultation et accueilli de manière contrastée – de maintenir le système actuel: les fournisseurs continueront de devoir financer les équipements nécessaires à la mise en œuvre des surveillances, ils continueront d'obtenir une indemnité équitable pour les frais occasionnés par l'exécution d'une mesure de surveillance, l'autorité qui a ordonné une surveillance continuera de devoir verser un émolument au service pour les prestations de celui-ci liées à l'exécution de la surveillance et le Conseil fédéral fixera les indemnités et les émoluments relatifs aux différents types de surveillances. Il n'est pas opportun de comparer l'obligation d'exécuter des surveillances de la correspondance avec l'obligation de dépôt (art. 265 CPP) pour justifier l'absence ou la suppression du versement d'une indemnité équitable aux fournisseurs pour les frais occasionnés par l'exécution d'une mesure de surveillance. En effet, si le détenteur d'un moyen de preuve refuse de se soumettre à l'obligation de dépôt, ce moyen de preuve peut être séquestré; ce n'est pas le cas des données devant être collectées au moyen d'une surveillance de la correspondance par télécommunication.

64 RS **780.115.1**

65 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ber-isc-ejpd-fda-pda-f.pdf

L'*al. 1* reprend et complète l'art. 16, al. 1, phr. 1 de l'actuelle LSCPT, en précisant que ce sont *les coûts* des équipements qui sont à la charge des personnes obligées de collaborer. Il implique notamment que ce sont les personnes obligées de collaborer qui doivent supporter les coûts liés à la livraison des données (au service). La livraison des données est en effet une composante de la disponibilité à surveiller et doit partant, en tant que dette portable, être prise en charge par les personnes obligées de collaborer. Cette disposition signifie en particulier que l'acquisition et l'entretien des équipements nécessaires à la mise en œuvre de la surveillance doivent en totalité être financés par les fournisseurs de services postaux et de télécommunication, y compris les coûts de personnel occasionnés par l'acquisition et l'entretien et les coûts d'amortissement des équipements. C'est le droit applicable, en particulier la LSCPT, l'OSCPT et les ordonnances contenant les détails techniques et administratifs, qui détermine les obligations que ces personnes doivent remplir afin que la surveillance puisse être mise en œuvre et que les données puissent être livrées à satisfaction. Ces obligations sont susceptibles de varier en fonction de la personne considérée (voir en particulier les art. 26 et 27).

L'*al. 2* reprend en substance l'art. 16, al. 1, phr. 2 de l'actuelle LSCPT, en éliminant une erreur rédactionnelle dans le texte allemand. Cet alinéa concerne les frais que les personnes obligées de collaborer ont en relation avec l'exécution d'une surveillance donnée, à l'exclusion donc des frais liés aux équipements, qui font l'objet de l'al. 1. Les coûts de chaque surveillance sont dans la plupart des cas majoritairement composés de coûts de personnel; des coûts de matériel sont toutefois aussi à imaginables. Les fournisseurs perçoivent une indemnité équitable forfaitaire pour ces frais (p.ex. 80 % de leurs frais effectifs, pouvant donner lieu à indemnisation, cf. art. 4*a*, al. 4 de l'actuelle OEI-SCPT). Cette indemnité – que le Conseil fédéral fixera par voie d'ordonnance (voir al. 4) – peut donc ne pas couvrir l'intégralité des frais variables effectifs d'un fournisseur. Il importe à cet égard également de ne pas perdre de vue le fait que l'utilisation de services de télécommunication dans un but délictueux représente une sorte de risque lié à l'activité des fournisseurs et le fait que c'est une tâche de tout citoyen que de contribuer à élucider des infractions (selon l'art. 167 CPP, les témoins reçoivent aussi une indemnité équitable). Il sied de préciser que même si c'est le service qui verse cette indemnité aux fournisseurs, la débitrice de celle-ci est en fin de compte l'autorité qui a ordonné la surveillance (pour le surplus, voir le commentaire de l'al. 3). L'al. 2 va dans le sens du ch. 4 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT).

L'*al. 3* précise expressément, pour des raisons de clarté, ce qui découle déjà de l'art. 16, al. 2 de l'actuelle LSCPT, à savoir que l'autorité qui a ordonné la surveillance doit verser un émolument – fixé par voie d'ordonnance par le Conseil fédéral (voir al. 4) – au service pour les prestations fournies par celui-ci en relation avec la surveillance de la correspondance par poste et télécommunication. On clarifie à cet égard que le service perçoit des autorités qui ont ordonné des surveillances un émolument global, qui contient non seulement l'émolument proprement dit pour les prestations du service (*let. a*) mais encore l'indemnité à l'attention des personnes obligées de collaborer (*let. b*); le service transmet l'indemnité aux personnes obligées de collaborer (voir al. 2).

L'*al. 4* reprend l'art. 16, al. 2 de l'actuelle LSCPT, qui constitue la norme de délégation à l'attention du Conseil fédéral lui ayant permis d'adopter l'actuelle OEI-SCPT. Le Conseil fédéral est lié aux principes de la couverture des frais et d'équivalence

lors de la répercussion des coûts découlant de mesures de surveillance. Sachant que le service n'exécute actuellement pas ses tâches en couvrant ses frais (taux de couverture des frais de 54 % pour l'année 2012), il se pose la question de savoir s'il est approprié de maintenir le taux (bas) actuel de couverture des frais, étant entendu que la poursuite pénale est une tâche cantonale. Le Conseil fédéral se penchera en détail sur cette question lorsqu'il fixera les émoluments que les autorités qui ordonnent des surveillances doivent verser.

Il sied encore de mentionner ici que le montant versé par l'autorité qui a ordonné la surveillance au service au titre d'émolument constitue des frais de procédure, plus précisément des débours, que l'autorité peut, dans le respect des règles de procédure, en tout ou en partie mettre à la charge de tiers, en particulier du prévenu condamné (art. 422, 425 et 426 CPP*)*.

2.10 Section 10 Dispositions pénales

Art. 39 Contraventions

L'*art. 39* a été modifié, par rapport à sa version envoyée en consultation, en particulier au vu des changements opérés à l'art. 40. Les art. 6 et 7 DPA sont en particulier applicables à la détermination des personnes auxquelles les dispositions pénales de l'*art. 39* sont applicables (voir art. 40 et commentaire y relatif).

L'*al. 1* répond à la nécessité d'introduire dans la nouvelle LSCPT des dispositions pénales permettant de sanctionner de manière efficace les personnes soumises à cette loi et qui ne respecteraient pas certaines des obligations fondées sur celle-ci, adoptant ainsi un comportement susceptible d'entraver les surveillances ordonnées. L'expérience montre que les fournisseurs importants de services de télécommunication qui sont actifs sur le marché suisse sont en principe conscients de leurs obligations. L'amende maximale que prévoit l'*al. 1* pour la commission intentionnelle des infractions prévues aux let. a à d est supérieure au montant maximal de 10 000 francs de l'amende prévue à l'art. 292 CP (Insoumission à une décision de l'autorité) (voir aussi art. 106, al. 1, CP). Ce dernier montant est en effet susceptible d'être trop bas pour dissuader de commettre les infractions précitées, en particulier au vu des économies pouvant être réalisées en ayant les comportements réprimés. Bien entendu, l'autorité appelée à prononcer une amende fondée sur l'*al. 1* tiendra compte des différentes circonstances du cas d'espèce, comme l'acte commis et la capacité économique de l'entreprise considérée (voir art. 8 DPA et art. 106, al. 3, CP). Précisons que d'autres contraventions contenues dans le droit pénal accessoire prévoient des amendes maximales d'un montant aussi bien inférieur que supérieur à celui de 100 000 francs prévu à l'*al. 1*. La sanction fondée sur l'art. 39 ne doit avoir lieu que subsidiairement par rapport à celle fondée sur des dispositions pénales plus sévères d'autres lois qui pourraient également être remplies. On pense en particulier à l'entrave à l'action pénale et à la violation des obligations de garder le secret, qui sont également réglées de manière détaillée dans le CP. Des cas de figure sont ainsi envisageables, dans lesquels un acte remplit à la fois l'énoncé de fait légal de l'art. 39, al. 1, let. d et celui, plus grave, de l'art. 320 ou 321ter CP. Dans ces cas, l'auteur de l'infraction ne doit pas être puni sur la base de la disposition pénale

moins sévère que constitue l'*art. 39*, étant donné qu'il n'y a aucune raison objective pour ce faire.

L'*al. 1, let. a* prévoit en cas d'inobservation des injonctions du service une sanction analogue à celle prévue à l'art. 292 CP. La sanction de l'art. 292 CP ne saurait toutefois être dissuasive. Ceci, notamment au regard des économies qu'une personne soumise à la LSCPT est susceptible de réaliser pour le cas où elle n'exécute pas une injonction de surveillance rendue par le service, qui se fonde sur un ordre de surveillance donné par l'autorité compétente, en principe par le ministère public, ou pour le cas où elle ne donne pas suite aux injonctions du service de prendre les mesures techniques et organisationnelles pour pallier ses manquements concernant sa disponibilité à renseigner et à surveiller (art. 33, al. 5). La création d'une disposition spécifique, prévoyant une sanction plus sévère que celle de l'art. 292 CP, se justifie par conséquent. Si ce mécanisme a également pour but accessoire d'inciter les personnes soumises à la LSCPT à exécuter les injonctions du service dans les meilleurs délais, il n'empêche toutefois pas ces personnes de contester ces injonctions conformément aux dispositions de la procédure fédérale (voir art. 42). Les règles relatives au contrôle de la validité de l'injonction du service par le juge pénal ordinaire, saisi d'une poursuite pour infraction à l'art. 39, al. 1, let. a à la suite du service, sont les mêmes que celles, développées par la doctrine[66] et la jurisprudence, qui s'appliquent en cas de violation de l'art. 292 CP.

Se fondant notamment sur ce qu'exige le ch. 2 de la motion Schweiger 06.3170 (Cybercriminalité. Protection des enfants), l'*al. 1, let. b* prévoit – toujours dans le but de permettre une exécution efficace des surveillances ordonnées – une disposition pénale sanctionnant la violation de l'obligation de conserver les données secondaires dans le domaine de la correspondance par télécommunication (art. 26, al. 5). Outre le fait que la sanction prévue à l'art. 292 CP n'est également pas assez sévère pour punir le comportement considéré, elle ne permet pas de réprimer un tel comportement. En effet, cet article trouve application lorsque des données existantes, dont la livraison est ordonnée par une autorité, ne sont pas livrées mais non lorsque des données ont déjà été détruites avant l'ordre de l'autorité ou lorsque des données n'ont pas du tout été collectées ou conservées. La disposition proposée doit, de manière cohérente, aussi s'appliquer à la violation de l'obligation de conserver les données secondaires dans le domaine de la correspondance par poste (art. 19, al. 4).

L'*al. 1, let. c* complète, après la procédure de consultation, les comportements mentionnés à l'al. 1 constituant des infractions. L'expérience démontre en effet que la sanction prévue dans le cas de figure faisant l'objet de cette lettre est nécessaire pour faire respecter les obligations considérées[67].

L'*al. 1, let. d* reprend en partie en substance les art. 12, al. 3 et 15, al. 7 de la LSCPT en vigueur. Cette disposition porte sur tous les faits qui concernent une surveillance de la correspondance par poste ou télécommunication, à savoir, en particulier, l'existence d'une surveillance ainsi que toutes les informations concernant cette surveillance – y compris les simples demandes fondées sur l'art. 15 – qui, sur la base de la LSCPT, sont échangées entre les personnes tombant dans le champ d'application de la loi, le service et les autorités[68]. La notion de «tiers» contenue à la *let. d* ne

66 Bernard Corboz, op. cit., n. 11 à 16 ad art. 292 CP
67 Thomas Hansjakob, op. cit. (note 11), n. 2 ad art. 19a OSCPT
68 Thomas Hansjakob, op. cit. (note 11), n. 26 ad art. 15 LSCPT.

vise pas les sous-traitants d'une personne obligée de collaborer qui doivent être informés des faits considérés afin que la surveillance en question puisse être exécutée. Contrairement à ce qui est le cas des art. 12, al. 3 et 15, al. 7 de l'actuelle LSCPT, la let. d ne fait pas des faits précités une composante du secret des postes et des télécommunications, au sens de l'art. 321ter CP. La *let. d* ne porte pas sur la divulgation à des tiers des données de contenu ou secondaires collectées dans le cadre d'une surveillance de la correspondance par poste ou télécommunication; ce comportement est saisi et puni par l'art. 321ter CP. Afin d'éviter des erreurs, il peut être indiqué pour le service de rendre les personnes tombant dans le champ d'application de la loi attentives aux conséquences pénales que pourrait avoir, en vertu de la *let. d*, la divulgation des faits et données précités.

Selon l'art. 105, al. 2, CP, applicable en vertu de l'art. 40, al. 1 et de l'art. 2, DPA, la tentative n'est punissable que dans les cas expressément prévus par la loi. L'*al. 2* contient une telle disposition. Au vu des conséquences que les comportements considérés peuvent avoir et à l'instar de ce qui vaut pour passablement de contraventions contenues dans le droit pénal accessoire et poursuivies et jugées selon le droit pénal administratif, la tentative portant sur ces comportements est digne d'être punie.

L'*al. 3* punit la commission par négligence des comportements considérés. Concernant les raisons qui plaident pour la punition de la négligence, voir par analogie ce qui a été dit ci-dessus concernant l'al. 2. L'amende maximale prévue à l'*al. 3* pour la commission par négligence des infractions est aussi supérieure au montant maximal de l'amende prévu à l'art. 106, al. 1 CP. Ce dernier montant est en effet dans certains cas également susceptible d'être trop bas en relation avec les conséquences négatives très importantes que les comportements réprimés peuvent avoir sur une enquête importante en cours. Pour le surplus, voir par analogie le commentaire de l'al. 1.

Art. 40 Juridiction

L'avant-projet envoyé en consultation (art. 32 AP-LSCPT) prévoyait que la poursuite et le jugement des infractions faisant l'objet de l'art. 39 incombent aux cantons, comme cela est en principe la règle, et non à une autorité administrative de la Confédération – en l'occurrence le service – ce qui excluait l'application de la DPA. Ceci a été à juste titre critiqué lors de la consultation. Le présent projet prévoit la solution inverse, ce qui est usuel dans le droit pénal accessoire.

Il découle de l'*al. 1* que la complicité est punissable. Ceci, sans qu'on doive le dire expressément, au vu du contenu de l'art. 5 DPA, applicable en vertu de l'art. 40 et des art. 1 et 2 DPA. Les art. 6 et 7 DPA (Infractions commises dans une entreprise par un mandataire, etc.) sont aussi applicables sans qu'on le dise expressément, également au vu de l'art. 40 et des art 1 et 2 DPA. La réglementation prévue aux art. 6 et 7 DPA remplace l'al. 4 de l'art. 31 de l'avant-projet envoyé en consultation. Cette réglementation est sensée, étant précisé que les «personnes» visées par la disposition pénale considérée sont avant tout les fournisseurs de services postaux et de télécommunication, leurs employés, leurs chefs et les entreprises elles-mêmes. En outre, la prescription de l'action pénale et de la peine pour les infractions mentionnées à l'art. 39 sont régies par l'art. 11 DPA, complété par l'art. 333, al. 6, let. b et e, CP tant que les délais y relatifs n'ont pas été adaptés aux nouveaux délais de prescription de la partie générale du CP. En vertu de ces articles, la prescription de

l'action pénale applicable à ces infractions est de 4 ans et la prescription de la peine est de 7½ ans.

Comme le prévoit l'*al. 2*, il est plus rationnel d'attribuer la compétence de poursuivre et juger les infractions au sens de l'art. 39 au service – qui devra s'organiser en conséquence – plutôt qu'aux cantons, comme cela était prévu dans l'avant-projet envoyé en consultation (art. 32 AP-LSCPT). Plusieurs arguments plaident en faveur de cette solution. Tout d'abord, le service est en général le mieux placé pour avoir connaissance des faits susceptibles de constituer une telle infraction. De plus, l'art. 39 sanctionne notamment le non-respect des injonctions du service lui-même. En outre, la LSCPT confère des tâches de surveillance administrative au service. Qui plus est, la poursuite et le jugement de ces infractions requièrent en principe des connaissances techniques spécifiques, que les autorités de poursuite pénale des cantons sont moins susceptibles de posséder que lui.

2.11 Section 11 Surveillance et voies de droit

Art. 41 Surveillance

Il importe de s'assurer que seules les personnes soumises à la LSCPT qui respectent la législation relative à la surveillance de la correspondance par poste et télécommunication puissent être actives sur le marché suisse. L'*art. 41*, relatif à la surveillance administrative des personnes soumises à la LSCPT, rendant l'art. 58 LTC en partie applicable par analogie, vise cet objectif. Il instaure un système de sanctions administratives, complémentaire au système des sanctions pénales prévues à l'art. 39 . Le service exerce ses compétences découlant de l'*art. 41* de manière contraignante à l'égard des personnes obligées de collaborer (art. 2). Il ne peut contraindre les autorités qui ordonnent des surveillances et celles habilitées à les autoriser, vu qu'il ne possède pas de compétence décisionnelle applicable à ces autorités (voir commentaire de l'art. 16, let. a et b).

L'*al. 1* est une norme analogue à l'art. 58, al. 1 LTC. C'est au service de jouer le rôle d'autorité de surveillance dans le domaine de la correspondance par poste et télécommunication, dès lors que c'est lui qui connaît le mieux la matière et les règles applicables.

L'*al. 2* est quant à lui une norme analogue à l'art. 58, al. 2, let. a, LTC. Il énumère les mesures que le service peut prendre lorsqu'il constate une violation du droit relatif à la surveillance de la correspondance par poste et télécommunication. Le cas échéant, cet article permet au service de prononcer des sommations pour que les personnes visées remédient aux manquements constatés ou des sommations prescrivant des mesures propres à prévenir toute récidive. Le destinataire de cette sommation devra informer le service des dispositions prises. La *phr. 2 de l'al. 2* est une norme analogue à l'art. 58, al. 5, LTC. En plus de prononcer les mesures précitées, le service peut agir au niveau pénal, en se fondant sur l'art. 40. Il sied de préciser que des mesures plus incisives que celles relevant de la compétence du service en vertu de l'*al. 2* pourront être prononcées, comme c'est le cas aujourd'hui, en cas de violation du droit relatif à la surveillance de la correspondance par poste et télécommunication. Il appartiendra au Département fédéral de l'environnement, des transports, de l'énergie et de la communication, en ce qui concerne la correspondan-

ce par poste, et à l'Office fédéral de la communication ainsi qu'à la Commission fédérale de la communication, en ce qui concerne la correspondance par télécommunication, de prendre ces mesures. Comme aujourd'hui, l'Office fédéral de la communication et la Commission fédérale de la communication pourront agir sur la base des art. 58 et 60 LTC et le service pourra informer ces autorités des violations qu'il a constatées afin de permettre à celles-ci de prendre, le cas échéant, les mesures précitées. Il n'est pas nécessaire de créer une disposition, s'inspirant de l'art. 58, al. 2, let. b, LTC, qui permette au service d'obliger un fournisseur de services de télécommunication à verser à la Confédération un montant correspondant à celui qu'il a épargné en n'exécutant pas la surveillance exigée ou en n'investissant pas pour satisfaire à ses obligations dans le domaine de la surveillance. Le fournisseur évite, en effet, une dépense dans ce cas mais n'obtient pas d'avantage financier, au sens de la disposition précitée. Le fournisseur devra toutefois verser au service un montant déterminé aux conditions de l'art. 34. En outre, l'art. 33, al. 5 permet au service d'enjoindre à ce fournisseur de prendre des mesures techniques et organisationnelles déterminées pour pallier ses manquements dans le domaine de la surveillance. Pour finir, le fournisseur considéré pourra être sanctionné pénalement en relation avec le non respect de l'injonction d'exécuter la surveillance ordonnée ou de celle visée à l'art. 33, al. 5 (art. 39, al. 1, let. a).

Art. 42 Voies de droit

Précisons d'emblée que l'*art. 42* ne concerne pas la voie de droit à la disposition des personnes ayant fait l'objet d'une surveillance de la correspondance par poste ou télécommunication ou aux personnes qui sont concernées par cette surveillance; cette voie de droit est régie par l'art. 279, al. 3, CPP ou 70*k* PPM. L'art. 279, al. 1, CPP règle en outre quels tiers surveillés doivent ultérieurement être informés; ce sont exclusivement des tiers au sens de l'art. 270, let. b, CPP. D'autres personnes concernées, par exemple des personnes qui ont communiqué avec la personne surveillée ou des personnes qui, dans le cadre d'une recherche par champ d'antennes ou lors du recours à un IMSI-catcher, sont inévitablement également saisies avant le filtrage des résultats de la surveillance, ne sont pas concernées par l'obligation de communication prévue à l'art. 279 CPP et n'ont pas de droit de recours au sens de l'al. 3 de la disposition précitée. Ceci est justifié, étant donné que ces personnes ne sont pas surveillées au sens de la loi. Les art. 269 à 279 CPP (en particulier les art. 269 à 269ter CPP dans leur version modifiée) règlent de manière exhaustive l'admissibilité d'une surveillance du point de vue de la procédure pénale. Ainsi, les résultats d'une surveillance (en temps réel ou rétroactive; contenus de communications ou données secondaires) ne peuvent par exemple pas être exploités sans l'autorisation d'un tribunal des mesures de contrainte (ou du Tribunal militaire de cassation); il est tout de suite mis fin à une surveillance non autorisée et les données recueillies sont détruites (art. 277 CPP).

Les personnes obligées de collaborer en vertu de la LSCPT (art. 2) ne sont concernées qu'indirectement par de telles questions relevant de la procédure pénale, dans la mesure où elles doivent exécuter ou tolérer une surveillance. La LSCPT n'a donc pas à se prononcer sur des aspects de procédure pénale mais doit assurer la mise en œuvre technique des surveillances admissibles du point de vue de la procédure pénale (sous réserve de la recherche en cas d'urgence et de la recherche de personnes condamnées). Ce n'est donc qu'en relation avec cet aspect technique et de droit administratif qu'il est nécessaire de régler ici les voies de droit des personnes tom-

bant dans le champ d'application de la LSCPT. Cette conception correspond au demeurant à l'avis de la doctrine et de la jurisprudence[69]. Les personnes qui tombent dans le champ d'application de la LSCPT ne peuvent ainsi pas faire valoir des griefs relevant de la procédure pénale dans le cadre d'un recours de droit administratif. L'admission d'un recours de droit administratif d'un fournisseur de services de télécommunication ne peut donc pas avoir pour conséquence qu'une surveillance autorisée par le tribunal des mesures de contrainte soit annulée mais ne peut qu'avoir pour conséquence que le fournisseur ne soit pas tenu d'exécuter lui-même une surveillance, dans le cas où il n'est pas en mesure de le faire pour des raisons techniques ou organisationnelles. Le fournisseur est toutefois obligé de tolérer la surveillance exécutée par le service ou des tiers (art. 26, al. 2) et de soutenir le service lors de l'exécution (art. 32, al. 2). La question des coûts, aussi, peut faire l'objet d'un recours de droit administratif (voir le commentaire de l'art. 38).

La distinction claire opérée entre le CPP et la LSCPT est sensée, au vu du fait que ces deux textes de loi – comme expliqué ci-dessus – ont des destinataires différents et cherchent à réglementer des objets différents (voir aussi le commentaire de l'art. 31). Ces domaines de réglementation distincts influencent directement aussi les voies de droit. La «dualité» des voies de droit est donc une conséquence de la séparation des aspects de droit administratif (LSCPT) et de procédure pénale (CPP), qui correspond aussi à l'exigence exprimée au chif. 2 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT).

L'*al. 1* concerne, au vu de ce qui précède, uniquement les voies de recours ouvertes aux personnes obligées de collaborer (art. 2) et aux autorités tenues de s'acquitter d'émoluments auprès du service contre les décisions de celui-ci.

La LSCPT actuelle ne contient pas de disposition régissant les voies de recours ouvertes aux personnes obligées de collaborer contre les décisions du service, en général (p.ex. en matière d'indemnités), et contre les décisions de celui-ci de faire exécuter une surveillance, fondée sur un ordre de surveillance donné par l'autorité compétente, en particulier. Seul l'art. 32 de l'actuelle OSCPT reconnaît le droit, pour ces personnes, de recourir contre une décision du service de faire exécuter une surveillance. Dans le cadre d'un tel recours, ces personnes ne peuvent toutefois – comme expliqué ci-dessus – invoquer que des questions d'ordre technique ou organisationnel liées à l'exécution de la mesure de surveillance qui leur est demandée. Pour des raisons de clarté et de sécurité juridique, le projet prévoit désormais une disposition régissant expressément les voies de recours ouvertes aux personnes soumises à la LSCPT contre les décisions rendues par le service.

Un grand nombre de participants à la procédure de consultation ont critiqué la réglementation proposée (art. 34 AP-LSCPT) aboutissant au fait que le recourant ne peut faire examiner par un tribunal la légalité de la décision de surveillance lui ayant été transmise par le service. Cet avis ne correspond toutefois pas à la réalité. D'une part, les décisions du service peuvent, dans la mesure où elles concernent la mise en œuvre technique et organisationnelle de l'ordre de surveillance, être contrôlées conformément aux dispositions générales de la procédure administrative fédérale.

69 Thomas Hansjakob, op. cit. (note 11), n. 3 ad art. 32 OSCPT; ATF **130** II 249, consid. 2.2.2 et 2.2.3. Voir aussi ATAF 2009/46, consid. 3.1.3, 3.2, 3.3 (non-entrée en matière sur le grief du fournisseur de services de télécommunication, selon lequel les droits de la personne surveillée seraient violés sans base légale).

D'autre part, la question de l'admissibilité sous l'angle de la procédure pénale de l'ordre de surveillance est examinée dans le cadre de la procédure pénale d'après les règles du droit de la procédure pénale. La conception selon laquelle le Tribunal administratif fédéral devrait également pouvoir contrôler l'admissibilité sous l'angle de la procédure pénale mettrait en danger durablement la sécurité juridique: une compétence parallèle aboutirait au fait que les décisions du tribunal des mesures de contrainte, qui se prononce sur des questions relevant de la procédure pénale, pourraient être révoquées sans respecter l'ordre des différentes instances et dans le cadre d'un «changement de voie de droit» non prévu par l'ordre juridique. Inversement, il serait imaginable qu'une décision du Tribunal administratif fédéral sur l'admissibilité de l'ordre de surveillance sous l'angle de la procédure pénale rende caduc un recours du prévenu fondé sur l'art. 279, al. 3, CPP et porte ainsi atteinte aux droits constitutionnels de celui-ci.

Au vu des règles générales de procédure applicables devant le Tribunal administratif fédéral, le recourant ne peut porter à l'examen de celui-ci que les questions de droit à la réponse desquelles il a un intérêt juridiquement protégé propre (art. 37 de la loi du 17 juin 2005 sur le Tribunal administratif fédéral [LTAF][70] en relation avec l'art. 48, al. 1, let. c, PA). Il s'ensuit que les personnes obligées de collaborer (art. 2), notamment les fournisseurs de services de télécommunication, n'auront de toute façon pas la qualité pour agir pour soulever des questions qui concernent la procédure pénale ou la protection des données des personnes communicantes. Un état de fait peut certes présenter aussi bien des questions de droit relevant du droit de la procédure pénale que du droit administratif (y compris le droit de la protection des données). Ainsi la question de savoir si un type de surveillance est admissible (p.ex. la recherche par champ d'antennes) concerne aussi bien le droit de la procédure pénale et de la protection des données (l'Etat peut-il surveiller les usagers de téléphones mobiles au moyen de la recherche par champ d'antennes?) que le rapport de droit administratif avec les fournisseurs de services de télécommunication (les fournisseurs de services de télécommunication doivent-il exécuter des recherches par champ d'antennes?). Ces questions ne doivent toutefois pas être mélangées, eu égard aux différents intérêts concernés et aux différentes questions qui se posent; les voies de droit doivent au contraire être prévues de manière nuancée.

La qualité pour recourir des personnes soumises à la LSCPT, en particulier des fournisseurs de services de télécommunication, est donc exclue pour tous les aspects de procédure pénale, étant donné qu'elles n'ont à cet égard pas d'intérêt juridiquement protégé. Ceci concerne, par exemple, la question de savoir si on est en présence de graves soupçons en vertu de l'art. 269, al. 1, let. a, CPP ou 70, al. 1, let. a, PPM ou si les conditions pour la surveillance du raccordement de télécommunication d'un tiers prévues à l'art. 270, let. b, CPP ou 70*a*, let. b, PPM son remplies. Ces questions n'ont qu'une incidence indirecte sur les fournisseurs de services de télécommunication.

L'*al. 2* ne fait en somme qu'exprimer explicitement ce qui a été exposé ci-dessus et vaut de toute façon en vertu des règles générales de procédure. Il est toutefois sensé de conserver cette disposition, car elle clarifie expressément un point important pour la pratique de la poursuite pénale et du droit administratif.

70 RS **173.32**

Considérant en particulier l'urgence dans laquelle une surveillance devrait être effectuée, l'*al. 3 phr. 1* prévoit, en dérogation de l'art. 55, al. 1 PA – lequel serait en principe applicable en vertu du renvoi effectué à l'art. 37 LTAF – que le recours n'a pas d'effet suspensif, sauf si la décision du service porte sur une prestation pécuniaire (p.ex. en matière d'indemnités ou d'émoluments), car il faut partir du principe qu'il n'y a pas d'urgence dans ce cas-là. Pour que le recours n'ait pas d'effet suspensif, il n'est donc pas nécessaire que le service le lui retire en application de l'art. 55, al. 2 PA. A l'instar de ce que prévoit l'art. 55, al. 3 PA, l'*al. 3 phr. 2* dispose toutefois que l'autorité de recours peut restituer l'effet suspensif au recours. Par ailleurs, un recours régi par la procédure pénale n'a en principe pas non plus d'effet suspensif (art. 387 CPP), puisque la surveillance a pour but d'obtenir des preuves, opération qui ne souffre en règle générale aucun retard.

2.12 Section 12 Dispositions finales

Art. 43 Exécution

L'*art. 43* prévoit la compétence du Conseil fédéral pour édicter la législation relative à l'exécution de la nouvelle LSCPT. Il prévoit également une telle compétence pour les cantons, qui renvoie en particulier à l'art. 37, al. 3.

Art. 44 Abrogation et modification du droit en vigueur

L'annexe à laquelle renvoie l'*art. 44* dispose en substance au ch. I que la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[71] est abrogée par l'entrée en vigueur de la nouvelle LSCPT. Celle-ci ne modifie en effet pas la LSCPT actuelle mais la remplace.

Le ch. II de l'annexe à laquelle renvoie l'*art. 44* mentionne les lois qui sont modifiées, sans être abrogées, par l'entrée en vigueur de la nouvelle LSCPT.

Art. 45 Dispositions transitoires

Les dispositions transitoires visent en principe à permettre au nouveau droit de se substituer le plus rapidement possible à l'ancien droit, afin de bénéficier le plus rapidement possible des avantages du nouveau droit, étant entendu que celui-ci est censé être meilleur que celui en vigueur. Ce sont les surveillances selon la présente loi (c'est-à-dire prévues à l'art. 269 CPP mais également régies par la LSCPT) et les recours portant sur des surveillances selon la présente loi qui sont visés par les dispositions considérées. On opère ainsi une délimitation avec les surveillances régies uniquement par le CPP (notamment celles au moyen d'IMSI-catchers [art. 269bis CPP] et de GovWare [art. 269ter CPP]) et les recours portant sur ces surveillances et faisant donc l'objet des dispositions transitoires prévues dans le CPP.

L'*al. 1* s'inspire de l'art. 448, al. 1, CPP, sans toutefois reprendre exactement la réglementation contenue dans celui-ci. Selon la réglementation proposée, on applique à l'exécution des surveillances le droit en vigueur au moment considéré. On

71 RO **2001** 3096, **2003** 2133 3043, **2004** 2149 3693, **2006** 2197 5437, **2007** 921 5437

n'appliquera donc pas le nouveau droit à un moment antérieur à son entrée en vigueur, même si la surveillance est encore en cours. Ainsi, on ne revient pas, avec l'entrée en vigueur de ce droit, sur ce qui a déjà été effectué. Bien entendu, dans le respect du principe de l'interdiction de la rétroactivité, le nouveau droit ne sera *a fortiori* pas applicable aux surveillances déjà exécutées au moment de son entrée en vigueur. Si une surveillance est en cours, le nouveau droit sera en revanche applicable dès son entrée en vigueur à la poursuite de la surveillance. Ceci permettra, sans compliquer de manière exagérée l'exécution de la surveillance en cours, de bénéficier à ce stade déjà des avantages du nouveau droit.

Quant à l'*al. 2*, il s'inspire de l'art. 453, al. 1, CPP, sans toutefois en reprendre exactement la réglementation. On applique en instance de recours le droit qui était applicable en première instance; ceci se justifie par le fait qu'on cherche à déterminer en instance de recours si le droit appliqué en première instance l'a été correctement.

L'*al. 3* concerne le passage de la durée de conservation des données secondaires postales et de télécommunication de 6 à 12 mois. Les données secondaires non encore atteintes par la limite de la durée de conservation de 6 mois, prévue par le droit en vigueur, au moment de l'entrée en vigueur de la nouvelle loi doivent, conformément à ce que prévoit le nouveau droit, être conservées pour une durée totale de 12 mois, ce depuis le début de leur conservation selon le droit en vigueur. *A contrario*, les données secondaires atteintes par la limite de conservation de 6 mois du droit en vigueur au moment de l'entrée en vigueur de la nouvelle loi ne doivent pas être conservées plus longtemps.

L'*al. 4* concerne la suppression du délai de deux ans – contenu dans la LSCPT actuelle – après l'ouverture de la relation commerciale durant lequel les renseignements en question doivent pouvoir être fournis. Les renseignements non encore atteints par la limite de 2 ans, prévue par l'ancien droit, au moment de l'entrée en vigueur de la nouvelle loi doivent, conformément au nouveau droit, pouvoir être fournis pour une durée indéterminée. *A contrario*, les renseignements atteints par la limite de 2 ans de l'ancien droit au moment de l'entrée en vigueur de la nouvelle loi n'ont plus à être fournis.

L'*al. 5* prévoit une règle simple: On applique en effet le droit en vigueur au moment où la surveillance a été ordonnée. Le moment où une surveillance (ayant déjà été ordonnée) a, le cas échéant, été prolongée ne joue par contre aucun rôle. Ce qui précède implique en particulier que les indemnités et les émoluments relatifs à une surveillance en cours au moment de l'entrée en vigueur de la nouvelle loi sont régis par l'ancien droit.

Art. 46 Référendum et entrée en vigueur

L'*art. 46* règle le référendum et l'entrée en vigueur.

Code de procédure pénale[72]

Art. 269, al. 2, let. a

L'expérience a montré que les instruments actuels – y compris la recherche en cas d'urgence (art. 35 P-LSCPT) – ne suffisent pas à localiser un enfant déplacé ou retenu illicitement. Une surveillance de la correspondance par poste et télécommunication, soit une mesure susceptible de contribuer à retrouver un enfant, ne peut être ordonnée, étant donné que l'enlèvement de mineur (art. 220 CP) ne figure pas dans le catalogue des infractions pour la poursuite desquelles une telle surveillance peut être ordonnée. Au vu de ce qui précède, il y a lieu de compléter l'*art. 269, al. 2, let. a,* CPP en y mentionnant l'art. 220 CP.

Art. 269bis (nouveau) Utilisation de dispositifs techniques spéciaux de surveillance de la correspondance par télécommunication

L'*art. 269bis* constitue une base légale expresse permettant au ministère public d'utiliser plus largement des dispositifs tels que les IMSI-catchers notamment afin d'identifier des appareils de communication mobiles et, partant, leurs utilisateurs. La notion d'appareils de communication mobiles ne comprend pas seulement les appareils de téléphonie mobile mais en particulier également les ordinateurs portables et les notebooks munis de cartes SIM pour la transmission de données par le réseau de téléphonie mobile. Cette base légale offre également la possibilité d'utiliser des IMSI-catchers pour écouter (et enregistrer) des communications et pour localiser ces appareils ou utilisateurs. Les autorités de poursuite pénales qui font aujourd'hui usage de ces dispositifs se fondent sur l'art. 280, let. a et c, CPP. Le complément précité relatif à l'identification est nécessaire pour la poursuite des infractions Il se justifie en outre du fait que l'identification considérée est une mesure qui touche moins fortement la sphère privée des utilisateurs en comparaison des mesures susmentionnées, légitimes, que constituent la localisation et l'écoute des conversations[73]. L'IMSI-catcher permet de simuler les effets d'une station de base d'un réseau de téléphonie mobile pour les appareils de téléphonie mobile qui se situent dans son champ. Cela a pour conséquence que ceux-ci s'annoncent à l'«IMSI-catcher» considéré et s'identifient auprès de lui comme ils le feraient auprès de n'importe quelle station de base d'un réseau de téléphonie mobile. Ceci est susceptible de permettre, sans aucune intervention de l'opérateur de téléphonie, d'identifier le numéro de la carte d'identification de l'usager utilisée (numéro SIM) ou le numéro d'identification international (numéro IMSI ou numéro IMEI), jusqu'ici inconnu, d'une personne donnée ou d'un équipement donné, de localiser les appareils dans cette zone et même d'écouter les conversations téléphoniques[74].

Un nombre relativement important de participants à la procédure de consultation, en particulier des cantons et des organisations en matière de poursuite pénale, s'est félicité de la création d'une base légale permettant l'utilisation de dispositifs tels que les IMSI-catchers dans le sens précité. Le Parti écologiste suisse ainsi que des organisations de protection des consommateurs de même que des organisations d'utilisateurs d'Internet, en particulier, y furent opposés. A l'appui de cette position, il a en

72 RS **312.0**
73 Sophie de Saussure, op. cit., n. 45 à 56 et 70.
74 Sylvain Métille, op. cit., n. 25.

particulier été prétendu que l'IMSI-catcher non seulement permet l'identification du téléphone mobile d'un usager déterminé mais encore détourne (et perturbe) les communications sur un réseau de téléphonie mobile de l'ensemble des personnes, suspectes ou non, se trouvant dans les parages de cet usager. S'est également posée la question de savoir si le classement systématique de la mesure de surveillance considérée était correct (art. 269 ss CPP ou art. 280 s. CPP).

Le classement systématique du recours à des dispositifs tels que les IMSI-catchers répond à l'exigence du ch. 2 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT) selon laquelle tout ce qui relève de la poursuite pénale doit en substance être biffé de la LSCPT. Du point de vue de la systématique, l'utilisation de dispositifs tels que les IMSI-catchers relève plus précisément des art. 269 ss CPP, et non des art. 280 s. CPP; ceci, même si l'utilisation de ce procédé de surveillance ne requiert en l'état actuel pas la collaboration d'un fournisseur de services de télécommunication et si le service n'a aucun rôle particulier à jouer en relation avec l'utilisation de ces dispositifs de surveillance (aucun ordre de surveillance n'a donc à lui parvenir). Il s'agit toutefois d'obtenir des données relevant de la correspondance par télécommunication, ce qui justifie d'insérer cette disposition à l'endroit précité[75].

Ce procédé de surveillance doit en particulier être distingué du type de surveillance que constitue la recherche par champ d'antennes, qui vise à obtenir des fournisseurs de services de télécommunication les données relatives aux appels de téléphonie mobile qui ont transité, durant un laps de temps déterminé, par leurs antennes desservant un lieu délimité par ses coordonnées géographiques et qui peuvent donc servir à déterminer le lieu où s'est trouvé, durant le laps de temps considéré, un téléphone portable et, partant, l'utilisateur de celui-ci. Il sied de préciser que les art. 269 à 279 CPP s'appliquent à l'usage de dispositifs techniques de surveillance au sens de l'art. 269bis CPP, sous réserve de dispositions contraires contenues dans cette disposition. Ceci implique en particulier que le recours à un IMSI-catcher ordonné par le ministère public doit être soumis à l'autorisation du tribunal des mesures de contrainte.

Il découle en particulier de la *let. a* que les infractions pour lesquelles une surveillance de la correspondance par télécommunication au moyen de dispositifs tels que les IMSI-catchers est possible sont les mêmes que celles pour lesquelles une surveillance classique, visée à l'art. 269 CPP, est admissible.

La *let. b* prévoit que les dispositifs tels que les IMSI-catchers, du fait de leurs caractéristiques techniques, en particulier du fait qu'ils sont susceptibles de perturber les télécommunications, doivent constituer des moyens de surveillance subsidiaires. Leur utilisation doit se limiter à combler les lacunes des méthodes classiques de surveillance disponibles actuellement; ils ne devraient en effet pas remplacer les moyens actuels de surveillance de la correspondance par télécommunication, au sens de l'art. 269 CPP[76].

75 Sophie de Saussure, op. cit., n. 16, 20 et 41 à 44; contra Sylvain Métille, op. cit., n. 26 et 40.

76 Sophie de Saussure, op. cit., n. 72.

Au vu du fait que ces dispositifs sont susceptibles de perturber les télécommunications, la let. c prévoit qu'on ne peut y avoir recours que si l'autorisation nécessaire pour ce faire a été donnée au préalable. Cette autorisation, délivrée par l'Office fédéral de la communication (OFCOM) – et non par le tribunal des mesures de contrainte –, se fonde sur les art. 32*a* et 34, al. 1ter LTC, sur l'art. 6, al. 4 de l'ordonnance du 14 juin 2002 sur les installations de télécommunication (OIT)[77] et sur les art. 49 ss de l'ordonnance du 9 mars 2007 sur la gestion des fréquences et les concessions de radiocommunication (OGC)[78]. Concrètement, pour obtenir cette autorisation, l'autorité qui souhaite utiliser un tel dispositif doit déposer une demande auprès de l'OFCOM. Cette demande doit contenir les paramètres techniques de l'équipement. L'office précité détermine si les conditions pour une autorisation sont remplies, en particulier si l'exploitation de l'appareil considéré ne portera pas atteinte de manière excessive, sous l'angle de l'efficacité des télécommunications, à d'autres intérêts publics ou aux intérêts de tiers. L'OFCOM évaluera donc le danger de perturbation des télécommunications, en particulier des réseaux de téléphonie mobile, induit par l'utilisation de l'appareil considéré[79]. Les autorisations de l'OFCOM sont octroyées à un utilisateur défini pour l'utilisation d'un certain nombre d'appareils d'un type défini. Une fois l'autorisation de l'OFCOM obtenue pour l'appareil considéré, celui-ci peut être utilisé dans le cadre de surveillances sans que cet office ne doive à chaque fois, pour chaque nouvelle surveillance, autoriser cet usage.

Art. 269ter (nouveau) Utilisation de programmes informatiques spéciaux de surveillance de la correspondance par télécommunication

L'*art. 269ter* vise à permettre au ministère public d'ordonner l'utilisation dans une procédure pénale, à des conditions strictes, de programmes informatiques spéciaux communément appelés Government Software (GovWare), c'est-à-dire l'introduction de ces programmes dans un système informatique, dans le but d'intercepter et de lire le contenu de communications et des données secondaires. La police s'en charge, sur ordre du ministère public. Ce procédé ne requiert donc pas la collaboration d'un fournisseur de services de télécommunication. Quant au service, il n'a aucun rôle particulier à jouer dans l'utilisation de GovWare, ce qui implique qu'aucun ordre de surveillance n'a à lui parvenir. Cette introduction a bien entendu lieu à l'insu du détenteur du système informatique considéré. Par «système informatique», on entend tout appareil permettant la correspondance par télécommunication, que ce soit par téléphonie ou non, comme les ordinateurs et les téléphones, portables ou fixes, ainsi que les tablettes numériques. L'utilisation du GovWare a lieu dans le cadre d'une procédure pénale; elle ne peut avoir lieu à titre préventif. Les GovWare sont souvent improprement appelés «chevaux de Troie». En effet, outre le fait que – à la différence du cheval de Troie – le GovWare est utilisé dans un but légal, à savoir lutter contre la criminalité, l'objectif n'est pas que le programme considéré se propage, contrairement à ce qui peut être le cas d'un cheval de Troie, mais de per-

77 RS **784.101.2**
78 RS **784.102.1**
79 Pour plus de détails concernant les perturbations susceptibles d'être causées par les IMSI-catchers et concernant les autorisations de l'OFCOM, voir Sophie de Saussure, op. cit., n. 57 à 59.

mettre au ministère public de surveiller un appareil considéré, respectivement une personne[80].

Le GovWare est en particulier utile pour lire des communications relevant de la téléphonie par Internet (voice over IP [VoIP]), plus précisément de la téléphonie par Internet du type peer-to-peer[81]; les données communiquées et interceptées dans ce contexte sont en effet cryptées et resteraient donc illisibles et inutilisables sans l'utilisation de GovWare. Ce mode de surveillance est également utile dans les cas où on ne pourrait, sans y avoir recours, intercepter une communication, même non cryptée. Tel est par exemple le cas lors de sessions de messagerie instantanée ouvertes depuis un ordinateur portable ou un téléphone portable avec diverses cartes SIM DATAS à prépaiement. Dans ces cas, seule l'implantation d'un programme dans l'ordinateur portable ou le téléphone portable permettra en effet d'intercepter la communication, même non cryptée.

Les GovWare permettent techniquement d'accéder à l'intégralité des informations privées (p.ex. documents, photos), soit des données potentiellement intimes, enregistrées dans un ordinateur. On ne doit toutefois pouvoir obtenir au moyen de GovWare que des données relevant de la correspondance susmentionnée (données acoustiques et optiques), dont fait partie la correspondance par Internet; les données relatives à la téléphonie par Internet et à la correspondance par e-mails présentent à cet égard un intérêt particulier (voir aussi commentaire de l'art. 1, al. 1 P-LSCPT). La limitation qui précède exclut juridiquement en particulier la perquisition en ligne d'un système informatique au moyen de GovWare.

Les opinions sont partagées sur le fait de savoir si l'art. 280 CPP, en particulier les let. a et b, permet l'utilisation de GovWare dans le sens précité[82]. La doctrine majoritaire estime toutefois que tel n'est pas le cas, étant entendu que certains auteurs estiment que cela ne serait possible que par une interprétation très extensive de l'art. 280 CPP. Le Tribunal fédéral n'a jusqu'à présent pas tranché cette question. Il importe à cet égard de préciser que des autorités de poursuite pénale (Confédération et cantons) ont, à de rares reprises, eu recours à des GovWare sur la base des dispositions de procédure pénale en vigueur avant l'entrée en vigueur du CPP, le 1er janvier 2011, en particulier sur la base de l'art. 66, al. 2 de la loi fédérale du 15 juin 1934 sur la procédure pénale ou des anciens codes de procédure cantonaux. La PJF, agissant sur mandant du MPC et après autorisation du Tribunal pénal fédéral, a en particulier eu recours à des GovWare dans quatre procédures, portant sur diverses catégories d'infractions. Ces dispositions se limitaient à permettre l'utilisation de dispositifs techniques de surveillance, sans donner beaucoup de précisions sur le but de leur utilisation. Elles permettaient cependant alors de fonder le recours à des GovWare, par une interprétation extensive de la notion de «dispositifs techniques de surveillance», allant toutefois moins loin que l'interprétation qui serait nécessaire pour fonder une telle surveillance sur l'art. 280 CPP. Dans le cadre des

80 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 3.

81 Voir Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 7 et Sylvain Métille, op. cit., n. 30.

82 Annegret Katzenstein in: Niggli/Heer/Wiprächtiger (éd.), Basler Kommentar, Schweizerische Strafprozessordnung, Bâle 2011, n. 16 ad art. 280 CPP; Thomas Hansjakob in: Donatsch/Hansjakob/Lieber (éd.), Kommentar zur Schweizerischen Strafprozessordnung, Zurich/Bâle/Genève, n. 2 ad art 280 CPP; Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 16 et 30; Sylvain Métille, op. cit., n. 37.

travaux d'élaboration du CPP, il avait toutefois été jugé que lesdites dispositions ne satisfaisaient pas à l'exigence de précision à laquelle doivent répondre les normes restreignant les droits fondamentaux, problème que l'on a cherché à pallier avec l'adoption de l'art. 280 CPP[83]. Au vu de ce qui précède, il apparaît nécessaire de créer une base légale expresse si l'on veut pouvoir avoir recours à des GovWare dans le sens précité. Ceci paraît d'autant plus indiqué qu'une telle base légale doit servir de fait justificatif légal (art. 14 CP) pour un comportement susceptible d'être saisi par l'art. 143bis CP (Accès indu à un système informatique).

Lors de la procédure de consultation relative à l'avant-projet de loi, les avis furent partagés sur le principe de prévoir, dans une disposition, la possibilité de recourir à des GovWare pour la surveillance de la correspondance par télécommunication. Passablement de cantons et d'organisations en matière de poursuite pénale se sont prononcés en faveur de cette possibilité. Le Parti écologiste suisse ainsi que des organisations de protection des consommateurs de même que des organisations d'utilisateurs d'Internet, en particulier, y furent opposés. Quant à la plupart des fournisseurs de services de télécommunication, comme beaucoup de personnes, ils furent très réservés. Se posait en particulier la question de savoir s'il fallait autoriser ce mode de surveillance, qui est incisif et est potentiellement susceptible de permettre de perquisitionner en ligne l'intégralité d'un ordinateur. Fut également exprimé l'avis selon lequel l'intégration de tels programmes dans des ordinateurs comporte des risques trop élevés pour la sécurité informatique (brèche dans le système de sécurité pouvant être utilisée par des criminels, «recyclage» du GovWare par des criminels pour un usage abusif, risques pour l'appareil du particulier qui héberge le GovWare, risques pour l'ensemble du réseau) ainsi que pour la fiabilité et l'intégrité des moyens de preuve (p.ex. modification d'un écrit par le GovWare). Il fut également prétendu que l'on ne peut savoir à l'avance comment interagiront le GovWare et les autres éléments du système informatique dans lequel il est implanté, ce qui peut provoquer la contamination par des logiciels nuisibles d'un nombre relativement important de systèmes informatiques en Suisse et à l'étranger et pose la question de la responsabilité (notamment de la Confédération) pour le dommage ainsi causé. L'efficacité de ce mode de surveillance fut également mise en doute. Il a en outre été prétendu que, au vu des caractéristiques de ce mode de surveillance, en particulier au vu de l'atteinte importante aux droit fondamentaux de la personne concernée qu'il implique, celui-ci ne devrait être utilisable qu'en relation avec une partie des infractions (les plus graves) mentionnées à l'art. 269 al. 2 CPP. La question de savoir si le classement systématique de cette mesure de surveillance était correct (art. 269 ss CPP ou art. 280 et 281 CPP) a également été posée.

De l'avis des spécialistes du domaine policier consultés, les craintes émises en relation avec les GovWare ne sont pas fondées. Le GovWare demeure en effet en permanence sous le contrôle des autorités de poursuite pénale (police, soumise au ministère public). Selon les circonstances, le GovWare est implanté dans l'appareil cible (ordinateur) par la police, sur ordre du ministère public, soit – de manière relativement simple – physiquement directement dans cet appareil, la police accédant alors aux locaux où se trouve celui-ci, soit – ce qui est plus compliqué à réaliser – à distance, par exemple par le biais de la messagerie électronique, ce qui peut nécessiter de déjouer l'intervention d'un antivirus. Le GovWare en question est

83 Message du 21 décembre 2005 relatif à l'unification du droit de la procédure pénale, FF **2006** 1234.

spécialement conçu et configuré pour l'ordinateur considéré, selon les ordres du ministère public, en fonction de ce que celui-ci souhaite obtenir comme types d'informations (p.ex. téléphonie par Internet, à l'exclusion des sites consultés ou des images obtenues au moyen de la caméra intégrée à l'ordinateur). Cette configuration sur mesure rend le recours à un GovWare difficile et particulièrement onéreux. L'engagement efficace et ciblé d'un Govware nécessite dans la règle au préalable l'exécution d'une surveillance de la correspondance par télécommunication dite classique, au sens de l'art. 269 CPP, ainsi qu'une analyse de l'environnement social de la personne cible (en particulier lorsque plusieurs personnes partagent la même connexion Internet, dans le but d'éviter de surveiller la correspondance par télécommunication d'une autre personne que la personne cible). Le GovWare peut donc exactement faire ce qu'on lui demande de faire, et pas plus. Il transmet les données obtenues sur un serveur utilisé par l'autorité de poursuite pénale, via le raccordement de la personne surveillée. La police, agissant sous le contrôle du ministère public, peut activer son fonctionnement, le prolonger avec l'autorisation judiciaire nécessaire délivrée par le tribunal des mesures de contrainte et le désactiver – pour le cas où sa désactivation automatique n'aurait pas été prévue –, tout ceci sans que le GovWare ne se propage. La police peut également, toujours agissant sous le contrôle du ministère public et avec l'autorisation du tribunal des mesures de contrainte, étendre une surveillance en cours à d'autres types de données que ceux initialement surveillés. Le fonctionnement du GovWare dépend donc de sa configuration. Il peut et doit être configuré de telle sorte qu'il ne permette que d'obtenir les données de correspondance par télécommunication, sans permettre d'accéder à l'ensemble des données contenues dans l'ordinateur considéré, ce qui exclut qu'une perquisition en ligne de cet ordinateur puisse être exécutée. Une entreprise externe qui aurait configuré le GovWare n'est de ce simple fait pas encore en mesure d'accéder aux données obtenues lors de la surveillance. De même, la personne possédant le serveur utilisé par l'autorité de poursuite pénale pour l'exécution d'une surveillance au moyen d'un GovWare n'est pas en mesure de lire les données obtenues; elle ne serait en effet qu'en mesure de constater le transfert de celles-ci. Les caractéristiques du GovWare, en particulier le fait qu'il est élaboré sur mesure pour l'appareil cible et que son usage est limité dans le temps, impliquent qu'il pourrait très difficilement être copié dans cet appareil et intégré dans un autre. Détourner un GovWare de la sorte nécessiterait en effet beaucoup de connaissances et de temps. Il serait en outre beaucoup plus simple pour une personne malveillante de se procurer, pour une somme très modique, un cheval de Troie sur le marché. Le recours à un GovWare ne représente en outre pas un risque pour les réseaux, étant donné qu'il n'implique pas de manipuler des composantes de ceux-ci.

Les spécialistes du monde scientifique contactés arrivent à la conclusion qu'il n'est pas possible de produire et de maintenir en activité des GovWare qui vont fonctionner correctement en toutes circonstances, c'est-à-dire sans influencer d'autres programmes ou fonctions, en précisant toutefois que les expériences menées montrent qu'il est possible d'utiliser de tels programmes sans que des dommages constatables immédiatement ne se produisent. Le recours au programme utilisé par les autorités de poursuite pénale ne peut probablement pas (encore) techniquement être limité à la seule surveillance de la communication: La porte dérobée ouverte par le GovWare permet techniquement aux enquêteurs d'accéder à toutes les données et informations contenues dans l'ordinateur considéré; n'importe quelle donnée relative au système et à l'utilisateur peut être copiée, modifiée, effacée ou ajoutée à l'insu du détenteur.

Cette porte dérobée mène en outre à un point faible dans le système de l'ordinateur, qui peut aussi être utilisée par des tiers[84].

Afin d'atteindre le but premier que vise la révision de la LSCPT, qui consiste non pas à surveiller plus qu'actuellement mais à adapter les méthodes de surveillance à l'évolution technique dans le domaine des télécommunications, il est de l'avis du Conseil fédéral indispensable de permettre l'utilisation par les autorités de poursuite pénale de GovWare. En décider autrement affaiblirait très notablement l'efficacité de la lutte contre la criminalité. Un cryptage ne pouvant être supprimé par les fournisseurs de services de télécommunication empêche en effet la surveillance de la correspondance par télécommunication au moyen de mesures de surveillance dites classiques puisque les données ainsi obtenues sont illisibles. Ce cryptage est aujourd'hui déjà utilisé en particulier dans le domaine de la téléphonie par Internet, qui est déjà très répandue et se développe encore, au détriment de la téléphonie classique. Beaucoup de délinquants connaissent ces failles en matière de surveillance liées à la téléphonie par Internet et recourent à celle-ci en connaissance de cause. Les GovWare sont susceptibles de permettre de pallier le problème précité; en effet, au lieu de dévier les données au cours de leur transmission – comme c'est le cas avec les mesures de surveillance de la correspondance par télécommunication classiques – le GovWare permet de tenter d'intercepter les données à la source, avant qu'elles ne soient cryptées[85]. En outre, avec l'arrivée progressive ces prochaines années des nouvelles ressources d'adressage que constituent les adresses IPv6, la surveillance de la correspondance par Internet, dont fait partie la téléphonie par Internet, deviendra de plus en plus difficile, voire impossible à réaliser avec les mesures de surveillance de la correspondance par télécommunication classiques, visées à l'art. 269 CPP. En effet, ce nouveau système facilite l'utilisation de protocoles de cryptage tels que IPSec. En outre, il existe actuellement une tendance accrue à communiquer de manière cryptée (p.ex. https). Il résulte de ce qui précède que le cryptage va nettement se répandre. Le recours à des GovWare est susceptible de permettre d'éviter que la surveillance ne soit contournée par l'usage d'Internet et le recours au cryptage de données. Au vu de ce qui précède, renoncer à permettre aux autorités de poursuite pénale de recourir à des GovWare reviendrait à empêcher de manière très importante la surveillance de la téléphonie par Internet et, de manière générale, la surveillance de la correspondance par Internet. Des mesures de surveillance de la correspondance par Internet qui sont aujourd'hui techniquement peut-être encore possibles seraient à l'avenir empêchées. Ceci serait toutefois clairement contraire au but susmentionné de la révision de la LSCPT en cours.

C'est en considération de ce qui précède, après une pondération des divers intérêts en présence, que le Conseil fédéral a décidé de proposer dans le présent projet une base légale expresse permettant l'utilisation de GovWare par les autorités de poursuite pénale. Il est proposé de ne permettre le recours à des GovWare qu'en relation avec les infractions énumérées dans la liste de l'art. 286, al. 2 CPP et non pour toutes celles mentionnées dans la liste de l'art. 269, al. 2 CPP, applicable aux surveillances classiques de la correspondance par télécommunication (voir al. 1, let. b et commentaire y relatif). Il est de plus proposé que l'usage de GovWare soit subsidiaire aux

84 Sabine Gless, Strafverfolgung im Internet, Revue Pénale Suisse, vol. 130 (2012), p. 12, 17 s.; Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5. 12. 2011, n. 2s. (en particulier note de bas de page 5) et 10.

85 Pour les détails, voir Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 5 à 9.

mesures classiques de surveillance de la correspondance par télécommunication, le principe de la proportionnalité demeurant réservé (voir al. 1, let. c et commentaire y relatif). La limitation de la surveillance à des données de communication doit être juridiquement assurée. Les règles proposées visent à le garantir, en mentionnant le «contenu des communications et les données secondaires de télécommunication …» comme champ d'application matériel des GovWare; la perquisition en ligne est interdite[86]. Est également exclue l'utilisation au moyen d'un GovWare de la caméra ou du micro d'un ordinateur dans un autre but que la surveillance de la correspondance par télécommunication (voir al. 3 et commentaire y relatif). De fortes garanties légales permettent de protéger toute personne concernée contre les abus potentiels découlant du recours à des Govware. Il est en effet prévu d'exiger une autorisation de l'autorité compétente pour autoriser les surveillances ordonnées (tribunal des mesures de contrainte) pour recourir à des GovWare (art. 274 CPP). De plus, les informations qui auraient pu être obtenues en violation des limites applicables, par exemple dans le cadre d'une perquisition en ligne, et non en relation avec des données relevant exclusivement de la correspondance par télécommunication, ne peuvent en aucun cas être exploitées comme moyens de preuve et doivent être détruites (al. 3 et art. 141, al. 1 et 277 CPP). La personne concernée pourra en outre interjeter recours contre la surveillance au moyen de GovWare ordonnée à son encontre (art. 279 CPP).

Le recours à des GovWare dans le sens expliqué ci-dessus est préférable aux alternatives théoriquement envisageables susceptibles de permettre d'atteindre le même but. On pourrait prévoir l'obligation de fournisseurs de services Internet permettant la téléphonie par Internet de livrer aux autorités de poursuite pénale, par l'intermédiaire du service, les données, en particulier de communication, des personnes qui ont recours à son programme pour communiquer téléphoniquement par Internet, en faisant une analogie avec l'obligation qui incombe aux fournisseurs de services de télécommunication. Mais une telle obligation serait extrêmement difficile, voire impossible, à mettre en œuvre. Elle ne tiendrait en effet en particulier pas compte de ce qu'offrent certains de ces fournisseurs de services Internet, c'est-à-dire en principe un programme, téléchargeable gratuitement depuis Internet, permettant de téléphoner (de manière cryptée) par Internet, au moyen de liaisons d'ordinateurs à ordinateurs (peer-to-peer), sans passer par une centrale qui serait exploitée par le fournisseur de services Internet, ce qui implique que celui-ci n'est pas en possession des données précitées et ne peut donc pas les livrer aux autorités de poursuite pénale. Cette obligation ne tiendrait en outre pas compte du fait que ce genre de fournisseurs de services Internet ont dans la grande majorité des cas leur siège à l'étranger, ce qui rendrait sa portée illusoire. Une autre alternative au recours à des GovWare serait d'obliger toutes les entreprises qui permettent de crypter la correspondance par télécommunication à livrer leurs clefs de cryptage, afin que l'on puisse décrypter cette correspondance. Cette obligation ne tiendrait pas compte du fait que ce genre de fournisseurs de services Internet aussi ont dans la grande majorité des cas leur siège à l'étranger, ce qui rendrait également sa portée illusoire.

Le fait de régler l'usage de GovWare dans le CPP et non dans la LSCPT répond à l'exigence du ch. 2 des motions Schmid-Federer 10.3831 (Révision de la LSCPT), Eichenberger 10.3876 (Révision de la LSCPT) et (von Rotz) Schwander 10.3877 (Révision de la LSCPT), selon laquelle tout ce qui relève de la poursuite pénale doit

86 Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 21.

en substance être biffé de la LSCPT. Concernant l'emplacement du CPP qui doit, du point de vue de la systématique, accueillir cette réglementation, deux sections entrent en considération: celle concernant la «surveillance de la correspondance par poste et télécommunication» (art. 269 ss CPP) et celle relative aux «autres mesures techniques de surveillance» (art. 280 s. CPP). Il y a à cet égard lieu de considérer ce qui suit: en recourant à un GovWare, on pénètre dans un système informatique (ordinateur) et on le manipule, ce qui n'est pas le cas avec les mesures de surveillance prévues à l'art. 269 CPP, avec lesquelles on se contente de «dévier» des données lors de leur transmission ou d'aller les chercher chez un fournisseur de services (de télécommunication). Le recours à un GovWare ne requiert en outre pas la collaboration d'un fournisseur de services de télécommunication et le service n'a aucun rôle particulier à jouer dans ce contexte. La base légale permettant le recours à des GovWare doit tout de même, du point de vue de la systématique, être intégrée dans les art. 269 ss CPP, et non dans les art. 280 s. CPP. Ce, au vu du fait que leur usage doit exclusivement être limité à la surveillance de la correspondance par télécommunication, et ne doit pas, par exemple, permettre la surveillance d'une pièce au moyen de la caméra intégrée à l'ordinateur. Il sied de préciser que les art. 269 à 279 CPP s'appliquent à l'usage de GovWare au sens de l'art. 269ter CPP, sous réserve de dispositions contraires contenues dans cette disposition.

L'*al. 1, let. a* ne renvoie pas à l'art. 269, al. 2 CPP, étant donné que les infractions pour lesquelles une surveillance de la correspondance par télécommunication au moyen de GovWare est possible sont différentes de celles pour lesquelles une surveillance classique, visée à l'art. 269 CPP, est admissible (voir let. b et commentaire y relatif).

Au vu des caractéristiques susmentionnées que présente l'utilisation de GovWare, notamment de la nature particulièrement intrusive de ce mode de surveillance, il est, partant des critiques formulées durant la procédure de consultation, proposé ce qui suit: contrairement à ce que prévoyait l'avant-projet, le recours aux GovWare ne doit être permis que pour les infractions mentionnées dans la liste de l'art. 286, al. 2, CPP, applicable à l'investigation secrète, et non pour toutes celles mentionnées dans la liste, plus importante, de l'art. 269, al. 2, CPP, applicable aux surveillances classiques de la correspondance par poste et télécommunication. Cette restriction, formulée à l'*al. 1, let. b*, n'est toutefois pas incontestée. En particulier, il est en substance allégué que, lorsque le recours à un GovWare s'avère nécessaire, ce n'est pas par cette limitation que l'on devrait tenir compte du fait que la gravité de l'atteinte aux droits fondamentaux de la personne concernée est plus importante lorsque l'on procède à une surveillance au moyen d'un GovWare et non au moyen du procédé conventionnel, c'est-à-dire par le truchement d'un fournisseur de services de télécommunication selon les art. 269 ss CPP; il est en effet prétendu[87] qu'on devrait en revanche en tenir compte lors de l'application du principe de la proportionnalité, en vertu de l'art. 269, al. 1, let. b CPP. La limitation susmentionnée implique en particulier que si, dans le cadre d'une surveillance effectuée au moyen de GovWare, des informations concernant des infractions figurant dans le catalogue de l'art. 269, al. 2, CPP mais non dans celui de l'art 286, al. 2, CPP sont recueillies, ces informations ne pourront être exploitées (art. 141, al. 1 et 278 CPP).

87 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 25.

Toujours au vu des caractéristiques susmentionnées du recours à des GovWare, l'*al. 1, let. c* dispose que l'usage de GovWare est subsidiaire aux mesures classiques de surveillance de la correspondance par télécommunication visées à l'art. 269 CPP, étant entendu que celles-ci sont déjà subsidiaires par rapport aux mesures d'instruction dites classiques (art. 269, al. 1, let. c, CPP). Le principe de la proportionnalité demeure bien entendu réservé (art. 269, al. 1, CPP). Ce qui précède permet de garantir que ce procédé de surveillance ne sera utilisé que si cela est vraiment nécessaire. Il importe pour le surplus de préciser que la cherté de l'élaboration d'un GovWare et de l'exploitation des données obtenues au moyen de celui-ci ainsi que les difficultés liées à sa mise en œuvre efficace sont de nature à en limiter l'usage et à en faire ainsi dans les faits un moyen subsidiaire de surveillance de la correspondance par télécommunication. Il sied dans ce contexte de rappeler qu'une mesure classique de surveillance de la correspondance par télécommunication est, en principe, au préalable nécessaire pour permettre l'engagement efficace d'un GovWare.

L'obligation du ministère public, découlant de l'*al. 2, let. a*, d'indiquer dans son ordre de surveillance quel type de données il souhaite obtenir contribue à permettre le contrôle (par le tribunal des mesures de contrainte) du respect de l'interdiction de chercher à obtenir d'autres données que celles relevant exclusivement de la correspondance par télécommunication[88], en particulier par une perquisition en ligne (voir al. 3 et commentaire y relatif).

Quant à l'obligation du ministère public, découlant de l'*al. 2, let. b*, d'indiquer aussi dans son ordre de surveillance s'il est nécessaire de pénétrer dans un local qui n'est pas public pour l'introduction de programmes informatiques dans le système informatique considéré, elle a pour but de rendre le tribunal des mesures de contrainte attentif à cette modalité d'exécution, afin qu'il puisse, cas échéant, l'autoriser expressément conformément à l'art. 274, al. 4, let. c, CPP (voir aussi commentaire de l'art. 274, al. 4, let. c CPP).

L'*al. 3* exclut en particulier d'exploiter des preuves obtenues lors de la perquisition en ligne au moyen d'un GovWare d'un système informatique, laquelle permet d'accéder à l'intégralité des données, potentiellement intimes, contenues dans celui-ci. Est également exclue l'exploitation des preuves obtenues par l'utilisation au moyen d'un GovWare de la caméra ou du micro d'un ordinateur dans un autre but que la surveillance de la correspondance par télécommunication, par exemple pour surveiller une pièce. Les GovWare ne peuvent effet, selon l'al. 1, être utilisés que dans le but d'obtenir des données relevant de la correspondance par télécommunication. Une perquisition en ligne semble en somme déjà exclue au vu de l'art. 247 CPP, selon lequel la personne concernée doit être au courant de la perquisition, étant entendu que le recours à un GovWare n'a de sens que s'il a lieu à l'insu de la personne. L'obligation du ministère public, découlant de l'al. 2, let. a, d'indiquer dans son ordre de surveillance quel type de données il souhaite obtenir contribue à permettre de contrôler le respect de l'interdiction de chercher à obtenir d'autres données que celles relevant exclusivement de la correspondance par télécommunication, en particulier par une perquisition en ligne[89]. Les données qui auraient été obtenues en violation de cette interdiction sont inexploitables (art. 141, al. 1, et 277 CPP)[90].

88 Sylvain Métille, op. cit., n. 33 et 38

89 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 21; Sylvain Métille, op. cit., n. 35 et 40.

90 Sylvain Métille, op. cit., n. 33 et 38.

Le postulat de la Commission des affaires juridiques du Conseil national 11.4042 (Surveillance au moyen de chevaux de Troie [1]) charge en substance le Conseil fédéral d'examiner la nécessité d'adapter la réglementation relative au recours à des GovWare et de présenter un rapport à ce sujet. Quant au postulat de la Commission des affaires juridiques du Conseil national 11.4043 (Surveillance au moyen de chevaux de Troie [2]), il invite en substance le Conseil fédéral à établir un rapport sur le recours aux instruments de surveillance électronique, en particulier aux chevaux de Troie, et sur les bases légales et conditions générales y relatives. Ce rapport doit traiter de la situation au niveau fédéral et, si possible, cantonal. Les considérations exposées plus haut donnent notamment suite aux demandes formulées dans ces postulats.

Art. 270, phrase introductive et let. b, ch. 1

Des adaptations terminologiques sont effectuées dans la *phrase introductive* et dans la *let. b, ch. 1*, en conformité avec les notions nouvellement utilisées dans le projet de LSCPT. La notion de «raccordement» est ainsi – selon le contexte – remplacée par la notion de «service» ou la notion de «correspondance» (voir le commentaire de l'art. 17 P-LSCPT).

Le texte en français en vigueur ne couvre que la réception d'envois et de communications par le prévenu au moyen de l'adresse postale ou du service de télécommunication du tiers. Ce texte est trop restrictif; il doit également permettre de saisir le comportement du prévenu qui consiste à émettre des envois et des communications au moyen de l'adresse postale ou du raccordement de télécommunication d'un tiers, à l'instar de ce que permettent les textes en allemand et en italien. Le texte en français a donc été adapté en conséquence.

Art. 271

L'*art. 271* est précisé et complété.

Il est proposé de ne pas maintenir la version de l'*al. 1* envoyée en consultation et de conserver sa formulation en vigueur, toutefois complétée (cf. ci-dessous). Celle-ci est en effet claire, alors que celle envoyée en consultation pouvait laisser penser que même l'évaluation des données qui n'ont pas été écartées en vertu du tri ne peut être effectuée par les autorités de poursuite pénale. Le tri pourra avoir lieu, sous la direction d'un tribunal, moyennant l'utilisation de mesures techniques permettant, par exemple, de ne conserver que les correspondances passées avec des correspondants ou des raccordements sélectionnés. Il n'y a aucune raison de conserver dans le dossier des informations sans lien avec l'enquête et soumises au secret professionnel. L'*al. 1* doit donc être complété et prévoir, à l'instar de ce qui est le cas à l'al. 3, la destruction de ces informations et l'interdiction de les exploiter.

L'*al. 2* s'inspire de l'al. 2 en vigueur. Il explique toutefois le cas de figure visé par celui-ci de manière plus logique, dès lors que l'*al. 2* doit être considéré comme exception par rapport à l'al. 1, qui pose le principe de la nécessité d'effectuer le tri des informations recueillies dans le cadre d'une surveillance. Lorsque les conditions cumulatives de l'al. 2 sont remplies, le tri mentionné à l'al. 1 ne doit pas avoir lieu. Ceci implique que, dans ce cas de figure, d'une part, les autorités de poursuite pénale peuvent accéder directement aux informations recueillies dans le cadre de la surveillance effectuée et que, d'autre part, la surveillance considérée peut être exécu-

tée par branchement direct. Les caractéristiques du branchement direct – qu'il ne faut pas confondre avec la surveillance en temps réel – rendent en effet matériellement impossible le tri visé à l'al. 1. Pour le surplus, voir l'art. 17, let. c P-LSCPT et le commentaire y relatif. Rappelons qu'en vertu de l'*al. 2, let. a*, le branchement direct n'est possible que lorsque le détenteur du secret professionnel fait l'objet d'une surveillance en tant que prévenu, et non lorsqu'il en est l'objet en tant que tiers, au sens de l'art. 270, let. b CPP. Conformément à ce qui a été prétendu à juste titre lors de la procédure de consultation, l'intérêt des clients, patients, etc. à ce que le secret professionnel soit protégé existe également dans l'hypothèse de l'*al. 2*, comme dans celles des al. 1 et 3. Etant donné que le cas de figure faisant l'objet de l'*al. 2* est un cas particulier de l'hypothèse visée à l'al. 1, les informations sans lien avec l'enquête et soumises au secret professionnel ne doivent pas être conservées dans le dossier; elles doivent être détruites et leur exploitation interdite, conformément à ce que prévoit l'al. 1.

L'*al. 3* est complété, de manière à mieux refléter ce qui se passe dans la réalité. A l'instar de ce que prévoit l'al. 1, il y a lieu d'éviter que les autorités de poursuite pénale aient connaissance d'informations couvertes par le secret professionnel. Le tri devant être effectué sous la direction d'un tribunal porte exclusivement sur des informations issues d'envois et de communications avec les personnes mentionnées aux art. 170 à 173 CPP. Les informations relevant de communications avec des personnes ne revêtant pas cette qualité ne doivent pas faire l'objet de ce tri[91].

Art. 272, al. 2, 1re phrase, et 3

Des adaptations terminologiques y ont été apportées; voir le commentaire de l'art. 270, phrase introductive et let. b, ch. 1.

Art. 273 Identification des usagers, localisation et caractéristiques techniques de la correspondance

Le *titre* de cette disposition a été modifié, de manière à être en adéquation avec son contenu.

La notion de données secondaires contenue à l'*al. 1* est simplifiée par rapport à celle en vigueur, sans que cela ne change son contenu matériel (voir le commentaire des art. 19, al. 1, let. b et 26, al. 1, let. b, P-LSCPT). Relevons que l'information relative à la durée de la correspondance («combien de temps») n'a de portée que pour la correspondance par télécommunication, et non pour celle par poste (voir le contenu de l'art. 19, al. 1, let. b P-LSCPT).

La période sur laquelle les données secondaires peuvent être demandées avec effet rétroactif, au sens de l'*al. 3*, passe de six à douze mois. Cette augmentation vise une poursuite plus efficace des infractions. Elle a pour corollaire l'allongement de la durée de conservation des données secondaires (art. 19, al. 4 et art. 26, al. 5, P-LSCPT). Pour le surplus, voir le commentaire des art. 19, al. 4 et 26, al. 5, P-LSCPT.

91 Laurence Aellen/Frédéric Hainard, Secret professionnel et surveillance des télécommunications, Jusletter 23.3.2009, n. 21 ss; Nathalie Zufferey/Jean-Luc Bacher, Commentaire romand: Code de procédure pénale suisse, Bâle 2011, n. 18 ad art. 271 CPP.

Art. 274, al. 4

L'*art. 274, al. 4, let. a* est adapté aux modifications effectuées à l'art. 271.

L'autorisation expresse prévue à l'*art. 274, al. 4, let. b* se justifie au vu du caractère particulièrement intrusif que constitue le fait de pénétrer dans un local qui n'est pas public, à l'insu de la personne concernée, pour introduire un GovWare dans le système informatique (p.ex. ordinateur) qui s'y trouve. Or l'introduction du GovWare dans un système informatique peut aussi être effectuée à distance, par exemple par le biais de la messagerie électronique (voir aussi commentaire de l'art. 269ter). Pour que le tribunal des mesures de contrainte soit rendu attentif à cette modalité d'exécution, le ministère public sera tenu de l'indiquer conformément à l'art. 269ter, al. 2, let. b (voir aussi commentaire de l'art. 269ter, al. 2, let. b).

Art. 278, al. 1bis

Le renvoi figurant à l'*art. 278, al. 1bis* est modifié et complété. Le renvoi à l'art. 3 de la LSCPT actuelle est remplacé par le renvoi à l'art. 35 P-LSCPT. Il y a également lieu d'opérer un renvoi à l'art. 36 P-LSCPT, dès lors que cet article ne vise pas, à l'instar de l'art. 35 P-LSCPT, une procédure pénale en cours (voir commentaire de l'art. 36 P-LSCPT) et que des découvertes fortuites peuvent également avoir lieu dans une situation visée par cet article.

Art. 279, al. 3, 1re phrase

Des adaptations terminologiques y ont été apportées; voir le commentaire de l'art. 270, phrase introductive et let. b, ch. 1.

Procédure pénale militaire du 23 mars 1979[92]

Art. 70bis (nouveau) Utilisation de dispositifs techniques spéciaux de surveillance de la correspondance par télécommunication

Voir, par analogie, le commentaire relatif à l'art. 269bis CPP.

Art. 70ter (nouveau) Utilisation de programmes informatiques spéciaux de surveillance de la correspondance par télécommunication

Voir, par analogie, le commentaire relatif à l'art. 269ter CPP, sauf pour ce qui concerne l'al. 1 let. b, concernant la limitation du catalogue des infractions (et les motifs y relatifs). En effet, conformément au renvoi contenu à l'art. 73*a*, al. 1, let. a, PPM, le catalogue applicable à l'investigation secrète est en principe le même que celui qui vaut pour la surveillance de la correspondance par poste et télécommunication, l'art. 73*a*, al. 2, PPM – dont le renvoi à l'art. 286, al. 2, CPP doit, pour des raisons de cohérence, être repris à l'*al. 2bis* – étant toutefois réservé.

92 RS **322.1**

Art. 70a, phrase introductive et let. b, ch. 1

Le commentaire relatif à l'art. 270, phrase introductive et let. b, ch. 1, CPP s'applique par analogie à l'*art. 70a, phrase introductive et let. b, ch. 1*.

Art. 70b

L'*art. 70b* est précisé et complété.

Il est proposé de ne pas maintenir la version de l'*al. 1* envoyée en consultation et de conserver la formulation actuelle, toutefois complétée (cf. ci-dessous). Celle-ci est en effet claire, alors que celle envoyée en consultation pourrait laisser penser que même l'évaluation des données qui n'ont pas été écartées en vertu du tri ne peut être effectuée par le juge d'instruction. Le tri pourra avoir lieu, sous la direction du président du tribunal militaire, moyennant l'utilisation de mesures techniques permettant, par exemple, de ne conserver que les correspondances passées avec des correspondants, respectivement des raccordements sélectionnés. Il n'y a aucune raison de conserver dans le dossier des informations sans lien avec l'enquête et soumises au secret professionnel. L'*al. 1* est donc complété et prévoit, à l'instar de ce qui est le cas à l'al. 3, la destruction de ces informations et l'interdiction de les exploiter.

Le commentaire relatif à l'art. 271, al. 2, CPP s'applique par analogie à l'*art. 70b, al. 2*.

Le commentaire relatif à l'art. 271, al. 3, CPP s'applique par analogie à l'*art. 70b, al. 3*.

Pour le surplus, le renvoi à l'art. 75, let. a et c contenu à l'*art. 70b, al. 3* est remplacé par un renvoi à l'art. 75, let. b, dès lors que c'est à cet article que correspondent les art. 170 à 173 CPP, mentionnés dans l'article 271 de ce même code, et qu'il y a lieu de prévoir un parallélisme entre cet article-ci et l'*art. 70b*.

Art. 70c, al. 2, 1re phrase, et 3

Des adaptations terminologiques y sont effectuées; voir le commentaire de l'art. 70*a*, phrase introductive et let. b, ch. 1.

Art. 70d Identification des usagers, localisation et caractéristiques techniques de la correspondance

Le commentaire relatif à l'art. 273, titre et al. 1 et 3, CPP *s'applique* par analogie à l'*art. 70d, titre et al. 1 et 3*.

Art. 70e, al. 4

Voir, par analogie, le commentaire relatif à l'art. 274, al. 4, CPP.

Art. 70k Recours

Des adaptations terminologiques y ont été apportées; voir le commentaire de l'art. 70*a*, phrase introductive et let. b, ch. 1.

Loi du 30 avril 1997 sur les télécommunications[93]

Art. 6a (nouveau) Blocage de l'accès aux services de télécommunication

L'*art. 6a* prévoit expressément l'obligation pour les fournisseurs de services de télécommunication de bloquer l'accès à la téléphonie et à Internet, aux conditions mentionnées. Ceci évite de devoir fonder cette obligation sur une interprétation extensive de l'art. 21 P-LSCPT. Cette obligation a pour but de contribuer à identifier les personnes qui accèdent à la téléphonie ou à Internet sans avoir souscrit d'abonnement, au moyen, par exemple, de cartes SIM à prépaiement, de cartes «wireless» à prépaiement et de moyens permettant l'accès à un réseau de téléphonie fixe. C'est en particulier sur la base des informations obtenues des autorités pénales, notamment des autorités de poursuite pénale, que les fournisseurs de services de télécommunication devront procéder au blocage. Il n'appartient pas au service de contacter l'OFCOM ou ces fournisseurs afin que ceux-ci procèdent à ce blocage. Les autorités pénales annonceront toutefois au service l'état de fait impliquant un tel blocage, afin que celui-ci puisse contrôler si les fournisseurs de services de télécommunication ont pris les mesures pour mettre à jour le système de commutation des demandes de renseignements sur les services de télécommunication (voir commentaire de l'art. 21 P-LSCPT). Si tel n'est pas le cas, les art. 39 à 41 P-LSCPT pourront être appliqués.

Pour des raisons de praticabilité, l'obligation de blocage précitée se limite à la situation dans laquelle un client d'un fournisseur de services de télécommunication a, lors de l'ouverture et de l'enregistrement de la relation commerciale (voir commentaire de l'art. 21 P-LSCPT), utilisé l'identité d'une personne qui n'existe pas ou qui n'a pas consenti à l'ouverture de cette relation ou encore à la situation dans laquelle le client a, lors de l'ouverture de la relation commerciale, présenté un document non conforme aux exigences de l'art. 23 P-LSCPT, c'est-à-dire à des situations qui se présentent dans le cas où le contrôle préalable à l'ouverture de la relation n'a pas eu lieu conformément aux prescriptions (voir commentaire de l'art. 23 P-LSCPT). Exiger, suite à un contrôle d'identité qui a eu lieu conformément aux prescriptions, le blocage de l'accès à la téléphonie et à Internet lorsque les clients ne correspondent plus à ceux qui ont été enregistrés lors de l'ouverture de la relation commerciale irait en revanche trop loin, également sous l'angle de l'atteinte portée à la liberté personnelle. En effet, un téléphone portable muni d'une carte SIM à prépaiement peut, par exemple, très bien être prêté à un ami, à plus ou moins long terme, dans un contexte tout à fait normal, c'est-à-dire sans que cet appareil ne soit forcément utilisé à des fins illicites. Une telle réglementation présupposerait en outre de prévoir pour les clients des fournisseurs de services de télécommunication une obligation de renouvellement de la relation commerciale et, pour ces fournisseurs, une obligation de contrôle et d'enregistrement des clients ne correspondant plus à ceux qui ont été enregistrés lors de l'ouverture de la relation commerciale. Ceci impliquerait des formalités et un travail administratif excessifs.

93 RS **784.10**

3 Conséquences

3.1 Conséquences pour la Confédération

Conformément à l'art. 38, al. 4 P-LSCPT, il appartient au Conseil fédéral de fixer le montant des émoluments.

Les coûts que devra supporter le service dans l'accomplissement de ses tâches légales seront financés par des émoluments. Sachant que le service ne couvre actuellement pas ses frais (taux de couverture des frais de 54 % pour l'année 2012), on ne peut éviter que la Confédération doive suppporter des coûts effectifs supplémentaires, si le Conseil fédéral n'augmente pas sensiblement le taux de couverture. Il se pose la question de savoir s'il est approprié de maintenir le taux (bas) actuel de couverture des frais, compte tenu du fait que la poursuite pénale est une tâche cantonale.

Il y a toutefois lieu considérer les besoins financiers et en personnel supplémentaires en relation avec les améliorations que la nouvelle LSCPT va apporter dans le domaine de la poursuite pénale.

Les conséquences financières du présent projet, sous l'angle des besoins en personnel du service et de ses frais d'exploitation et d'investissement, sont estimées comme suit:

- L'art. 2, let. b à f P-LSCPT a pour conséquence une différenciation des divers fournisseurs de services dans le domaine des télécommunications, avec diverses obligations, et implique une augmentation substantielle du nombre d'obligés. Le nombre des interlocuteurs du service, actuellement composé de 50 fournisseurs actifs, va probablement augmenter de 150 à 200 fournisseurs. Ceci va conduire à une prise en charge sensiblement plus grande et, partant, à une augmentation des activités du service de piquet du service. L'art. 5 P-LSCPT prévoit en outre que le service soit représenté au sein de l'organe consultatif que le DFJP peut mettre en place. Ces facteurs ont pour conséquence la nécessité de créer un nouveau poste à temps plein, des frais d'exploitation de 300 000 francs par an ainsi que des frais d'investissement uniques de 150 000 francs (en particulier pour l'extension et les adaptations du réseau).
- Les art. 6 à 14 P-LSCPT impliquent une augmentation des effectifs de 4 postes à plein temps, de 2,15 millions de francs par an au titre des frais d'exploitation et de 1,6 millions de francs pour les frais d'investissement. Ces coûts sont dus avant tout à l'exploitation du nouveau système informatique pour la conservation de longue durée des données issues des mesures de surveillance. Ce système doit, entre autres, assurer une conservation sûre et intègre d'une énorme quantité de données sur une longue période. S'ajoute à ce qui précède la mise à la disposition d'éventuelles interfaces avec les systèmes informatiques des autorités de poursuite pénale. Les coûts supplémentaires tiennent notamment compte des frais liés à l'acquisition d'une nouvelle infrastructure, à l'amortissement d'anciennes composantes de systèmes, à des frais de réseau, de réseau informatique et de licence, à des contrats de conseil et de maintenance ainsi qu'à la mise en œuvre des directives relatives à la sécurité.

– L'art. 15, al. 2 P-LSCPT, l'art. 16 P-LSCPT et l'art. 18 P-LSCPT étendent les prestations de renseignement du service et lui donnent de nouvelles tâches dans le domaine de la formation et de l'activité technique ainsi que dans le contrôle de qualité. Ceci a pour conséquence la création de 3 postes à plein temps, ainsi que des frais d'exploitation de 800 000 francs par an et des frais d'investissement de 600 000 francs, afin, d'une part, de pouvoir créer et exploiter les moyens nécessaires à la formation et, d'autre part, de pouvoir mettre en œuvre les contrôles de qualité exigés.

– Les nouvelles tâches du service relatives à la surveillance de la correspondance par télécommunication, en particulier découlant des art. 26, al. 2, 32 et 33 P-LSCPT, rendent nécessaires la création de 4 postes à plein temps, auxquels s'ajouteront des frais annuels d'exploitation de 500 000 francs et des frais d'investissement uniques de 700 000 francs. Les dispositions précitées impliquent en particulier un transfert de tâches de certains fournisseurs de services de télécommunication (ceux qui sont dispensés de tout ou partie des obligations des fournisseurs de services de télécommunication mais qui doivent tolérer une surveillance effectuée par le service) au service. A cet effet, celui-ci devra en effet prévoir les infrastructures de surveillance correspondantes, fournir plus de prestations de support externe, entreprendre des adaptations aux systèmes informatiques et effectuer des installations sur place chez les fournisseurs de services de télécommunication considérés. Il ne faut en outre pas négliger les besoins accrus en termes d'enseignement et de formation des collaborateurs du service.

– Les art. 40 et 41 P-LSCPT attribuent nouvellement au service des compétences relevant du droit de la surveillance et du droit pénal administratif, dont l'exercice appelle la création d'un poste à plein temps.

En résumé, on peut établir le pronostic suivant quant aux conséquences du présent projet de loi sur le personnel et les finances:

– création de 13 postes supplémentaires à plein temps;

– 3,05 millions de francs au titre des frais d'investissement;

– augmentation de 3,75 millions de francs par an au titre des frais d'exploitation (à l'exclusion des frais de personnel).

Il est précisé que l'estimation des coûts ne tient compte que du financement des mesures exposées d'un point de vue qualitatif. Les conséquences financières éventuelles liées à une augmentation quantitative des mesures de surveillance, qui pourraient théoriquement aussi découler de l'extension du champ d'application, ne peuvent par contre pas être estimées à l'heure actuelle.

3.2 Conséquences pour les cantons

L'évolution future des coûts en matière de surveillance de la correspondance par poste et télécommunication va se répercuter sur le montant des émoluments.

Le passage au nouveau système informatique de traitement exploité par le service est susceptible d'entraîner une baisse des coûts pour les cantons pour ce qui concerne l'équipement. Le surcoût causé à la Confédération en relation avec l'augmentation des délais de conservation des données auprès du service est toutefois suscep-

tible d'avoir des incidences sur les émoluments payés par les autorités de poursuite pénale, notamment par celles des cantons (voir commentaire général du ch. 2.2). Concernant les émoluments, voir le commentaire de l'art. 38 P-LSCPT.

3.3 Conséquences économiques

Le présent projet engendrera des coûts supplémentaires pour les personnes obligées de collaborer au sens de la LSCPT. Pour ce qui concerne les fournisseurs de services de télécommunication, en particulier, cette augmentation est toutefois à relativiser: le coût des surveillances ne représente en somme pour ces entreprises qu'un montant faible par rapport à leur chiffre d'affaire. L'augmentation doit également être relativisée au vu du gain en efficacité dans la poursuite des infractions qui sera obtenu grâce à la nouvelle LSCPT. Rappelons que le Conseil fédéral pourra, en vertu de l'art. 26, al. 6, P-LSCPT, dispenser des fournisseurs de services de télécommunication de certaines obligations légales – en particulier ceux qui offrent des services de télécommunication de faible importance économique ou dans le domaine de l'éducation –, ce qui influencera à la baisse les coûts qu'ils doivent supporter.

4 Relation avec le programme de la législature

Le présent projet est prévu dans le message du 25 janvier 2012 sur le programme de la législature 2011 à 2015[94].

5 Aspects juridiques

La nouvelle LSCPT se fonde sur les art. 92, al. 1, et 123, al. 1, Cst., qui attribuent à la Confédération la compétence en matière de services postaux et de télécommunications et en matière de législation relative au droit pénal et à la procédure pénale.

Elle ne pose pas de problèmes de constitutionnalité ou en relation avec le droit international.

Les art. 13, al. 1, Cst., 8, al. 1, CEDH et 17, par. 1 du Pacte international du 16 décembre 1966 relatif aux droits civils et politiques[95] garantissent le secret de la correspondance et des télécommunications, autrement dit, le droit au respect de la correspondance, ainsi que des relations établies par la poste et les télécommunications. Ce droit constitue un aspect essentiel du droit au respect de la vie privée. La surveillance de la correspondance ainsi que des relations établies par la poste et les télécommunications constituent une atteinte grave au droit fondamental précité. En vertu des art. 36 Cst. et 8 CEDH, la restriction d'un droit fondamental doit être fondée sur une base légale, être justifiée par un intérêt public et doit être proportionnée au but visé. L'essence des droits fondamentaux est en outre inviolable. Les mesures de surveillance de la correspondance par poste et télécommunication doivent ainsi figurer dans une loi au sens formel qui soit précise. Une atteinte grave exige en principe une base légale formelle, claire et précise. L'accessibilité de la loi

94 FF **2012** 479
95 RS **0.103.2**

aux personnes concernées exige que celle-ci soit formulée de manière assez précise pour leur permettre – en s'entourant, au besoin, de conseils éclairés – de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences pouvant résulter d'un acte déterminé[96]. Les garanties minimales contre les abus de pouvoir que la loi doit, au sens de l'art. 8 CEDH, prévoir sont les suivantes: la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements[97]. Les conditions précitées sont satisfaites par la nouvelle LSCPT.

Les exigences de la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité[98] sont en outre remplies.

La nouvelle LSCPT contient des délégations législatives au Conseil fédéral et aux cantons.

96 ATF **123** I 112, consid. 7a

97 Cf. entre autres, arrêt *Kopp c. Suisse* du 25 mars 1998, § 64 et 72, Recueil 1998-II et arrêt *Liberty et autres c. Royaume-Uni* du 1er octobre 2008, requête no 58243/00, § 59 ss et les références.

98 RS **0.311.43**