00.000

Rapport explicatif
relatif à la modification de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

Condensé

Les importants progrès techniques qu'ont connus les télécommunications, en particulier Internet, ces dernières années offrent aux utilisateurs un grand espace de liberté, qui permet une multitude de possibilités d'interactions. Une grande quantité d'informations peut facilement et rapidement y être échangée à relativement peu de frais et avec discrétion. Cet espace de liberté est dans la grande majorité des cas utilisé à bon escient, par les particuliers et les entreprises. Toutefois, il est également exploité par des délinquants, dans un but répréhensible. En effet, les nouvelles techniques aujourd'hui à la disposition du grand public, en particulier celles relevant d'Internet, comme par exemple la téléphonie par Internet, peuvent, au même titre que les moyens de communication classiques, être utilisés pour commettre des infractions. Ceci, notamment dans les domaines de la pornographie enfantine, de la criminalité organisée et des stupéfiants. L'accès à ces nouvelles techniques est susceptible de faciliter la commission d'infractions. Il est donc impératif de se donner les moyens de se protéger et de lutter contre cette délinquance, sans pour autant empêcher les bienfaits incontestables de ces techniques. L'objectif principal de la révision de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) est de permettre la surveillance des personnes fortement soupçonnées de commettre des infractions graves. Il sied en outre d'assurer l'ordre et la sécurité publics, pour, en fin de compte, protéger les citoyens et garantir une utilisation sûre de ces techniques. Il s'agit donc de lutter contre les abus. Par contre, à l'instar de ce qui est le cas actuellement, il n'y a, bien entendu, pas lieu de permettre de surveiller tout un chacun ayant un comportement respectueux de la loi; la liberté personnelle est ainsi sauvegardée. Un objectif important est également de pouvoir effectuer des surveillances, en dehors de toute procédure pénale, dans le but de retrouver des personnes disparues, lorsque, au vu des circonstances, il y a lieu de penser que leur santé ou leur vie sont gravement menacées.

La présente révision de la LSCPT a donc pour but premier d'adapter dite loi à l'évolution technique qui a eu lieu ces dernières années. Il sied en effet de faire en sorte que les surveillances nécessaires ne puissent pas être tenues en échec par l'utilisation de nouvelles technologies, ni actuellement ni dans les prochaines années. En résumé, l'objectif n'est, avant tout, pas de pouvoir surveiller plus, mais mieux.

Le code de procédure pénale (CPP), qui a été adopté par le Parlement le 5 octobre 2007 et va entrer en vigueur le 1er janvier 2011, unifie les dispositions de procédure applicables à la Confédération et aux cantons. Les dispositions procédurales de la LSCPT ont ainsi été transférées dans le CPP et, partant, abrogées dans la LSCPT. L'objectif poursuivi par la révision de dite loi nécessite non seulement des modifications et compléments dans celle-ci mais également des dispositions procédurales relatives à la surveillance de la correspondance par poste et télécommunication, se trouvant désormais dans le CPP.

La structure de la LSCPT est modifiée par la présente révision. Une meilleure systématique, évitant en particulier les redites et éliminant les dispositions qui ne doivent pas figurer dans une loi mais dans une ordonnance, est adoptée. Certains articles sont précisés et complétés. La numérotation des articles est nouvelle.

La révision proposée prévoit une définition plus précise et plus complète des personnes qui sont soumises à la LSCPT, c'est-à-dire des personnes qui exécutent des surveillances (de la correspondance par poste et télécommunication) en vertu de cette loi. En relation avec la gestion, par le service chargé de la surveillance de la correspondance par poste et télécommunication exploité par la Confédération (service), du système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication, la révision proposée introduit de plus dans la LSCPT des dispositions correspondant aux exigences applicables en matière de protection des données. Est nouvellement prévue la possibilité d'avoir recours à la surveillance de la correspondance dans le cas où 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 est recherchée. La révision projetée clarifie et complète en outre les tâches du service et les obligations des personnes soumises à la LSCPT; elle permet en particulier d'avoir recours à l'introduction de certains programmes informatiques dans des systèmes servant à la communication, afin de rendre la surveillance possible. Elle fait passer de six à douze mois la période rétroactive sur laquelle les autorités de poursuite pénale peuvent demander des données dites secondaires et, comme corollaire, allonge d'autant la durée obligatoire de conservation de ces données. Une adaptation de la réglementation relative à la protection du secret professionnel dans le cadre des surveillances est en outre proposée. Conformément à ce que prévoit la LSCPT dans sa version découlant du programme de consolidation (PCO) 2011-2013 mis en consultation le 14 avril 2010 par le Conseil fédéral, l'indemnisation des personnes qui exécutent des surveillances en vertu de dite loi – en particulier des fournisseurs de services de télécommunication – pour les activités qu'elles déploient dans le cadre de cette surveillance n'est pas prévue par la nouvelle LSCPT. Sont aussi introduites dans la LSCPT des dispositions pénales applicables aux personnes soumises à la LSCPT qui ne respecteraient pas certaines de leurs obligations, ainsi qu'une disposition relative à la surveillance administrative. L'avant-projet (AP) contient pour finir une disposition relative à la voie de droit ouverte contre les décisions du service et aux griefs recevables.

Table des matières

1 Présentation de l'objet

1.1 Contexte

Le domaine des télécommunications, en particulier d'Internet, a connu ces dernières années d'importants progrès techniques. Ces progrès offrent aux utilisateurs un grand espace de liberté, permettant une multitude de possibilités d'interactions. Il est possible d'y échanger facilement et rapidement une grande quantité d'informations à relativement peu de frais et avec discrétion. Dans la grande majorité des cas, cet espace de liberté est utilisé à bon escient, par les particuliers et les entreprises. Il est toutefois également exploité par des délinquants, dans un but répréhensible. En effet, les nouvelles techniques dont dispose aujourd'hui le grand public, en particulier dans le domaine d'Internet, comme par exemple la téléphonie par Internet, peuvent, à l'instar des moyens de communication classiques, être utilisés pour commettre des infractions. Ceci, notamment dans les domaines de la pornographie enfantine, de la criminalité organisée et des stupéfiants. Ces nouvelles techniques sont susceptibles de faciliter la commission d'infractions. Il faut donc impérativement se donner les moyens de se protéger et de lutter contre cette délinquance, sans pour autant empêcher les bienfaits incontestables de ces techniques. L'objectif premier de la révision de loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[1] est de permettre la surveillance des personnes fortement soupçonnées de commettre des infractions graves et d'assurer l'ordre et la sécurité publics, pour, en fin de compte, protéger les citoyens et garantir une utilisation sûre de ces techniques. Il s'agit donc de lutter contre les abus. Il n'y a par contre pas lieu, bien entendu, de permettre la surveillance de tout un chacun ayant un comportement respectueux de la loi; ainsi, la liberté personnelle est respectée. Le fait de pouvoir effectuer des surveillances, en dehors de toute procédure pénale, dans le but de retrouver des personnes disparues, lorsque, au vu des circonstances, il y a lieu de penser que leur santé ou leur vie sont gravement menacées, constitue également un objectif important.

L'évolution technique rend les surveillances de la correspondance par télécommunication plus difficiles à exécuter, en particulier dans le domaine de la téléphonie par Internet. Certains outils doivent donc être ajoutés à ceux figurant dans la LSCPT, afin que l'on puisse adapter dite loi à l'évolution technique qui a eu lieu ces dernières années. Il y a en effet lieu de faire en sorte que les surveillances nécessaires ne puissent être tenues en échec par l'utilisation de nouvelles technologies, ni actuellement, ni dans les prochaines années. En résumé, l'objectif n'est, avant tout, pas de pouvoir surveiller plus, mais mieux.

Dans un souci de sécurité du droit, le besoin s'est fait sentir de prévoir une définition plus précise et plus complète des personnes qui sont soumises à la LSCPT, c'est-à-dire des personnes qui exécutent des surveillances (de la correspondance par poste et télécommunication) en vertu de cette loi. En relation avec la gestion, par le service chargé de la surveillance de la correspondance par poste et télécommunication exploité par la Confédération (service), du système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication, le besoin s'est de plus fait sentir de prévoir dans la LSCPT des dispositions correspondant aux exigences applicables en matière de protection des

[1] RS **780.1**

données. Le besoin s'est également fait sentir de préciser et de compléter les tâches du service ainsi que les obligations des personnes soumises à la LSCPT.

Le souhait a aussi été exprimé de pouvoir avoir recours à la surveillance de la correspondance dans le cas où 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 est recherchée.

L'augmentation de la période rétroactive sur laquelle les autorités de poursuite pénale peuvent demander des données dites secondaires et, de manière conséquente, l'allongement d'autant de la durée obligatoire de conservation de ces données ont également été requis.

En outre la réglementation relative à la protection du secret professionnel dans le cadre de surveillances, notamment dans le cas de branchements directs, a été adaptée.

L'introduction dans la LSCPT de dispositions concernant le traitement des données relatives aux surveillances ordonnées a en outre été sollicitée, de même que l'introduction de dispositions pénales applicables aux personnes soumises à la LSCPT qui ne respecteraient pas certaines de leurs obligations.

Il a pour finir été jugé judicieux d'examiner l'introduction dans la LSCPT d'une disposition relative à la surveillance administrative et d'une autre concernant la voie de droit ouverte contre les décisions du service et les griefs recevables.

Nous reviendrons plus en détail sur ces différents aspects (voir ch. 1.4 et ch. 2).

1.2 Objet de la nouvelle loi

L'objet de la nouvelle LSCPT est pour l'essentiel le même que celui de l'actuelle. Elle a pour but de permettre et de régir la surveillance de la correspondance par poste et télécommunication, y compris par Internet, en particulier dans le cadre d'une procédure pénale. Une surveillance demeure également possible en dehors d'une procédure pénale, avec quelques innovations (voir ch. 1.4 et ch. 2). L'objectif principal de la nouvelle LSCPT est d'adapter la loi actuelle à l'évolution technique qui a eu lieu ces dernières années, afin que les surveillances nécessaires ne puissent être tenues en échec par cette évolution, ni actuellement, ni dans les prochaines années. Le but n'est donc pas de surveiller plus, mais mieux.

La nouvelle LSCPT détermine également, tout comme l'actuelle mais avec plus de précision, qui lui est soumis, quelles sont les tâches du service et les obligations des personnes qui lui sont soumises. Elle contient désormais des dispositions correspondant aux exigences applicables en matière de protection des données en relation avec l'exploitation par le service du système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication. Elle réglemente en particulier explicitement, ce qui est aussi nouveau, le recours à l'introduction de certains programmes informatiques dans les systèmes de communication, afin de rendre la surveillance possible.

Conformément à ce que prévoit la LSCPT dans sa version découlant du programme de consolidation (PCO) 2011-2013[2] mis en consultation le 14 avril 2010 par le

[2] http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf

Conseil fédéral, la nouvelle LSCPT ne prévoit pas l'indemnisation des personnes qui exécutent des surveillances, en particulier des fournisseurs de services de télécommunication, pour les activités déployées par celles-ci dans le cadre des surveillances.

La nouvelle LSCPT régit pour finir – ce qui est également nouveau – les conséquences, sur le plan pénal et administratif, du non respect par les personnes qui lui sont soumises de leurs obligations.

La structure de la LSCPT a changé. Elle suit désormais un plan plus logique et évite les redites. Le système prévu par celle-ci n'a pas fondamentalement changé. Il en va de même de la structure et du contenu des articles qui la composent, ceux-ci ayant plutôt été précisés et complétés. La numérotation des articles est toutefois nouvelle. Au vu de ce qui précède, on commentera de manière plus détaillée les changements qu'opère la nouvelle LSCPT par rapport à la loi actuelle.

1.3 Genèse de l'avant-projet

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 les dispositions législatives nécessaires.

En septembre 2008, afin de le conseiller dans cette tâche, l'OFJ a constitué un groupe d'experts, 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 Centre de services informatiques - Surveillance de la correspondance par poste et télécommunication du SG DFJP (CSI-DFJP-SCPT [ISC-EJPD-ÜPF]) (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 du présent avant-projet (AP).

1.4 Changements principaux proposés

1.4.1 Champ d'application

Le champ d'application matériel de la nouvelle LSCPT (art. 1 AP) doit être précisé par rapport à celui de la LSCPT actuelle. Il s'agit en effet en particulier de tenir expressément compte du rôle grandissant, depuis plusieurs années, de la correspondance par télécommunication particulière qu'est la correspondance par Internet.

Le champ d'application personnel de la LSCPT doit également être précisé et complété (art. 2 AP). En effet, il y a lieu de ne pas perdre de vue qu'il y a d'autres personnes que les fournisseurs de services postaux ou de télécommunication, y

compris les fournisseurs d'accès à Internet (Internet-Anbieter/Zugangsvermittler, Access-Provider), qui possèdent, à un moment ou à un autre, des données de communication susceptibles d'intéresser les autorités de poursuite pénale dans le cadre de la lutte contre la délinquance. Il en est par exemple ainsi des fournisseurs d'hébergement sur Internet ([reine] Service-Provider, hosting-Provider).

1.4.2 Traitement des données personnelles

La surveillance de la correspondance par poste et télécommunication est susceptible de porter sur des données dites sensibles. Il y a donc lieu de faire en sorte que les dispositions relatives au traitement de ces données ne se trouvent pas simplement dans une ordonnance, mais dans une loi au sens formel. Conformément à cet objectif, la nouvelle LSCPT contient désormais des dispositions correspondant aux exigences applicables en matière de protection des données en relation avec l'exploitation par le service du système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication (section 2, art. 6 à 13 AP). Ces dispositions reprennent en partie les art. 7 à 10 de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[3]. L'essentiel du contenu des art. 6 à 13 AP est toutefois nouveau.

Le nouveau système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication exploité par le service, l'"Interception System Schweiz" (ISS), dont la mise en fonction complète est prévue pour l'entrée en vigueur de la nouvelle LSCPT, constituera un net progrès sous l'angle de la protection des données par rapport à l'actuel. En effet, alors que, avec le système actuel, les données obtenues dans le cadre d'une surveillance de la correspondance par télécommunication et enregistrées auprès du service sont mises à la disposition des autorités concernées au moyen d'envois postaux de supports de données et de documents, elles ne le seront, en principe, avec le nouveau système, sauf problème technique (art. 9, al. 5 AP), que par un droit d'accès au système exploité par le service. Ainsi, une partie substantielle des risques en matière de protection des données inhérents au système actuel, comme par exemple la perte (lors de l'envoi ou chez le destinataire) des données, les multiples copies qui en sont faites et leur stockage sans grandes précautions, pourra être supprimée. Le fait que, avec l'évolution technologique, la quantité de données obtenues dans le cadre de surveillances est de plus en plus grande – ce qui implique que leur communication par la poste, au moyen de supports de données et de documents, aux autorités concernées est de plus en plus difficile (grande quantité de supports et de documents) et risquée – plaide également pour ce changement de système. Il en est de même du fait que, avec la rapide évolution que connaît la technique, il est de plus en plus difficile de lire (matériel de lecture difficilement disponible et conditions de conservation défavorables) dans la durée des supports de données, problème auquel on peut en grande partie échapper en confiant la conservation centralisée des données au service, potentiellement pendant une longue période. Plaide pour finir aussi pour ce changement le fait que, dans le système actuel, chaque canton doit s'équiper en matériel, coûteux, pour exploiter les données livrées, ce qui n'est pas sensé d'un point de vue économique. Dès lors que, avec le nouveau système, les données obtenues dans le cadre d'une surveillance ne seront en principe que

[3] RS **780.11**

communiquées par un droit d'accès au système exploité par le service, elles devront demeurer enregistrées dans ce système, pour une durée déterminée (art. 11 AP).

Le passage au nouveau système entraînera un surcoût pour la Confédération. Ces frais supplémentaires sont toutefois acceptables, au vu des améliorations que le nouveau système va amener 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. Les moyens supplémentaires pour l'introduction de ce nouveau système sont déjà prévus (décision du Conseil fédéral du 17 juin 2009).

1.4.3 Surveillance en dehors d'une procédure pénale

La surveillance en dehors d'une procédure pénale (art. 27 à 29 AP) doit être complétée, en particulier en prévoyant que l'on puisse y avoir recours également 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 (art. 28 AP).

1.4.4 Tâches du service

L'évolution technique qui a eu lieu ces dernières années rend nécessaire l'adaptation à celle-ci des tâches du service dans le domaine de la surveillance de la correspondance par télécommunication (art. 16 à 18 AP). Ces tâches doivent être précisées et complétées, ceci également dans un souci de sécurité juridique. De nouvelles tâches, notamment dans le domaine de la surveillance de la correspondance par Internet, en particulier de la téléphonie par Internet, sont attribuées au service et le seront par voie d'ordonnance.

1.4.5 Prestations en matière de surveillance de la correspondance par télécommunication des personnes soumises à la LSCPT

Les prestations attendues de la part des personnes soumises à la LSCPT dans le domaine de la surveillance de la correspondance par télécommunication doivent, comme corollaire à ce qui est prévu pour les tâches du service (voir ch. 1.4.4), être précisées et complétées (art. 20 à 25 AP).

Les prestations supplémentaires attendues des personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT, y compris des fournisseurs d'accès à Internet, découlent avant tout de l'évolution que la technique a connue dans le domaine de la correspondance par Internet, notamment dans le domaine de la téléphonie par Internet, évolution qui leur profite également en termes économiques. La bonne exécution des surveillances ordonnées nécessite, en particulier au vu de l'évolution technique de la correspondance par Internet, de la part de ces personnes un devoir de collaboration lorsque l'on doit avoir recours à l'introduction de certains programmes informatiques dans des systèmes de communication, afin de rendre la surveillance possible, conformément aux art. 270bis

du code de procédure pénale[4] et 70a[bis] de la procédure pénale militaire[5] (art. 21, al. 4 AP). De manière générale, elle nécessite un comportement plus actif (art. 21 à 25 AP) de leur part, susceptible de permettre d'anticiper les problèmes qui pourraient avoir lieu dans le cadre de surveillances futures.

Afin de permettre une poursuite plus efficace des infractions, il est en outre prévu d'allonger de six mois à douze mois la durée de conservation des données dites secondaires dans le domaine de la correspondance par télécommunication, y compris par Internet (art. 23 AP). Ceci découle en particulier de l'adoption partielle de la motion 06.3170 de Rolf Schweiger par le Parlement, laquelle demandait, entre autres, un tel allongement de la durée de conservation de ces données. Cette demande partait en effet de la constatation, fondée sur l'expérience, que la durée pendant laquelle les données devaient être conservées, soit six mois, était trop courte pour permettre aux autorités d'entreprendre des recherches fructueuses, en ce sens que les données secondaires pertinentes étaient souvent déjà effacées au moment où l'autorité ordonnait la surveillance considérée. Dès lors que ce problème se pose 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 logique que l'augmentation de la durée de conservation s'applique également aux données secondaires relatives à la correspondance par poste (art. 19, al. 2 AP). Quant à l'allongement de six mois à douze mois de la période sur laquelle les données secondaires peuvent être demandées avec effet rétroactif (art. 273 al. 3 du code de procédure pénale[6] et art. 70*d* al. 3 de la procédure pénale militaire[7]), il est le corollaire de l'allongement de la durée de conservation de ces données, découle d'un même constat et procède d'un même souci d'efficacité.

1.4.6 Absence d'indemnisation des personnes soumises à la LSCPT pour leurs prestations en matière de surveillance de la correspondance

Le 14 avril 2010, le Conseil fédéral a mis en consultation le programme de consolidation (PCO) 2011-2013[8], qui a pour but d'alléger le budget de la Confédération. La suppression de l'indemnisation des personnes qui exécutent des surveillances en vertu de la LSCPT est une mesure qui fait partie de ce programme. Est visée l'indemnité, mentionnée à l'art. 16, al. 1, phr. 2 de la LSCPT actuelle, allouée aux personnes qui exécutent des surveillances en vertu de la LSCPT, en particulier aux fournisseurs de services de télécommunication, pour les frais occasionnés par la surveillance (art. 30, al. 1 AP). Le présent avant-projet se fonde sur l'état de fait tenant déjà compte de cette suppression. Il sied de préciser, en guise de remarque, que d'autres considérations, juridiques, plaident pour cette suppression. Les données que doivent livrer les personnes soumises à la LSCPT dans le domaine de la surveillance de la correspondance relèvent en effet, comme celles que doivent livrer les banques, du devoir d'édition (Editionspflicht), lequel ne donne pas lieu à indemnisation. L'indemnisation est contraire au système en droit pénal. Il ne semble en outre pas opportun d'accorder une indemnité aux personnes soumises à la LSCPT

4 RS ... (FF **2007** 6583)
5 RS **322.1**
6 RS ... (FF **2007** 6583)
7 RS **322.1**
8 http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf

dans le domaine de la surveillance de la correspondance, dès lors que celles-ci ont un intérêt à ce que des infractions ne soient pas commises par leur entremise.

L'émolument que l'autorité qui a ordonné la surveillance doit verser au service demeure, en revanche.

Pour le surplus, voir le commentaire de l'art. 30 AP et ch. 3.1.

1.4.7 Dispositions pénales

Il y a lieu d'introduire dans la nouvelle LSCPT des dispositions pénales (art. 31 AP) 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. Il sied à cet égard de préciser que de telles sanctions ne visent pas en premier lieu les fournisseurs importants de services de télécommunication que l'on trouve actuellement sur la marché helvétique, lesquels sont en principe conscients de leurs obligations.

Il s'agit en effet tout d'abord de prévoir pour l'inobservation des injonctions du service une sanction analogue à celle prévue à l'article 292 du code pénal[9] (art. 31, al. 1, let. a AP), laquelle ne saurait toutefois être dissuasive, 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. Si ce mécanisme a bien entendu également comme 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. Il sied cependant de ne pas perdre de vue que les personnes soumises à la LSCPT ne peuvent pas contester une décision du service de faire exécuter une surveillance sous l'angle de la légalité de l'ordre de surveillance sur lequel cette décision se fonde (voir ch. 1.4.9). Les règles relatives au contrôle de la validité de l'injonction du service par le juge pénal, saisi d'une poursuite pour infraction à l'art. 31 al. 1, let. a AP, sont les mêmes que celles, développées par la doctrine[10] et la jurisprudence, qui s'appliquent en cas de violation de l'art. 292 du code pénal[11].

En se fondant notamment sur la motion 06.3170 de Rolf Schweiger, partiellement adoptée par le Parlement, il a ensuite été décidé – toujours dans le but de permettre une exécution efficace des surveillances ordonnées – de prévoir une disposition pénale (art. 31, al. 1, let. b AP) sanctionnant la violation de l'obligation de conserver les données dites secondaires dans le domaine de la correspondance par télécommunication (art. 23 AP). Outre le fait que la sanction prévue à l'art. 292 du code pénal[12] 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

9 RS **311.0**
10 Bernard CORBOZ, Les Infractions en droit suisse, vol. II, Berne 2002, n. 11 à 16 ad art. 292 CP
11 RS **311.0**
12 RS **311.0**

une autorité, ne sont pas livrées mais non lorsque des données ont déjà été détruites avant cet ordre de l'autorité ou lorsque des données n'ont pas du tout été collectées ou conservées. La nouvelle disposition proposée doit, de manière cohérente, aussi s'appliquer à la violation de l'obligation de conserver les données dites secondaires dans le domaine de la correspondance par poste (art. 19 al. 2 AP).

1.4.8 Surveillance

Il y a lieu de pouvoir 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 librement, dans les limites de la loi, être actives sur le marché suisse. La nouvelle disposition proposée relative à la surveillance administrative des personnes soumises à la LSCPT (art. 33 AP), rendant l'art. 58 de la loi sur les télécommunications[13] en partie applicable par analogie, a pour but de réaliser cet objectif. Elle permet au service de prononcer des sommations en cas de violation de la législation relative à la surveillance de la correspondance par poste et télécommunication.

L'art. 33 AP instaure donc un système de sanctions administratives, distinct et complémentaire au système de sanctions pénales.

1.4.9 Voies de droit

Les considérations qui suivent ne concernent pas la voie de droit à la disposition des personnes ayant fait l'objet d'une surveillance ou aux personnes qui sont concernées par cette surveillance, selon les modalités prévues à l'art. 279, al. 3 du code de procédure pénale[14]. Elles concernent en revanche les voies de recours ouvertes aux personnes soumises à la LSCPT contre les décisions du service.

La LSCPT actuelle ne contient pas de disposition régissant les voies de recours ouvertes aux personnes soumises à la LSCPT contre les décisions du service, en général, 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'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[15] reconnaît le droit, pour ces personnes, de recourir contre une décision du service de faire exécuter une surveillance. Il ressort de la jurisprudence[16] et de la doctrine[17] que, dans le cadre d'un tel recours, ces personnes ne peuvent toutefois invoquer que des questions d'ordre technique ou organisationnel liées à l'exécution de la mesure de surveillance qui leur est demandée, en prétendant que cette surveillance exigerait de leur part des moyens techniques ou des connaissances qui leur feraient défaut. L'AP reprend cette réglementation (art. 34, al. 2, phr. 2). Dans le cadre d'un tel recours, les personnes soumises à la LSCPT pourront également, *a fortiori*, invoquer le fait que la

13 RS **784.10**
14 RS ... (FF **2007** 6583)
15 RS **780.11**
16 ATF 130 II 249, consid. 2.2.2 et 2.2.3
17 Thomas HANSJAKOB, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2ème éd., Saint-Gall 2006, n. 3 ad art. 32 OSCPT

surveillance ordonnée est, en l'état actuel de la technique, objectivement impossible à exécuter. Il sied à cet égard de noter que, au vu de la réglementation proposée, il est fort peu probable que le service transmette à une personne soumise à la LSCPT active dans le domaine de la correspondance par télécommunication un ordre de surveillance qui ne soit techniquement pas possible à exécuter. En effet, le service a notamment pour tâche de contrôler que l'ordre de surveillance qui lui a été transmis par l'autorité ayant ordonné celle-ci peut techniquement être exécuté, à défaut de quoi il doit en informer l'autorité qui a ordonné la surveillance et l'autorité habilitée à autoriser la surveillance (art. 16, let. a AP). Dans le cadre de la réglementation précitée, le service a la possibilité de rendre, pour le cas où une personne soumise à la LSCPT a invoqué des questions d'ordre technique ou organisationnel pour s'opposer à l'exécution de la mesure de surveillance, une décision lui ordonnant de prendre (dans un certain délai) les mesures nécessaires pour pouvoir à l'avenir exécuter la (sorte de) surveillance considérée[18]. Cette décision pourra, quant à elle, faire l'objet d'un recours conformément aux dispositions générales de la procédure fédérale (art. 34, al. 1 AP).

Il découle donc de la jurisprudence[19] et de la doctrine[20], dont le contenu est repris dans l'art. 34 AP, que les personnes soumises à la LSCPT n'ont pas la qualité pour recourir contre une décision du service qui les oblige à transmettre des données couvertes par un ordre de surveillance dûment approuvé par l'autorité pénale compétente, en remettant en cause la légalité de cet ordre. Ce régime est justifié. En effet, il y a lieu de constater qu'il n'y a pas de relation directe entre l'autorité de poursuite pénale, qui ordonne la surveillance, et les personnes soumises à la LSCPT, notamment les fournisseurs de services de télécommunication. Ces dernières reçoivent en effet le mandat d'exécuter la surveillance directement du service, avec lequel elles sont liées par un rapport de droit administratif indépendant de la procédure pénale. Dans ce domaine, le service ne joue donc qu'un rôle d'intermédiaire entre les autorités habilitées à ordonner et à autoriser une surveillance, d'une part, et les personnes soumises à la LSCPT, d'autre part. Il ne dispose ainsi d'aucun pouvoir d'examen matériel contraignant pour les autorités précitées. Il incombe donc exclusivement à l'autorité habilitée à autoriser une surveillance de vérifier la légalité d'une surveillance ordonnée et, cas échéant, de s'opposer à l'exécution de celle-ci lorsqu'il la juge illégale.[21] En vertu de la jurisprudence[22] et de la doctrine[23] précitées, la possibilité de contester la légalité d'un ordre de surveillance est réservée uniquement aux personnes ayant fait l'objet de la surveillance ou aux personnes qui sont impliquées, selon les modalités prévues à l'art. 279, al. 3 du code de procédure pénale[24]. Le fait qu'il ne semble pas praticable d'informer de l'ordre de surveillance toutes les personnes concernées par un type de surveillances touchant des inconnus (p. ex. "Kopfschaltungen") ou un nombre indéterminé de personnes (p. ex. "Antennensuchläufe") ne signifie pas encore qu'il faille permettre aux personnes soumises à la LSCPT, en particulier aux fournisseurs de services de télécommunication, de recourir sans la limitation susmentionnée contre une décision du service les enjoignant d'exécuter une

18 Jugement du Tribunal administratif fédéral du 10 mars 2009, A-2336/2008, consid. 7.4
19 ATF 130 II 249, consid. 2.2.2 et 2.2.3
20 Thomas HANSJAKOB, op. cit., n. 3 ad art. 32 OSCPT
21 ATF 130 II 249, consid. 2.2.2 et 2.2.3
22 ATF 130 II 249, consid. 2.2.2 et 2.2.3
23 Thomas HANSJAKOB, op. cit., n. 3 ad art. 32 OSCPT
24 RS ... (FF **2007** 6583)

surveillance. En effet, les personnes concernées par les types de surveillance précités ne sont pas des prévenus, ni des tiers surveillés au sens de l'art. 270, let. b du code de procédure pénale[25] ni même des personnes qui ont utilisé le même raccordement que le prévenu ou le tiers surveillé (au sens de l'art. 270, let. b du code de procédure pénale[26]). Ce qui implique que, par une application a contrario de l'art. 279 du code de procédure pénale[27], elles n'ont pas à être informées de la surveillance ordonnée par l'autorité de poursuite pénale et ne peuvent recourir contre cette surveillance. Il serait au surplus inutile d'informer ces personnes, étant donné que la majorité des informations considérées seront sans intérêt pour la procédure et ne seront, en vertu de 276, al. 1 du code de procédure pénale[28], même pas versées au dossier, ce qui implique que l'atteinte à la vie de ces personnes est faible[29].

Pour des raisons de clarté et de sécurité juridique, il est souhaitable d'introduire dans la LSCPT une disposition expresse (art. 34 AP) régissant dans le sens exposé ci-dessus les voies de recours ouvertes aux personnes soumises à cette loi contre les décisions rendues par le service.

Il n'y a pas lieu d'introduire dans la LSCPT – afin de ne pas retarder l'exécution d'une mesure de surveillance ordonnée – une disposition prévoyant de manière générale et absolue l'absence d'effet suspensif d'un recours que déposeraient les personnes soumises à la LSCPT contre une décision du service de faire exécuter une surveillance. En effet, premièrement, conformément à l'art. 55, al. 2 de la loi fédérale du 20 décembre 1968 sur la procédure administrative[30], le service peut toujours prévoir qu'un recours contre sa décision n'aura pas d'effet suspensif et l'effet suspensif peut être retiré en instance de recours après le dépôt de celui-ci. Deuxièmement, les sanctions pénales (voir ch. 1.4.7) et administratives (voir ch. 1.4.8) qu'il est prévu d'introduire dans la LSCPT sont susceptibles de dissuader des personnes soumises à la LSCPT qui voudraient retarder l'exécution d'une mesure de surveillance de déposer un recours dilatoire. Et troisièmement, lorsqu'un fournisseur de services de télécommunication prétend qu'il n'est pas en mesure d'exécuter la surveillance ordonnée, cette exécution peut, cas échéant, avoir lieu en ayant recours au service ou à un tiers, aux frais du fournisseurs considéré (art. 24 AP), ce qui peut, au demeurant, aussi avoir un effet dissuasif dans le sens précité.

1.5 Droit comparé

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 de l'avant-projet. La surveillance de la téléphonie par Internet, en particulier, y est également prévue. Il existe toutefois quelques différences de modalités par rapport à la réglementation prévue dans l'avant-projet. Le droit allemand dispose par exemple que les données correspondant aux données dites secondaires dans notre pays doivent être conservées par les fournisseurs de services de télécommunication

25 RS ... (FF **2007** 6583)
26 RS ... (FF **2007** 6583)
27 RS ... (FF **2007** 6583)
28 RS ... (FF **2007** 6583)
29 Cf. le message du 1er juillet 1998 relatif à la LSCPT actuelle, FF **1998** 3722
30 RS **172.021**

pendant six mois, et non pas pendant douze mois, comme le propose l'avant-projet, en lieu et place de six mois actuellement (voir art. 23 AP et commentaire y relatif).

2 Commentaire article par article

2.1 Section 1: Dispositions générales

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

L'*al. 1* définit le champ d'application matériel de la LSCPT. Il ne subit pas de changement fondamental par rapport à sa version dans l'actuelle LSCPT. Bien que cela soit aujourd'hui implicite et admis, on précise explicitement, pour des raisons de clarté, que la correspondance par Internet, qui comprend notamment la correspondance par messagerie électronique[31] et la téléphonie par Internet, est un type particulier de correspondance par télécommunication, au sens où la notion de télécommunication est définie aux art. 2 et 3, let. c de la loi du 30 avril 1997 sur les télécommunications[32]. Avec cette précision, il est inutile de répéter, à chaque fois que la loi mentionne la notion de correspondance par télécommunication, que la correspondance par Internet est aussi visée par cette notion; cela devient ainsi implicite.

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 code de procédure pénale[33], qui s'appliquera 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 en substance pas par rapport à sa formulation dans l'actuelle LSCPT.

La mention du sauvetage contenue dans l'*al. 1, let. c* de l'actuelle LSCPT peut être supprimée, car cet objectif découle logiquement de la volonté de rechercher la personne disparue (art. 27 AP).

L'*al. 1, let. d* prévoit que la LSCPT est applicable dans un nouveau cas, qui ne figure pas dans la LSCPT actuelle, à savoir celui où on recherche une personne condamnée à une peine privative de liberté ou qui fait l'objet d'une mesure de privation de liberté, sur la base d'un jugement définitif et exécutoire (art. 28 AP).

Les règles régissant à l'*al. 2* les renseignements sur les services de paiement soumis à la loi du 30 avril 1997 sur la poste[34] doivent être adaptées, les renvois opérés dans la LSCPT actuelle n'étant plus corrects. En effet, avec l'entrée en vigueur du code de procédure pénale[35], l'obligation de témoigner sera réglée par dit code. Il n'est pas besoin d'y faire mention, dès lors que cela est évident. En outre, l'obligation de

31 Bernard CORBOZ, op. cit., n. 6 ad art. 321ter CP
32 RS **784.10**
33 RS ... (FF **2007** 6583)
34 RS **783.0**
35 RS ... (FF **2007** 6583)

renseigner les autorités est régie par les art. 284 et 285 du code de procédure pénale[36], la poste devant, 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. Il y a lieu d'opérer un tel renvoi, dès lors que cette qualification ne s'impose pas de soi.

Art. 2 Champ d'application à raison des personnes

L'*art. 2* détermine, comme cela est le cas dans l'art. 1, al. 2 de l'actuelle LSCPT, quel est le champ d'application personnel de la LSCPT, c'est-à-dire quelles sont les personnes soumises à cette loi, qui ont des obligations en vertu de celle-ci, qui exécutent des surveillances en vertu de celle-ci. Il sied à titre préliminaire de préciser que la LSCPT ne s'applique plus uniquement à des organismes, mais, d'une manière générale, 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.

La formulation de l'*al. 1* est modifiée par rapport à celle de l'art. 1, al. 2 de l'actuelle LSCPT, afin de permettre aux autorités de poursuite pénale d'obtenir des données de communication, susceptibles d'intéresser la procédure, de personnes qui ne rentrent pas dans le champ d'application de la LSCPT actuellement en vigueur. Sont par exemple concernés les services libres postaux (services de courrier, service de poste rapide, etc.) (art. 10 de l'ordonnance du 26 novembre 2003 sur la poste[37]) et les fournisseurs d'hébergement ([reine] Service-Provider, Hosting-Provider) sur Internet, qui ne sont ni soumis à concession ni à l'obligation d'annoncer[38]. Afin de maintenir toutefois une certaine limitation des personnes déployant une activité dans le domaine de la correspondance par poste et télécommunication chargées d'exécuter des surveillances en vertu de la LSCPT, il y a lieu de limiter dans l'*al. 1* le champ d'application personnel de cette loi aux personnes mentionnées aux *let. a et b* qui exercent leur activité à titre professionnel, peu importe que ce soit à temps complet ou partiel et contre rémunération ou à titre gratuit. Ne sont donc pas chargées d'exécuter de telles surveillances les personnes qui exercent leur activité à titre de loisir, de passe-temps. Si ces personnes exercent leur activité dans le domaine de la correspondance par télécommunication à titre non professionnel, l'al. 2 trouve application et les obligations qu'elles doivent respecter sont celles mentionnées à l'art. 26 AP. Les personnes entrant dans le champ d'application personnel de la LSCPT au sens de l'al. 1, qui sont soumises à cette loi et sont donc tenues d'exécuter des surveillances en vertu de celle-ci sont, considérées dans leur globalité, désignées dans le texte de loi par l'expression "personnes qui exécutent des surveillances (de la correspondance par poste et télécommunication) en vertu de la présente loi" ou, plus rarement, par des expressions en substance identiques. Dans le domaine de la correspondance par télécommunication, cette notion englobe non seulement les fournisseurs de services de télécommunication, visés par l'*al. 1, let. a*, mais également les personnes visées par l'*al. 1 let. b*. En résumé, sont chargées d'exécuter des surveillances de la correspondance par poste et télécommunication en vertu de la LSCPT, les personnes qui, cumulativement, agissent avec une des qualités mentionnées à l'al. 1, let. a et b et exercent leur activité à titre professionnel.

36 RS ... (FF **2007** 6583)
37 RS **783.01**
38 Thomas HANSJAKOB, op. cit., n. 24 ad art. 1 LSCPT

L'*al. 1, let. a* reprend l'art. 1, al. 2 de la LSCPT actuelle et le modifie, dans le sens où on précise explicitement, pour des raisons de clarté, que, de même que la correspondance par Internet est un type particulier de correspondance par télécommunication, les fournisseurs d'accès à Internet (Internet-Anbieter/Zugangsvermittler) constituent un type particulier de fournisseurs de services de télécommunication. Cette précision implique qu'il est inutile de répéter, à chaque fois que la loi mentionne la notion de fournisseur de services de télécommunication, que les fournisseurs d'accès à Internet (Internet-Anbieter/Zugangsvermittler) sont aussi visés par cette notion; ceci est ainsi implicite. Le contenu de la notion de fournisseur de services de télécommunication est défini par les art. 2 et 3, let. b et c de la loi du 30 avril 1997 sur les télécommunications[39]. Le fournisseur de service de télécommunication s'engage à transporter pour le compte d'un tiers les informations visées aux articles précités. Constituent par exemple des fournisseurs de services de télécommunication les grands opérateurs actifs sur le marché suisse qui permettent aux usagers de téléphoner, au moyen d'un téléphone fixe ou d'un téléphone mobile, ou d'accéder à Internet. Il va de soi que ces fournisseurs de services de télécommunication sont tenus d'exécuter des surveillances de la correspondance par télécommunication, étant donné qu'il exercent leur activité à titre professionnel, ce même dans l'hypothèse où ils fournissent leurs services gratuitement.

L'*al. 1, let. b* a pour but de permettre expressément aux autorités de poursuite pénale d'obtenir des données de communication, susceptibles d'intéresser la procédure pénale en cours, auprès de personnes qui ne constituent pas à proprement parler des fournisseurs de services postaux ou de télécommunication au sens des art. 2 et 3, let. b et c de la loi du 30 avril 1997 sur les télécommunications[40], mais qui jouent un rôle d'intermédiaire dans le processus de correspondance considéré, en possédant à un moment donné de telles données. Constituent par exemple de telles personnes les fournisseurs d'hébergement ([reine] Service-Provider, Hosting-Provider) sur Internet (qu'ils soient des particuliers ou des organisations, des entreprises), également pour les services de correspondance par messagerie électronique (p. ex. boîte aux lettres) qu'ils mettent à la disposition des tiers. Sont également considérés comme telles les revendeurs (qu'ils soient des particuliers ou non) de cartes SIM à prépaiement, qui ont été obtenues auprès d'entreprises qui constituent des fournisseurs de services de télécommunication. Il en va de même des personnes (qu'elles soient des particuliers ou non) à qui des données de communication font l'objet d'un "outsourcing" par des fournisseurs de services de télécommunication. Ces personnes sont tenues d'exécuter des surveillances de la correspondance par télécommunication si elles exercent leur activité à titre professionnel, ce même si elles fournissent leurs services gratuitement.

Les internet cafés ou cyber cafés ainsi que les écoles en tous genres, hôtels, restaurants, hôpitaux et particuliers, qui laissent par exemple leur réseau Wi-Fi à la disposition de leurs clients ou de tiers pour se connecter à Internet ne constituent pas des fournisseurs de services de télécommunication, visés par l'al. 1 let. a, ou des personnes visées par l'al. 1 let. b. Ils ne sont donc pas tenus d'exécuter personnellement des surveillances de la correspondance par télécommunication. Ceci ne saurait toutefois impliquer qu'une surveillance de la correspondance par

[39] RS **784.10**
[40] RS **784.10**

télécommunication efficace, réalisée par le fournisseur d'accès à Internet des personnes précitées, ne puisse avoir lieu (voir aussi commentaire de l'art. 22 AP).

L'*al. 2* reprend l'art. 1, al. 4 de la LSCPT actuelle. Il y ajoute les personnes mentionnées à l'al. 1 qui n'exercent pas leur activité à titre professionnel et qui, partant, ne sont pas chargées d'exécuter des surveillance de la correspondance par télécommunication. Cet ajout est justifié du fait qu'il est essentiel de tout de même permettre la surveillance de la correspondance par télécommunication dans ces cas de figure.

Art. 3 Service de surveillance

L'*art. 3* reprend en substance l'art. 2 de l'actuelle LSCPT.

Outre les tâches que lui attribue le présent AP, le service a notamment la faculté – et non l'obligation – de fournir aux autorités et aux personnes qui exécutent des surveillances en vertu de la LSCPT des conseils techniques en matière de surveillance de la correspondance par poste et télécommunication (voir aussi commentaire de l'art. 15 AP).

Art. 4 Traitement des données personnelles

L'*art. 4* reprend l'actuel art. 7, al. 1 de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[41], et en adapte le champ d'application personnel, au vu de l'art. 2, al. 1, let. b AP. Les détails relatifs aux modalités de ce traitement demeurent réglés dans l'ordonnance précitée.

Art. 5 Secret des postes et des télécommunications

L'*art. 5* reprend en substance les art. 12, al. 3 et 15, al. 7 de l'actuelle LSCPT.

2.2 Section 2: Système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication

Art. 6 Principe

L'*art. 6* reprend en substance l'al. 1 de l'actuel art. 8 de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[42].

Le système exploité par le service ne contient pas les données recueillies lors de la surveillance de la correspondance par poste, car celles-ci sont directement transmises à l'autorité qui a ordonné la surveillance, conformément à l'art. 19 AP.

Art. 7 But du système de traitement

Voir le commentaire sous le ch. 1.4.2.

41 RS **780.11**
42 RS **780.11**

Art. 8 Contenu du système de traitement

Les données mentionnées à l'*art. 8* sont celles que l'on peut obtenir dans le cadre d'une surveillance. Elles peuvent donner des renseignements divers, comme, par exemple, le contenu des conversations téléphoniques de la personne surveillée, le contenu de ses communications par Internet ou sa localisation.

Art. 9 Accès au système de traitement

La réglementation de l'*al. 1* correspond à la situation actuelle. L'autorité qui a ordonné une surveillance ne peut accéder, sous réserve de l'al. 2, qu'aux données contenues dans le système qui ont été recueillies lors de la surveillance considérée, et non à toutes les données recueillies lors d'une surveillance contenues dans le système. Selon cette réglementation, par exemple, les policiers travaillant sur un dossier peuvent, avec l'autorisation du ministère public qui dirige les opérations, qui a ordonné la surveillance considérée et qui a accès aux données recueillies lors de cette surveillance, aussi accéder à ces données. Mais cela n'est possible que si le ministère public les y autorise et uniquement pour les données que celui-ci les autorise à consulter, en application du principe de la proportionnalité. Un policier peut par exemple être autorisé à ne consulter que les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation, mais pas les communications de cette personne.

La réglementation prévue à l'*al. 2* permet d'éviter que l'autorité ayant ordonné une surveillance et les personnes désignées par celle-ci accèdent à des données dont elles n'ont plus besoin. Elle implique également la nécessité d'un comportement actif de l'autorité ayant ordonné une surveillance pour, passé un certain délai, maintenir l'accès à des données dont elle a encore besoin, sans quoi l'accès à celles-ci lui est supprimé. Le service doit avertir l'autorité ayant ordonné une surveillance que le délai d'accès aux données recueillies lors de celle-ci approche de son terme afin de permettre à cette autorité de déposer, cas échéant, à temps une demande de prolongation de délai pour accéder plus longtemps à ces données. En décider autrement est susceptible de poser des problèmes pratiques dans l'exploitation des données et d'impliquer un surplus de travail administratif inutile.

L'*al. 3* a pour but de permettre au service de savoir si une autre autorité que celle ayant ordonné la surveillance qui le contacte pour accéder en ligne aux données recueillies lors de cette surveillance (voir al. 4) doit pouvoir accéder à ces données. On ne parle à dessein pas d'"instances" mais d'"autorités" qui seraient subséquemment saisies du dossier, car on vise également le cas où la surveillance a été ordonnée par la police pour retrouver une personne disparue et où l'autorité subséquente est un autre corps de police (p.ex. parce que les recherches s'orientent dans un autre canton que celui dont relève le corps de police qui a ordonné la surveillance).

Pour l'*al. 4*, voir le commentaire, par analogie, des al. 1 à 3.

Pour l'*al. 5*, voir le commentaire sous le ch. 1.4.2.

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

Les droits visés à l'*al. 1* sont tous régis dans le code de procédure pénale[43].

L'*al. 2* vise l'hypothèse où la demande d'entraide est une demande d'extradition et celle où cette demande porte sur un autre cas d'entraide judiciaire. Le droit de consulter le dossier et le droit d'accès aux données de la personne concernée par les données recueillies lors de l'exécution d'une demande d'extradition (art. 1, al. 1, let. b) 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)[44], les art. 26 et 27 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[45], applicable en vertu de l'art. 12, al. 1, phr. 1 de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP)[46], et les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[47]. L'art. 18*a*, al. 4 de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP)[48] est introduit par la code de procédure pénale[49]. Dans les autres cas d'entraide judiciaire (art. 1, al. 1, let. b), ces droits sont régis par les art. 18*a*, al. 4 et 80*b* de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP)[50], 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[51] et l'art. 46 de la loi fédérale du 22 juin 2001 sur la coopération avec la Cour pénale internationale (LCPI)[52] ainsi que soit par les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[53], si l'autorité saisie de la demande d'entraide est une autorité de la Confédération, soit par le droit cantonal, si cette autorité est le ministère public 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)[54] et les Conventions internationales conclues par la Suisse en matière d'entraide judiciaire internationale avec les Etats étrangers (par exemple avec le Canada et le Brésil) prévoient l'applications de de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP)[55], dont les articles 18*a*, al. 4 et 80*b*. Lorsque l'autorité saisie de la demande d'entraide est le ministère public d'un canton, l'art. 37, al. 1 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[56] s'applique à titre subsidiaire au droit d'accès aux données recueillies lors d'une surveillance si le droit cantonal n'assure pas un niveau de protection adéquat. L'autorité abordée dans le cadre de l'exercice du droit de consulter le dossier ou du droit d'accès aux données doit être en mesure, dans les hypothèses où ces droits sont restreints et dans la mesure où cela est nécessaire, de répondre à la demande considérée de manière à ne pas révéler des informations couvertes par le secret de fonction.

43 RS ... (FF **2007** 6583)
44 RS **351.1**
45 RS **172.021**
46 RS **351.1**
47 RS **235.1**
48 RS **351.1**
49 RS ... (FF **2007** 6583)
50 RS **351.1**
51 RS **351.93**
52 RS **351.6**
53 RS **235.1**
54 RS **351.20**
55 RS **351.1**
56 RS **235.1**

L'*al. 3* renvoie au droit cantonal. Il y a à cet égard lieu de préciser que l'art. 37, al. 1 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[57] s'applique à titre subsidiaire au droit d'accès aux données recueillies lors d'une surveillance si le droit cantonal n'assure pas un niveau de protection adéquat.

La réglementation prévue à l'*al. 4* reflète clairement que ce n'est pas le service, uniquement détenteur des données, qui est le maître du fichier, mais, conformément à l'art. 13 AP, les autorités ayant accès au système de traitement, en vertu de l'art. 9 AP.

Art. 11 Délai de conservation des données

La communication du délai de prescription de l'action pénale que l'autorité en charge du dossier doit faire au service, en vertu de l'*al. 1, phr. 2*, a pour but de permettre à ce dernier de satisfaire à son obligation d'information contenue à l'al. 5 (voir commentaire de l'al. 5). Cette communication est importante, étant donné que le délai de prescription de l'action pénale varie en fonction de la peine prévue pour l'infraction retenue et étant donné que pour connaître cette infraction, il faut avoir accès au contenu du dossier pénal. Or, le service n'y a pas accès.

La durée de conservation maximale des données dans le système de traitement mentionnée à l'*al. 2* se justifie en particulier par le fait que les procédures d'entraide durent souvent longtemps. Le durée correspond au délai maximal de prescription de l'action pénale connu en droit suisse (si on fait abstraction des infractions imprescriptibles), alors même que l'infraction considérée peut être imprescriptible dans le droit de l'Etat requérant.

La durée de conservation maximale des données dans le système de traitement prévue à l'*al. 3* 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.

La communication de la fin du délai de prescription de la peine que l'autorité en charge du dossier doit faire au service, en vertu de l'*al. 4, phr. 2*, en relation avec les données recueillies lors de la recherche de personnes condamnées à une peine privative de liberté (*al. 4, phr. 1*), a pour but de permettre à ce dernier de satisfaire à son obligation d'information contenue à l'al. 5 (voir commentaire de l'al. 5). Cette communication est importante, étant donné que le délai de prescription de la peine varie en fonction de la peine prononcée et étant donné que pour connaître cette peine, il faut avoir accès au contenu du dossier pénal. Or, le service n'y a pas accès. Quant à la durée de conservation maximale des données dans le système de traitement mentionnée à l'*al. 4, phr. 3*, elle se justifie en particulier par le fait que ce qui est susceptible d'être en jeu est le bien juridique le plus précieux, à savoir la vie humaine. Il sied de préciser 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 le cas pour la sanction que constitue une peine privative de liberté.

A teneur de l'*al. 5*, l'autorité en charge du dossier ou, s'il n'y a plus d'autorité en charge du dossier, la dernière à l'avoir été ou celle qui a succédé à celle-ci doit en principe demander le transfert des données considérées pour respecter les prescriptions relatives à la conservation des dossiers (art. 103, al. 1 du code de

[57] RS **235.1**

procédure pénale[58]) ou les règles applicables à l'archivage. On peut en effet imaginer des cas dans lesquels les données doivent être effacées du système, en vertu des al. 1 à 4, tout en devant encore demeurer au dossier, en vertu de l'art. 103, al. 1 du code de procédure pénale[59], au vu de l'exigence de prescription de la peine que cette disposition mentionne. En outre, il n'appartient pas au service mais à l'autorité en charge du dossier ou, s'il n'y a plus d'autorité en charge du dossier, à la dernière à l'avoir été ou à celle qui a succédé à celle-ci de prendre les dispositions nécessaires au respect des prescriptions en matière d'archivage. En matière d'archivage, on applique les dispositions de la collectivité (Confédération ou cantons) dont relève l'autorité qui a ordonné la surveillance considérée, étant donné que c'est une autorité relevant de cette collectivité qui est le maître du fichier pour ce qui concerne les données recueillies lors d'une surveillance relevant de sa compétence. Une fois que les données ont été transférées à l'autorité compétente, le service les détruit du système de traitement. Il en va de même des données dont le transfert n'a pas été demandé à l'expiration de leur délai de conservation. Afin d'éviter que le transfert de données ne soient pas demandé par erreur (oubli) à l'expiration de leur délai de conservation dans le système de traitement – ce qui est susceptible d'entraîner la perte irrémédiable de données devant encore être conservées en vertu de l'art. 103, al. 1 du code de procédure pénale[60] ou des dispositions applicables en matière de protection des données –, le service a un devoir d'information de l'échéance prochaine du délai de conservation des données dans son système de traitement. Dans les hypothèses visées par l'al. 1 et l'al. 4, phr. 1, le service doit pour ce faire pouvoir compter sur la communication de l'autorité en charge du dossier (voir commentaire de l'al. 1 et de l'al. 4, phr. 1). Cette solution "centralisée" semble préférable à celle qui consisterait à laisser toutes les autorités, susceptibles d'être saisies de dossiers contenant des données recueillies dans le cadre d'une surveillance de la correspondance par télécommunication, contacter le service avant l'échéance de ce délai. Cette alternative impliquerait en effet la nécessité pour la Confédération et chaque canton de s'organiser pour ne pas rater la fin du délai précité et multiplierait d'autant les risques de ne pas y parvenir. Afin de rendre la tâche du service plus aisée, la Confédération et chaque canton doivent désigner l'autorité à qui le service doit adresser cet avis. On ne peut en effet pas exiger du service qu'il doive rechercher, après de longues années, l'autorité en charge du dossier, la dernière à l'avoir été ou celle qui a succédé à celle-ci. Ceci serait trop compliqué, si l'on considère le nombre important d'autorités susceptibles d'être saisies de dossiers contenant des données recueillies dans le cadre d'une surveillance de la correspondance.

Art. 12 Sécurité

La réglementation prévue à la *phr. 1* se justifie du fait que le service - même s'il n'est pas maître du fichier (voir commentaire de l'art. 13 AP) – est le détenteur des données, étant donné que celles-ci sont contenues dans un système de traitement qu'il exploite.

58 RS ... (FF **2007** 6583)
59 RS ... (FF **2007** 6583)
60 RS ... (FF **2007** 6583)

La *phr. 3* reprend l'al. 2 de l'actuel art. 9 de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[61]. Le champ d'application personnel est en outre complété, au vu de l'art. 2, al. 1, let. b AP.

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 détenteur des données contenues dans le système de traitement (voir commentaire de l'art. 12 AP).

2.3 Section 3: Tâches du service

Art. 14 Renseignements sur les raccordements de télécommunication

L'*art. 14* reprend en substance l'art. 14, al. 2 de l'actuelle LSCPT. Les raccordements de télécommunication visés comprennent également les raccordements dans Internet (voir aussi commentaire de l'art. 1, al. 1 AP).

Art. 15 Tâches générales dans le domaine de la surveillance

L'*art. 15* mentionne les tâches du services 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 donc reprises des art. 11 et 13 de l'actuelle LSCPT. Contrairement à ce qui est la cas actuellement dans la LSCPT, il n'y a désormais 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. 16 AP).

La *let. a* reprend en substance les art. 11, al. 1, let. a et 13, al. 1, let. a de l'actuelle LSCPT.

La *let. b* reprend en substance les art. 11, al. 1, let. b et 13, al. 1, let. b de l'actuelle LSCPT. Il tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; les injonctions du service ne doivent donc pas seulement s'adresser aux fournisseurs de services postaux et de télécommunication, mais également aux personnes mentionnées à l'art. 2, al. 1, let. b AP. Quant au fait de mentionner la tâche de contrôle de l'exécution de la surveillance par le service, il ne fait que souligner le rôle d'intermédiaire que joue celui-ci entre les autorités de poursuite pénale et les personnes soumises à la LSCPT.

La *let. c* 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 l'art. 271, al. 1, modifié par le présent AP, et l'art. 274, al. 4, let. a du code de procédure pénale[62] ainsi qu'avec l'art. 70*b*, al. 1, modifié par le présent AP, et l'art. 70*e*, al. 4, let. a de la procédure pénale militaire[63]. Ces articles mentionnent le régime

61 RS **780.11**
62 RS ... (FF **2007** 6583)
63 RS **322.1**

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 de l'art. 271 du code de procédure pénale[64]). Le service prend les dispositions nécessaires permettant la mise en œuvre des mesures décidées dans le cadre des articles précités; mais il n'opère par exemple pas lui-même le tri dont il est fait mention dans ces articles (art. 271, al. 1 du code de procédure pénale[65] et art. 70*b*, al. 1 de la procédure pénale militaire[66]).

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

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

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. 15*, car elles ne correspondent 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. La formule des art. 11, al. 2, phr. 1 et 13 al. 2, let. e de l'actuelle LSCPT n'est également pas reprise en substance dans l'*art. 15*, étant donné qu'elle est superflue, dès lors qu'elle ne prévoit que la possibilité – et non l'obligation – du service de fournir aux autorités et aux personnes qui exécutent des surveillances en vertu de la LSCPT des conseils techniques en matière de surveillance de la correspondance par poste et télécommunication. Nonobstant la suppression précitée, le service conserve bien entendu la faculté de fournir ces conseils aux autorités et personnes précitées.

Les tâches du service mentionnées à l'article 11 de l'actuelle LSCPT qui ne sont pas reprises dans l'art. 15 AP seront transférées dans l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[67]. Concernant les tâches du service mentionnées à l'art. 13 de l'actuelle LSCPT qui ne sont pas reprises dans l'art. 15 AP, voir le commentaire de l'art. 16 AP.

Art. 16 Tâches dans le domaine de la surveillance de la correspondance par télécommunication

L'*art. 16* mentionne des tâches du service qui sont spécifiques aux surveillances ordonnées dans le domaine de la correspondance par télécommunication, à l'exclusion de la correspondance par poste.

La tâche du service mentionnée à la *let. a* 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 soumise à la LSCPT, active dans le domaine de la correspondance par télécommunication, un ordre de surveillance qui n'est selon le service techniquement pas possible à exécuter ou dont l'exécution est liée à des difficultés importantes. Ce mécanisme sert en particulier à rendre l'autorité qui a ordonné la surveillance et l'autorité habilitée à autoriser la surveillance plus facilement conscientes de ces prétendues impossibilité ou difficultés. L'autorité ayant ordonné la surveillance et l'autorité habilitée à autoriser la surveillance pourront – sans y être obligées – tenir compte de cet avis pour, cas échéant, respectivement révoquer la surveillance ordonnée ou ne pas l'autoriser. Ce mécanisme permet ainsi notamment d'éviter les complications qui

64 RS ... (FF **2007** 6583)
65 RS ... (FF **2007** 6583)
66 RS **322.1**
67 RS **780.11**

découleraient d'un recours contre la décision du service de faire exécuter la surveillance, fondé sur le fait que cette exécution ne serait techniquement pas possible (art. 34, al. 2 AP; voir ch. 1.4.9). 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 (voir art. 34, al. 2 AP et ch. 1.4.9). Le mécanisme proposé permet en outre aux autorités précitées de prendre en considération les difficultés importantes qui seraient liées à l'exécution d'une surveillance ordonnée. Sont considérées comme difficultés importantes des coûts manifestement disproportionnés pour l'exécution de la surveillance ou des problèmes d'ordre légal. Le délai dans lequel le service devra informer l'autorité qui a ordonné la surveillance et l'autorité habilitée à autoriser la surveillance sera fixé dans une ordonnance. Ce délai devra bien évidemment être particulièrement court, notamment pour permettre à l'autorité ayant ordonné cette surveillance d'en ordonner, cas échéant, rapidement une autre.

La *let. b* reprend en substance l'art. 15, al. 2, phr. 1 de l'actuelle LSCPT. Elle le complète en tenant compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'elle ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP.

La *let. c* reprend en substance le texte de l'art. 13. al. 1, let. c de l'actuelle LSCPT. Elle le complète en tenant compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'elle ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP. Elle l'adapte au fonctionnement du nouveau système de surveillance, l'ISS, qui ne prévoit en principe plus la mise à la disposition des autorités concernées des données obtenues dans le cadre de la surveillance au moyen d'envois postaux de supports de données et de documents mais au moyen d'un droit d'accès au système exploité par le service (voir ch. 1.4.2).

La *let. d* modifie et complète le texte de l'art. 13. al. 1, let. d de l'actuelle LSCPT, qui concerne la modalité particulière et exceptionnelle d'exécution d'une surveillance que constitue le branchement direct (Direktschaltung). Dans le système de surveillance actuel, les données obtenues dans le cadre d'une surveillance ordonnée passent en principe par le service, en tant qu'interface entre les personnes chargées d'exécuter les surveillances ordonnées et les autorités ayant ordonné celles-ci, et sont enregistrées dans le système exploité par le service. Ceci est également le cas lorsque la surveillance ordonnée est une surveillance dite en temps réel (Echtzeit-Überwachung), c'est-à-dire qui n'est pas une surveillance rétroactive (rückwirkende Überwachung). Le nouveau système de surveillance, l'ISS, prévoira de ce point de vue un fonctionnement identique à celui mentionné ci-dessus (voir ch. 1.4.2 et art. 16, let. c et e AP). Lorsque l'exécution de la surveillance ordonnée a lieu sous la forme d'un branchement direct, les données provenant de la personne chargée d'exécuter la surveillance sont transférées par celle-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. d définit dans quelles conditions la modalité du branchement direct peut être utilisée dans le cadre d'une surveillance. Les cas dans

lesquels on peut avoir recours 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 que la loi lui attribue, entre les personnes chargées d'exécuter les surveillances ordonnées et les autorités concernées. L'art. 271, al. 2 du code de procédure pénale[68] et l'art. 70*b*, al. 2 de la procédure pénale militaire[69], dans sa version découlant du code de procédure pénale[70], 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 saurait retarder leur travail. En effet, 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. La *let. d* tient en outre compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP.

La *let. e* reprend pour l'essentiel l'art. 13, al. 1, let. e de l'actuelle LSCPT. Il tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP. Afin de désigner plus clairement les données qui correspondent à la notion de données secondaires et de le faire de manière uniforme dans le code de procédure pénale[71] (ainsi que dans la procédure pénale militaire[72], dans sa version découlant du code de procédure pénale[73]) et dans la future LSCPT, on remplace de plus dans la LSCPT l'expression qui désigne les données secondaires par celle, en substance identique, qui les désigne à l'art. 273, al. 1, let. a et b du code de procédure pénale[74] (et à l'art. 70*d*, al. 1, let. a et b de la procédure pénale militaire[75], dans sa version découlant du code de procédure pénale[76]). Les données secondaires dans le domaine de la correspondance par télécommunication sont donc désormais désignées comme suit: les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation. La *let. e* est en outre adaptée au fonctionnement du nouveau système de surveillance, l'ISS, qui ne prévoit en principe plus la mise à la disposition des autorités concernées des données obtenues dans le cadre de la surveillance au moyen d'envois postaux de supports de données et de documents mais au moyen d'un droit d'accès au système exploité par le service (voir ch. 1.4.2).

L'ordre, prévu à la *let. f*, que le service peut donner à la personne chargée d'exécuter la surveillance de la correspondance par télécommunication de ne lui transmettre que certaines données composant un flux de données considéré ne peut avoir lieu qu'avec l'accord préalable de l'autorité qui a ordonné la surveillance. Parmi le flux de données en question, il s'agit, par exemple, de n'obtenir que les données relatives au

68 RS ... (FF **2007** 6583)
69 RS **322.1**
70 RS ... (FF **2007** 6583)
71 RS ... (FF **2007** 6583)
72 RS **322.1**
73 RS ... (FF **2007** 6583)
74 RS ... (FF **2007** 6583)
75 RS **322.1**
76 RS ... (FF **2007** 6583)

trafic Internet ou à la téléphonie par Internet. 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. Cette tâche du service de n'exiger qu'une partie du flux des données a comme pendant l'obligation des personnes soumises à la LSCPT mentionnée à l'art. 21, al. 3, phr. 2 AP. Elle ne doit en outre pas être confondue avec la possibilité qu'a le service, sur requête de l'autorité qui a ordonné la surveillance, de ne mettre à la disposition de celle-ci qu'une partie des données qu'il a obtenues de la personne chargée d'exécuter la surveillance. Il est en outre tenu compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP.

Les tâches du service mentionnées à l'art. 13 de l'actuelle LSCPT qui ne sont pas reprises dans l'art. 16 AP, le seront dans l'art. 15 AP, à moins d'être supprimées (voir commentaire de l'art. 15 AP) ou d'être transférées dans l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication[77].

Art. 17 Contrôle de qualité

L'*art. 17* vise 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 qui aurait été constaté, par l'autorité de poursuite pénale considérée ou par lui-même, en relation avec les données livrées par les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT, en particulier en relation avec la qualité de celles-ci. Un tel problème existe, par exemple, lorsque, par hypothèse, l'autorité de poursuite pénale constate que les données dites secondaires obtenues lors d'une surveillance rétroactive démontrent 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.

L'*al. 2* prévoit que si, pour effectuer les contrôles précités, le service doit prendre connaissance du contenu de ces données, il doit au préalable, pour des motifs tenant à la protection des données, en obtenir l'autorisation de l'autorité qui a ordonné la surveillance. Il sied en effet de préciser que le service n'a pas, sans autre, le droit de 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 nécessaire si le service est en mesure d'effectuer ses contrôles sans devoir prendre connaissance des données considérées.

77 RS **780.11**

Art. 18 Certification

La tâche du service mentionnée à l'*art. 18* a pour but de contribuer à ce que les fournisseurs de services de télécommunication puissent exécuter sans problème les surveillances qu'ils sont chargés d'effectuer.

Cette tâche a pour corollaire la possibilité des fournisseurs de services de télécommunication de se faire certifier, ce qui permet de démontrer, si le certificat leur est attribué, qu'ils seront en mesure d'exécuter correctement le type de mesures de surveillance certifié. Dès lors que les grands fournisseurs de services de télécommunication actifs sur le marché suisse – qui sont utilisés par la grande majorité des utilisateurs – possèdent en principe la technique et le personnel nécessaires pour exécuter correctement les mesures de surveillance ordonnées, il est justifié de ne prévoir dans l'art. 18 AP qu'une possibilité pour les fournisseurs de services de télécommunication de se faire certifier, et non une obligation. Ceci, à la différence de ce qui est la cas dans la situation visée par l'art. 24 AP (voir commentaire de l'art. 24 AP). C'est le service qui certifie. Cette certification a lieu aux frais des fournisseurs de services de télécommunication, selon les modalités fixées par le service. Ceci implique que les tests de certification peuvent être effectués directement par le service ou par une tierce personne, le service se limitant dans ce cas-ci, au moment d'accorder ou non le certificat, à contrôler le protocole de certification suivi par cette tierce personne et les résultats de tests effectués par celle-ci. La possibilité qu'a le service de faire effectuer les tests de certification par une tierce personne est justifiée par le fait que ceux-ci impliquent un long travail, qui peut être incompatible avec les ressources en personnel du service.

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

Art. 19

L'*al. 1* se base sur l'art. 12, al. 1 de l'actuelle LSCPT. Il tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP, de manière à ce que les devoirs mentionnés n'obligent pas seulement les fournisseurs de services par poste mais également les personnes visées par l'art. 2, al. 1, let. b AP.

L'*al. 2*, qui s'inspire de l'art. 12, al. 2 de l'actuelle LSCPT, concerne la durée de conservation des données dites secondaires dans le domaine de la correspondance par poste. Afin de désigner plus clairement les données qui correspondent à la notion de données secondaires et de le faire de manière uniforme dans le code de procédure pénale[78] (ainsi que dans la procédure pénale militaire[79], dans sa version découlant du code de procédure pénale[80]) et dans la future LSCPT, on remplace dans la LSCPT l'expression qui désigne les données secondaires par celle, en substance identique, qui les désigne à l'art. 273, al. 1, let. a et b du code de procédure pénale[81]

78 RS ... (FF **2007** 6583)
79 RS **322.1**
80 RS ... (FF **2007** 6583)
81 RS ... (FF **2007** 6583)

(et à l'art. 70*d*, al. 1, let. a et b de la procédure pénale militaire[82], dans sa version découlant du code de procédure pénale[83]). Les données secondaires dans le domaine de la correspondance par poste sont donc désormais désignées comme suit: les données indiquant quand et avec quelles personnes la personne surveillée a été ou est en liaison par poste et les données relatives au trafic et à la facturation. L'allongement de six mois à douze mois de la durée de conservation des données secondaires dans le domaine de la correspondance par poste est notamment une conséquence de l'adoption partielle de la motion 06.3170 de Rolf Schweiger par le Parlement, laquelle demandait, entre autres, l'allongement d'autant de la durée de conservation des données secondaires dans le domaine de la correspondance par télécommunication, y compris par Internet (art. 23 AP). La problématique soulevée dans cette motion 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 relatives à la correspondance par poste (voir ch. 1.4.5).

L'art. 12 al. 3 de la LSCPT actuelle est en substance repris à l'art. 5 AP.

2.5 Section 5: Obligations dans le domaine de la surveillance de la correspondance par télécommunication

Art. 20 Renseignements sur les raccordements de télécommunication

L'*art. 20* reprend pour l'essentiel l'art. 14 de l'actuelle LSCPT. Les raccordements de télécommunication visés comprennent également les raccordements dans Internet (voir aussi commentaire de l'art. 1, al. 1 AP). La phrase initiale de l'*al. 1* reprend celle de l'art. 14, al. 1 de l'actuelle LSCPT et tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP, en prévoyant que les devoirs mentionnés n'obligent pas seulement les fournisseurs de services de télécommunication mais également les personnes visées par l'art. 2, al. 1, let. b AP. Ceci permet en particulier de saisir les revendeurs, par exemple de cartes SIM. Les renseignements mentionnés à l'art. 20 ne sont pas couverts par le secret des télécommunications, à la différence des communications et des données dites secondaires; ces renseignements peuvent donc être communiqués dans le cadre d'une procédure simplifiée[84]. Leur communication n'a donc pas à avoir lieu dans le cadre d'une procédure soumise aux conditions restrictives de l'art. 269 du code de procédure pénale[85], en particulier à la liste des infractions mentionnée à l'al. 2 de l'article précité[86]. Ces renseignements sont très importants pour l'avancement des investigations[87], lesquelles sont susceptibles, au vu de leurs résultats, de permettre d'ordonner une surveillance aux conditions strictes de l'art. 269 du code de procédure pénale[88].

82 RS **322.1**
83 RS ... (FF **2007** 6583)
84 Cf. le message du 1er juillet 1998 relatif à la LSCPT actuelle, FF **1998** 3722
85 RS ... (FF **2007** 6583)
86 Thomas HANSJAKOB, op. cit., n. 1 à 4 et 23 ad art. 14 LSCPT
87 Cf. le message du 1er juillet 1998 relatif à la LSCPT actuelle, FF **1998** 3722
88 RS ... (FF **2007** 6583)

L'*al. 1, let. a* reprend l'art. 14, al. 1, let. a de l'actuelle LSCPT, en y ajoutant le prénom et la date de naissance, lesquels sont des éléments d'identification classiques, également pour les autorités et aux fins mentionnées à l'art. 20 AP.

L'*al. 1, let. b* reprend l'art. 14, al. 1, let. b de l'actuel LSCPT.

L'*al. 1, let. c* reprend 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 raccordements (p.ex. téléphone fixe, mobile et Internet) dont dispose cette personne, et non pas seulement un type de raccordement dont celle-ci dispose. Cela permet de déterminer en connaissance de cause quel type de raccordement doit faire l'objet de la surveillance. Il sied aussi d'éviter de devoir interroger les fournisseurs de services de télécommunication autant de fois que la personne considérée a de types différents de raccordements.

L'*al. 2* reprend en substance l'art. 15, al. 5bis de l'actuelle LSCPT et tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP, en prévoyant que les devoirs mentionnés n'obligent pas seulement les fournisseurs de services de télécommunication mais également les personnes visées par l'art. 2, al. 1, let. b AP. Ceci permet en particulier de saisir les revendeurs, par exemple de cartes SIM à prépaiement. L'*al. 2* étend en outre au domaine d'Internet l'obligation qu'ont les personnes qui exécutent des surveillances de la correspondance de la télécommunication en vertu de la LSCPT de fournir les renseignements considérés. Alors que cette obligation vise aujourd'hui, dans le domaine de la téléphonie mobile, les cartes SIM à prépaiement, elle visera en effet également, dans le domaine d'Internet, les cartes "wireless" à prépaiement. Afin que les personnes qui exécutent des surveillances de la correspondance de la télécommunication en vertu de la LSCPT soient en mesure de satisfaire à leur obligation de renseignement précitée dans le domaine d'Internet, il y aura lieu d'étendre, dans l'ordonnance du 31 octobre 2001 sur le surveillance de la correspondance par poste et télécommunication[89], l'obligation de contrôle et d'enregistrement applicable au cartes SIM à prépaiement, faisant l'objet de l'art. 19*a* de l'ordonnance précitée, aux cartes "wireless" à prépaiement. Il sied de préciser que l'obligation de renseignement susmentionnée ne porte que sur les renseignements enregistrés lors de l'enregistrement qui doit avoir lieu avant la remise par une personne soumise à la LSCPT de cartes SIM à prépaiement ou de cartes "wireless" à prépaiement au moment de l'ouverture d'une relation commerciale (Erstregistrierung), et non sur les données concernant des personnes qui pourraient acquérir ces mêmes cartes par la suite. Ceci implique que les personnes soumises à la LSCPT ne doivent être en mesure de fournir, pendant la durée considérée, que les renseignements qu'ils ont dû exiger lors de la remise de ces cartes (Erstregistrierung), à l'exclusion de données sur d'éventuels acquéreurs futurs de ces mêmes cartes, un enregistrement subséquent de ces données n'étant pas obligatoire. En décider autrement impliquerait des formalités et un travail administratif excessifs (voir aussi commentaire de l'art. 6a de la loi sur les télécommunications du 30 avril 1997[90]). Il y a également lieu de noter que l'*al. 2* ne limite pas la portée de l'al. 3 de l'art. 20 AP; en effet, les personnes visées par l'*al. 2* doivent également respecter l'obligation qui découle de l'al. 3.

89 RS **780.11**
90 RS **784.10**

L'*al. 3* reprend et complète l'art. 14, al. 4 de la LSCPT actuelle, au vu de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP. Il prévoit que le devoir mentionné n'oblige pas seulement les fournisseurs d'accès à Internet mais également les personnes visées par l'art. 2, al. 1, let. b AP. Pour des raisons de cohérence avec le rôle d'interface attribué au service dans la LSCPT, il est mentionné que les indications visées doivent être fournies au service, et non pas, comme dans l'actuelle LSCPT, à l'autorité compétente[91].

L'*al. 4* reprend l'art. 14, al. 3 de l'actuelle LSCPT et le complète en reprenant les phr. 2 des al. 5 et 6 de l'art. 15 de la LSCPT actuelle.

Art. 21 Obligations lors de l'exécution de surveillances

L'*al. 1* reprend en substance l'art. 15, al. 1 de l'actuelle LSCPT et le complète, au vu de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP. Il prévoit que les devoirs mentionnés n'obligent pas seulement les fournisseurs de services de télécommunication mais également les personnes visées par l'art. 2, al. 1, let. b AP. Afin de désigner plus clairement les données qui correspondent à la notion de données secondaires et de le faire de manière uniforme dans le code de procédure pénale[92] (ainsi que dans la procédure pénale militaire[93], dans sa version découlant du code de procédure pénale[94]) et dans la future LSCPT, on remplace dans la LSCPT l'expression qui désigne les données secondaires par celle, en substance identique, qui les désigne à l'art. 273, al. 1 let. a et b du code de procédure pénale[95] (et à l'art. 70*d*, al. 1 let. a et b de la procédure pénale militaire[96], dans sa version découlant du code de procédure pénale[97]). Les données secondaires dans le domaine de la correspondance par télécommunication sont donc désormais désignées comme suit: les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation. Le renvoi à l'art. 16, let. d AP ne fait que mettre en évidence le fait que, dans le cas d'une surveillance exécutée par branchement direct, les données recueillies sont, exceptionnellement, directement transmises au service de police désigné par l'autorité qui a ordonné la surveillance, et non pas d'abord au service, qui joue en principe le rôle d'intermédiaire.

L'*al. 2* reprend en substance l'art. 15, al. 4 de l'actuelle LSCPT. Il le complète, au vu de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP, en prévoyant que les devoirs mentionnés n'obligent pas seulement les fournisseurs de services de télécommunication mais également les personnes visées par l'art. 2, al. 1, let. b AP. Afin de désigner plus clairement les données qui correspondent à la notion de données secondaires et de le faire de manière uniforme dans le code de procédure pénale[98] (ainsi que dans la procédure pénale militaire[99], dans sa version découlant du code de procédure pénale[100]) et

91 Thomas HANSJAKOB, op. cit., n. 24 ad art. 14 LSCPT
92 RS ... (FF **2007** 6583)
93 RS **322.1**
94 RS ... (FF **2007** 6583)
95 RS ... (FF **2007** 6583)
96 RS **322.1**
97 RS ... (FF **2007** 6583)
98 RS ... (FF **2007** 6583)
99 RS **322.1**

dans la future LSCPT, on remplace dans la LSCPT l'expression qui désigne les données secondaires par celle, en substance identique, qui les désigne à l'art. 273, al. 1 let. a et b du code de procédure pénale[101] (et à l'art. 70*d*, al. 1 let. a et b procédure pénale militaire[102], dans sa version découlant du code de procédure pénale[103]). Les données secondaires dans le domaine de la correspondance par télécommunication sont donc désormais désignées comme suit: les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation.

L'*al. 3* mentionne l'obligation des personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT de ne transmettre au service, à la demande de celui-ci, qu'une partie du flux des données considéré. Cette obligation a comme pendant la tâche du service mentionnée à l'art. 16, let. f AP. Dès lors que le transfert d'une partie seulement du flux de données considéré est susceptible d'impliquer, par le tri qu'il suppose, un surcroît de travail pour les personnes soumises à la LSCPT par rapport au transfert de tout ce flux, il y a lieu de prévoir une base légale le prévoyant. Cette obligation ne doit en outre pas être confondue avec la possibilité qu'a le service, sur requête de l'autorité qui a ordonné la surveillance, de ne mettre à la disposition de celle-ci qu'une partie des données qu'il a obtenues de la personne chargée d'exécuter la surveillance. (Pour le surplus, voir le commentaire de l'art. 16, let. f AP.) L'*al. 3* tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP.

L'*al. 4* décrit les obligations spécifiques des personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT dans la mise en œuvre du procédé de surveillance prévu à l'art. 270bis du code de procédure pénale[104] et à l'art. 70a^{bis} de la procédure pénale militaire[105], introduits dans dits code par le présent AP. Ce procédé consiste à accéder au système informatique surveillé pour y intégrer un ou des programmes informatiques, dans le but de permettre, d'une part, l'interception et, d'autre part, la lecture des données sans cryptage (voir commentaire de l'art. 270bis du code de procédure pénale[106]). Dans l'exécution de ce procédé de surveillance, les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT doivent au besoin fournir au service un concours particulier, allant au-delà des obligations qui sont en principe les leurs, rendu nécessaire par les spécificités du mode de surveillance considéré. Ce concours est soumis à la condition qu'il soit techniquement nécessaire pour la bonne exécution de la surveillance. L'*al. 4* tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs d'accès à Internet mais encore aux personnes visées à l'art. 2, al. 1, let. b AP. Ceci permet en particulier de saisir des personnes à qui des données font l'objet d'un "outsourcing" par des fournisseurs de services de télécommunication.

100 RS ... (FF **2007** 6583)
101 RS ... (FF **2007** 6583)
102 RS **322.1**
103 RS ... (FF **2007** 6583)
104 RS ... (FF **2007** 6583)
105 RS **322.1**
106 RS ... (FF **2007** 6583)

L'*al. 5* reprend en substance l'art. 15, al. 2 phr. 2 de l'actuelle LSCPT. Il le complète, au vu de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP, en prévoyant que les devoirs mentionnés n'obligent pas seulement les fournisseurs de services de télécommunication mais également les personnes visées par l'art. 2, al. 1, let. b AP.

Art. 22 Identification des utilisateurs qui accèdent à Internet

L'*art. 22* prévoit l'obligation des personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT de prendre les mesures techniques nécessaires permettant l'identification des utilisateurs accédant à Internet par leur entremise. Cette obligation s'applique à tous les modes d'accès à Internet, dans les limites qui découlent de l'art 20, al. 2 AP. Elle complète en outre l'art. 20, al. 3 AP. L'art. 22 AP oblige spécialement les fournisseurs d'accès à Internet (Internet-Anbieter/Zugangsvermittler) et a une portée particulière pour les cas dans lesquels les utilisateurs accèdent à Internet par le biais d'un réseau sans fil (wireless LAN, WLAN, wireless local area network, hotspot, Wi-Fi, etc.). Cet article vise notamment les cas où un tel réseau d'un internet café ou cyber café, d'une école, d'une commune, d'un hôtel, d'un restaurant, d'un hôpital ou d'un particulier, par exemple, est laissé par ceux-ci à la disposition des tiers utilisateurs (par exemple les clients de l'hôtel) pour accéder à Internet, que ce soit à titre payant ou gratuit (voir aussi commentaire de l'art. 2, al. 1 AP). Dans ce cas, le fournisseur d'accès à Internet (Internet-Anbieter/Zugangsvermittler) des établissements, organismes et personnes précités (par exemple de l'hôtel) doit être en mesure d'identifier ces tiers, respectivement les ordinateurs personnels de ceux-ci qui se sont connectés à Internet au moyen du réseau considéré. Une telle identification peut avoir lieu de différentes manières. Il appartient au fournisseur de services de télécommunication considéré de prendre les mesures nécessaires, au besoin avec le concours du "titulaire" du réseau Internet visée (par exemple de l'hôtel), pour satisfaire à son obligation d'identification. Cette identification peut par exemple avoir lieu – que l'accès à Internet soit gratuit ou payant – par le biais d'un téléphone portable: Le tiers utilisateur qui désire se connecter à Internet doit au préalable communiquer son numéro de téléphone portable, avant de recevoir, en l'espace de quelques secondes, un mot de passe lui permettant de s'y connecter. Ainsi, grâce à ce numéro de téléphone portable, le fournisseur de services de télécommunication considéré est en mesure de contribuer à l'identification de la personne qui a accédé à Internet par son entremise. L'*art. 22* tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs d'accès à Internet mais encore aux personnes visées à l'art. 2, al. 1, let. b AP. Ceci permet en particulier de saisir des personnes à qui des données font l'objet d'un "outsourcing" par des fournisseurs de services de télécommunication. (Voir aussi le commentaire de l'art. 2, al. 1 AP.)

Art. 23 Conservation des données

L'*art. 23*, qui s'inspire de l'art. 15, al. 3 de l'actuelle LSCPT, concerne la durée de conservation des données dites secondaires dans le domaine de la correspondance par télécommunication. Afin de désigner plus clairement les données qui correspondent à la notion de données secondaires et de le faire de manière uniforme

dans le code de procédure pénale[107] (ainsi que dans la procédure pénale militaire[108], dans sa version découlant du code de procédure pénale[109]) et dans la future LSCPT, on remplace dans la LSCPT l'expression qui désigne les données secondaires par celle, en substance identique, qui les désigne à l'art. 273, al. 1, let. a et b du code de procédure pénale[110] (et à l'art. 70*d*, al. 1 let. a et b procédure pénale militaire[111], dans sa version découlant du code de procédure pénale[112]). Les données secondaires dans le domaine de la correspondance par télécommunication sont donc désormais désignées comme suit: les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation. L'allongement de six mois à douze mois de la durée de conservation des données secondaires dans le domaine de la correspondance par télécommunication, y compris par Internet, est notamment une conséquence de l'adoption partielle de la motion 06.3170 de Rolf Schweiger par le Parlement (voir ch. 1.4.5). Le même allongement est prévu pour la durée de conservation des données secondaires dans le domaine de la correspondance par poste (voir commentaire de l'art. 19, al. 2, AP). L'*art. 23* tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP.

Art. 24 Certification

La prise en charge par les fournisseurs de services de télécommunication qui ne se sont pas fait certifier des frais liés à la nécessité de recourir à un tiers ou au service pour la bonne exécution des surveillances ordonnées, prévue à *l'art. 24, phr. 1*, est la contrepartie du fait que leur certification est en principe facultative (voir commentaire de l'art. 18 AP). Cette réglementation est susceptible d'être une incitation pour ces fournisseurs à se faire certifier, au sens de l'art. 18 AP. Dans le cas de figure de l'*art 24, phr. 2*, les fournisseurs de services de télécommunication n'ont, à la différence de ce qui est le cas dans la situation visée par l'art. 18 AP, plus la possibilité de choisir de se faire certifier ou non; ils doivent en effet le faire, selon les mêmes modalités que celles prévues par l'art. 18 AP, afin de démontrer qu'ils seront, cas échéant, en mesure d'exécuter correctement les prochaines mesures de surveillance qui seront ordonnées.

Art. 25 Information sur les technologies et services

L'*art. 25* vise, tout comme l'art. 24 AP, à garantir que les surveillances ordonnées puissent être exécutées correctement. 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 se seraient passés lors de l'exécution de ces surveillances. L'art. 25 sert également à prendre sans tarder les mesures nécessaires pour, cas échant, permettre au Conseil fédéral de fixer par

107 RS ... (FF **2007** 6583)
108 RS **322.1**
109 RS ... (FF **2007** 6583)
110 RS ... (FF **2007** 6583)
111 RS **322.1**
112 RS ... (FF **2007** 6583)

voie d'ordonnance, en vertu de l'art. 30, al. 2, phr. 2, AP, un montant forfaitaire en guise d'émolument pour l'exécution d'un type de surveillance nouvellement introduit, qui ne rentrerait pas dans la catégorie d'un autre type de surveillance déjà mentionné dans dite ordonnance. Il sied à cet égard de noter que, en vertu de l'art. 4 de l'ordonnance du 7 avril 2004 sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication[113], laquelle s'inscrit dans le système de l'actuelle LSCPT (voir le commentaire de l'art. 30 AP), l'émolument que doit verser au service l'autorité qui a ordonné la surveillance n'est, lorsque la surveillance considérée n'est pas prévue dans l'ordonnance précitée, pas fixé sur la base d'un forfait mais en fonction du temps et des moyen techniques mis en œuvre ("nach Aufwand") par le service[114]. Au vu des objectifs poursuivis par l'*art. 25*, l'obligation de renseignement prévue dans cette disposition existe indépendamment du fait de savoir si la technologie ou le service en question a été ou non développé par la personne considérée soumise à la LSCPT. L'*art. 25* tient compte de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP; il est donc précisé qu'il ne renvoie pas seulement aux fournisseurs de services de télécommunication mais encore aux personnes visées à l'art. 2, al. 1, let. b AP.

Art. 26 Exploitants de réseaux de télécommunication internes et de centraux domestiques et personnes visées à l'art. 2, al. 1, n'exerçant pas leur activité à titre professionnel

L'*art. 26* reprend l'art. 15, al. 8 de l'actuelle LSCPT et le complète en relation avec le contenu de l'art. 2, al. 2, AP.

2.6 Section 6: Surveillance en dehors d'une procédure pénale

Art. 27 Recherche dans un cas d'urgence

L'*art. 27* regroupe, en substance, les art. 3*a*, 6, let. d, 8, al. 5 et 9, al. 1bis de l'actuelle LSCPT. Le contenu des articles précités est, en vertu de la loi fédérale sur l'organisation des autorités pénales de la Confédération[115], censé être intégré dans l'art. 3 de la LSCPT actuelle. Le texte considéré est repris dans l'art. 27 de la nouvelle LSCPT. Pour des motifs de clarté, il est expressément précisé que la surveillance peut bien entendu viser la localisation de la personne considérée. Cette réglementation n'a pas sa place dans le code de procédure pénale[116], dès lors qu'elle ne s'applique pas à une procédure pénale en cours. La surveillance en question ne peut porter que sur les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic, soit des données dites secondaires, ainsi que sur la localisation de la personne surveillée. Elle ne peut en revanche porter sur des communications, le contenu de conversations. En cas de nécessité, en conformité avec le principe constitutionnel de la proportionnalité, il est possible de surveiller un raccordement

113 RS **780.115.1**
114 Arrêt du Tribunal fédéral du 20 mars 2007, 1A.255/2006, consid. 3.4 et 3.5
115 RS ... (FF **2008** 7371)
116 RS ... (FF **2007** 6583)

qui n'est pas celui de la personne disparue mais celui 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.

Art. 28 Recherche de personnes condamnées

L'*art. 28* prévoit désormais la possibilité 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 possibilité s'impose, notamment du fait qu'elle est déjà prévue dans le domaine de l'entraide pénale internationale[117], en vertu de l'art. 18*a*, al. 1 de la loi fédérale du 20 mars 1981 sur l'entraide pénale internationale[118]. Cette réglementation, à l'instar de celle de l'art. 27 AP, n'a pas sa place dans le code de procédure pénale[119], dès lors qu'elle aussi ne s'applique pas à une procédure pénale en cours, celle-ci étant à ce stade terminée. A l'instar de ce que prévoient en substance les art. 269 al. 1, let. c du code de procédure pénale[120] et 27, al. 2, let. a AP, cette mesure de surveillance est subsidiaire aux autres mesures qui peuvent être entreprises pour trouver la personne recherchée. Contrairement à ce qui est le cas de la surveillance faisant l'objet de l'art. 27 AP, la surveillance ne se limite pas à des données dites secondaires, mais peut également porter sur les conversations, susceptibles de donner des renseignements sur le lieu où se trouve la personne condamnée ou faisant l'objet de la mesure entraînant une privation de liberté.

Art. 29 Procédure

L'*art. 29* mentionne la procédure applicable dans les cas visés par les art. 27 et 28 AP.

Pour ce qui concerne la procédure, l'*al. 1* effectue un renvoi, par analogie, aux art. 271 à 279 du code de procédure pénale[121]. Dès lors que, dans l'art. 28 AP, l'on est en présence d'un jugement définitif et exécutoire, et pas seulement de graves soupçons de commission d'une infraction, il n'y a pas lieu de subordonner le recours à une telle surveillance aux conditions, supplémentaires, de l'art. 269, al. 1, let. a et b du code de procédure pénale[122], que constituent la mention de l'infraction considérée dans la liste figurant à l'art. 269, al. 2 dudit code et la justification au regard de la gravité de l'infraction.

L'*al. 2* règle la compétence pour ordonner et autoriser une surveillance faisant l'objet des art. 27 et 28 AP. Dans le domaine de l'entraide pénale internationale, ces questions sont réglées à l'art. 18*a* de la loi fédérale du 20 mars 1981 sur l'entraide pénale internationale[123], dans sa version modifiée par le code de procédure pénale[124]. Dans dit domaine, la compétence d'ordonner la surveillance pour

117 Thomas HANSJAKOB, op. cit., n. 8 ad art. 1 LSCPT
118 RS **351.1**
119 RS ... (FF **2007** 6583)
120 RS ... (FF **2007** 6583)
121 RS ... (FF **2007** 6583)
122 RS ... (FF **2007** 6583)
123 RS **351.1**
124 RS ... (FF **2007** 6583)

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.

2.7 Section 7: Frais et émoluments

Art. 30

L'*al. 1* reprend l'art. 16, al. 1 de la LSCPT dans sa version découlant du programme de consolidation (PCO) 2011-2013[125], lequel a été mis en consultation le 14 avril 2010 par le Conseil fédéral et supprime l'indemnisation des personnes qui exécutent des surveillances en vertu de la LSCPT (voir ch. 1.4.6). L'*al. 1* complète en outre ce texte, au vu de la modification du champ d'application personnel de la LSCPT, qui découle de l'art. 2, al. 1, let. b AP, en prévoyant que ne sont pas seulement concernés les fournisseurs de services postaux et les fournisseurs de services de télécommunication mais également les personnes visées par l'art. 2, al. 1, let. b AP. Le versement d'une indemnité aux personnes qui exécutent des surveillances en vertu de la LSCPT en relation avec leurs obligations découlant de l'art. 21, al. 4 AP n'est également pas prévu.

L'*al. 2, phr. 1*, précise expressément, pour des raisons de clarté, que l'autorité qui a ordonné la surveillance doit verser un émolument au service pour les prestations y relatives fournies par celui-ci. L'*al. 2, phr. 2* reprend l'art. 16, al. 2 de la LSCPT dans sa version découlant du programme de consolidation (PCO) 2011-2013[126] (voir ch. 1.4.6), qui est la disposition sur laquelle se fonde l'ordonnance du Conseil fédéral dans laquelle celui-ci fixe ces émoluments[127], en fonction du type de surveillance considéré. Il n'y est plus fait mention des indemnités, dès lors que le versement de celles-ci n'est en effet plus prévu, à l'al. 1. Le Conseil fédéral devra notamment régler, dans l'ordonnance précitée, l'émolument que l'autorité qui a ordonné une surveillance prévue à l'art. 270bis du code de procédure pénale[128] ou à l'art. 70a^{bis} de la procédure pénale militaire[129] doit verser au service. En fixant dans cette ordonnance le montant de l'émolument prévu pour chaque type de surveillance considéré, le Conseil fédéral décide à quelle hauteur la somme totale des émoluments versés doit couvrir les frais de fonctionnement du service.

Dans le système qui prévoit le versement d'une indemnité équitable aux personnes qui exécutent des surveillances en vertu de la LSCPT, l'autorité qui a ordonné la surveillance verse tout d'abord un montant au titre d'émolument au service. Celui-ci verse ensuite – en fonction du type de surveillance considéré – tout ou partie de cette somme à la personne ayant exécuté la surveillance, au titre d'indemnité, et garde le solde éventuel en contrepartie des prestations fournies à l'autorité qui a ordonné la surveillance[130]. Dans le système de l'art. 16, al. 1 de la LSCPT dans sa version découlant du programme de consolidation (PCO) 2011-2013[131] (voir ch. 1.4.6) et dans le système correspondant de la future LSCPT, lesquels prévoient au contraire

125 http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf
126 http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf
127 RS **780.115.1**
128 RS ... (FF **2007** 6583)
129 RS **322.1**
130 RS **780.115.1**
131 http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf

l'absence d'indemnisation des personnes qui exécutent des surveillances en vertu de la LSCPT, le montant que l'autorité qui a ordonné la surveillance verse au titre d'émolument au service ne comprend donc plus la part correspondant à l'indemnité précitée.

Il sied encore simplement de mentionner ici, pour le surplus, 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 dite 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 du code de procédure pénale[132]).

2.8 Section 8: Dispositions pénales

Art. 31 Contraventions

Les contraventions prévues à l'*art. 31* peuvent être commises par des individus, en vertu de l'art. 2 AP, ou, en vertu de l'*al. 4*, par des entreprises, tombant également dans le champ d'application personnel de la LSCPT, selon l'art. 2 AP.

L'amende maximale que prévoit l'*al. 1* pour la commission intentionnelle des infractions prévues aux let. a et b est supérieure au montant maximal de l'amende prévu à l'art. 106, al. 1 du code pénal[133], qui est de 10 000 francs. Ce dernier montant est en effet dans certains cas susceptible d'être trop bas pour dissuader de commettre l'une des infractions précitées, au vu des économies pouvant être réalisées en ayant les comportements réprimés.

La mention à l'al. 2 relative à la punissabilité de la tentative et de la complicité est rendue nécessaire par l'art. 105, al. 2 du code pénal[134].

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 du code pénal[135]. 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.

L'*al. 4* a pour but de permettre de punir, outre les individus, visés par l'al. 1, également les entreprises, tombant dans le champ d'application personnel de la LSCPT, selon l'art. 2 AP, qui commettraient les infractions mentionnées aux let. a et b de l'al. 1. Dès lors que l'application de l'art. 102, al. 1, 3 et 4 du code pénal[136] est exclue, en vertu de l'art. 105, al. 1 de ce même code, les infractions visées par les let. a et b de l'al. 1 étant des contraventions, il y a lieu, pour atteindre le but poursuivi, de prévoir expressément l'application par analogie de l'art. 102, al. 1, 3 et 4 du code pénal[137] et de l'art. 112 du code de procédure pénale[138], lequel remplace l'art. 102*a*

132 RS ... (FF **2007** 6583)
133 RS **311.0**
134 RS **311.0**
135 RS **311.0**
136 RS **311.0**
137 RS **311.0**
138 RS ... (FF **2007** 6583)

du code pénal[139], avec l'entrée en vigueur du code de procédure pénale[140]. L'amende maximale est toutefois fixée à un million de francs, dès lors que l'amende maximale prévue à l'art. 102, al. 1 du code pénal[141], pour des crimes et des délits, qui est de cinq millions de francs, semble trop élevée au regard des infractions considérées.

Pour le surplus relatif à l'art. 31, voir ch. 1.4.7.

Art. 32 Juridiction

L'*art. 32* n'instaure pas la compétence d'une autorité administrative fédérale de poursuivre et de juger les infractions. La loi fédérale du 22 mars 1974 sur le droit pénal administratif[142] n'est pas applicable. Les cantons sont donc compétents pour ce faire, comme c'est en principe la règle.

2.9 Section 9: Surveillance et voies de droit

Art. 33 Surveillance

L'*al. 1* est une norme analogue à l'art. 58, al. 1 de la loi du 30 avril 1997 sur les télécommunications[143]. 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 de la loi du 30 avril 1997 sur les télécommunications[144]. 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. Cas échéant, cet article permet au service de prononcer des sommations de remédier au manquement constaté ou des sommations de prendre les 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 de la loi du 30 avril 1997 sur les télécommunications[145]. En plus de prononcer les mesures précitées, le service peut déposer une dénonciation pénale, en se fondant sur l'art. 31 AP. Il sied de préciser que des mesures plus incisives que celles relevant de la compétence du service en vertu de l'al. 2 continuent – comme cela est actuellement le cas – de pouvoir être prononcées en cas de violation du droit relatif à la surveillance de la correspondance par poste et télécommunication. Il revient toutefois au Département fédéral de l'environnement, des transports, de l'énergie et de la communication, concernant la correspondance par poste, et à l'Office fédéral de la communication ainsi qu'à la Commission fédérale de la communication, concernant la correspondance par télécommunication, de prendre ces mesures. Comme actuellement, l'Office fédéral de la communication et la Commission fédérale de la communication peuvent agir sur la base des art. 58 et 60 de la loi du 30 avril 1997 sur les télécommunications[146]

139 RS **311.0**
140 RS ... (FF **2007** 6583)
141 RS **311.0**
142 RS **313.0**
143 RS **784.10**
144 RS **784.10**
145 RS **784.10**
146 RS **784.10**

et le service informe ces autorités des violations qu'il a constatées afin de permettre à celles-ci de prendre, cas échéant, les mesures précitées.

Pour le surplus relatif à l'art. 33, voir ch. 1.4.8.

Art. 34 Voies de droit

L'*al. 1* est la disposition générale qui régit les recours contre les décisions rendues par le service. Il régit en particulier les recours contre les décisions du service fixant les émoluments (voir aussi le commentaire de l'art. 30 AP).

L'*al. 2* est une disposition spéciale par rapport à l'al. 1 AP. Il vise en effet les recours contre un type particulier de décisions du service, à savoir celles de faire exécuter une surveillance, fondée sur un ordre de surveillance rendu par l'autorité compétente. A la différence de ce qui est le cas pour les décisions visées par l'al. 1, les griefs invocables contre ces décisions sont limités.

Pour le surplus relatif à l'art. 34, voir ch. 1.4.9.

2.10 Section 10: Dispositions finales

Art. 35 Exécution

L'*art. 35* 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. 29 al. 2 AP.

Art. 36 Abrogation et modification du droit en vigueur

L'annexe à laquelle renvoie l'*art. 36* dispose en substance en son ch. I que la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[147] 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. 36* mentionne les lois qui sont modifiées, sans être abrogées, par l'entrée en vigueur de la nouvelle LSCPT:

Code de procédure pénale suisse dans sa version du 5 octobre 2007[148]

Art. 269, al. 2, let. a

Le 1er janvier 1984, la Convention du 25 octobre 1980 sur les aspects civils de l'enlèvement international d'enfants[149] est entrée en vigueur pour la Suisse. Cette convention oblige la Suisse à localiser un enfant déplacé ou retenu illicitement au moyen de toutes les mesures appropriées pour ce faire (art. 7, let. a de la Convention). La poursuite pénale du parent qui a enlevé l'enfant pour enlèvement de

147 RO
148 RS ... (FF **2007** 6583)
149 RS **0.211.230.02**

mineur (art. 220 CP[150]) fait également partie de ces mesures. Différentes mesures d'instruction et de contrainte relevant de la procédure pénale servant aussi à localiser le parent ayant enlevé l'enfant (comme par exemple la surveillance des cartes de crédit ou les perquisitions) sont aujourd'hui, certes, disponibles dans le cadre d'une procédure pénale. Une surveillance de la correspondance par poste et télécommunication ne peut en revanche être ordonnée, étant donné que l'énoncé de fait légal de l'enlèvement de mineur (art. 220 CP[151]) ne figure pas dans le catalogue des infractions pour la poursuite desquelles une telle surveillance peut être ordonnée. Ceci n'a par erreur pas été changé jusqu'à ce jour, également avec l'adoption de la loi fédérale du 21 décembre 2007[152] sur l'enlèvement international d'enfants et les Conventions de La Haye sur la protection des enfants et des adultes. Il y a lieu de remédier à cet oubli en complétant l'*art. 269, al. 2, let. a* du code de procédure pénale.

Art. 270, let. b, ch. 1 (texte en français)

Le texte actuel en français ne couvre que la réception d'envois et de communications par le prévenu au moyen de l'adresse postale ou du raccordement 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 du tiers, à l'instar de ce que permettent les textes en allemand et en italien. Le texte en français est donc adapté à ces textes-ci.

Art. 270bis Interception et décryptage de données *(nouveau)*

L'*al. 1* constitue la base légale expresse pour recourir, sur ordre du ministère public, à un procédé faisant appel à des outils de surveillance particuliers, qui consiste à accéder au système informatique surveillé pour y intégrer un ou des programmes informatiques particuliers, dans le but de permettre, d'une part, l'interception et, d'autre part, la lecture des données. L'*art. 270bis* constitue – si les conditions qu'il pose sont respectées – un fait justificatif légal par rapport à la surveillance considérée, laquelle serait autrement susceptible de tomber sous le coup de l'art. 143bis du code pénal[153]; à ces conditions, une telle surveillance est en effet licite (art. 14 du code pénal[154]).

Ce procédé a une portée particulière dans le domaine de la surveillance de la téléphonie par Internet (Voice over IP [VoIP]), plus précisément dans la téléphonie par Internet du type Peer-to-Peer, qui met en communication deux ordinateurs, étant donné que dans ce type de téléphonie les données communiquées et interceptées sont cryptées et, donc, illisibles et inutilisables. Le procédé de surveillance considéré consiste à introduire un programme particulier dans l'ordinateur surveillé qui permet d'avoir accès sans cryptage aux données échangées. Ce procédé 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

150 RS **311.0**
151 RS **311.0**
152 RS **211.222.32**
153 RS **311.0**
154 RS **311.0**

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. Si ce programme ne peut, dans les deux cas de figure précités, déployer ses effets parce que l'ordinateur surveillé est équipé d'un antivirus qui le neutralise, le procédé de surveillance mentionné à l'*art. 270bis* permet d'introduire dans l'ordinateur surveillé un programme complémentaire, qui a pour but de déjouer l'antivirus, de manière à tout de même permettre au programme susmentionné de déployer ses effets, permettant ainsi d'intercepter et de lire les données.

Le procédé de surveillance considéré à l'*art. 270bis* nécessite un comportement plus invasif que les autres procédés. En effet, alors qu'avec les autres procédés de surveillance les informations recueillies proviennent simplement de données stockées ou sont simplement déviées, leur obtention nécessite, lorsqu'on a recours au procédé visé par l'*art. 270bis*, de pénétrer activement dans le système informatique surveillé. Au vu des caractéristiques de ce procédé, l'utilisation de celui-ci ne constitue donc plus une simple question technique. C'est la raison pour laquelle le recours à ce procédé n'est pas régi dans la nouvelle LSCPT mais dans le code de procédure pénale[155]. Les obligations spécifiques des personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT (art. 2, al. 1 AP) dans la mise en œuvre du procédé de surveillance prévu à l'*art. 270bis* sont toutefois mentionnées dans la nouvelle LSCPT, à l'art. 21 al. 4 AP.

Le procédé de surveillance en question permet d'accéder à l'ensemble du système informatique dans lequel le programme informatique est introduit. Il permet donc d'accéder à des données d'emblée sans rapport avec les motifs justifiant une surveillance, comme par exemple, suivant les cas, des correspondances, des photos et des films relevant de la sphère privée, voire intime. Pour éviter une consultation de données d'emblée inutiles, la dernière phr. de l'al. 1 exige donc que le ministère public indique le type de données qu'il souhaite obtenir au moyen de la surveillance qu'il ordonne.

Il sied de noter que le recours à ce procédé de surveillance est, au vu des caractéristiques précitées de celui-ci, subsidiaire aux autres mesures de surveillance de la correspondance par télécommunication. Ceci est justifié, au vu du fait que ce procédé est plus invasif que ces autres mesures de surveillance. Le recours à ce procédé de surveillance n'est donc possible qu'à de strictes conditions supplémentaires (par rapport à celles mentionnées à l'art. 269 du code de procédure pénale[156]), c'est-à-dire que si les autres mesures de surveillance déjà prises sont restées sans succès ou lorsque les autres mesures de surveillance n'auraient aucune chance d'aboutir ou rendraient la surveillance excessivement difficile, conditions dont l'existence devra être contrôlée par l'autorité habilitée à autoriser la surveillance (al. 2 et art. 274 du code de procédure pénale[157]). Il sied à cet égard encore de ne pas perdre de vue que le recours aux autres mesures de surveillance elles-mêmes est déjà subsidiaire par rapport aux mesures d'instruction dites classiques (art. 269, al. 1, let. c du code de procédure pénale[158]), ce qui confère en somme un caractère de "double subsidiarité" au procédé de surveillance visé par l'*art. 270bis* par rapport à ces

155 RS ... (FF **2007** 6583)
156 RS ... (FF **2007** 6583)
157 RS ... (FF **2007** 6583)
158 RS ... (FF **2007** 6583)

mesures d'instructions classiques. Ce qui précède permet de garantir que ce procédé de surveillance ne sera utilisé que si cela est vraiment nécessaire. Il n'est en revanche pas nécessaire pour ce faire de limiter l'usage de ce procédé de surveillance à un catalogue d'infractions plus restreint que celui figurant à l'art. 269, al. 2 du code de procédure pénale[159]. En effet, toutes les infractions mentionnées dans l'article précité sont susceptibles, dans un cas particulier, de présenter une gravité justifiant d'avoir recours à ce procédé de surveillance. En outre, l'art. 269, al. 1, let. b du code de procédure pénale[160] exige déjà que l'infraction présente une gravité particulière pour avoir recours à une mesure de surveillance de la correspondance par télécommunication, ce qui vaut en particulier également pour le procédé de surveillance précité.

La personne dans le système informatique de laquelle un ou des programmes informatiques auront été intégrés dans le but de permettre la surveillance ordonnée sera avertie de l'installation de ce ou ces programmes, en vertu de l'art. 279 du code de procédure pénale[161].

L'*al. 2* prévoit que, comme toute mesure de surveillance ordonnée, celle qui fait l'objet de l'al. 1 doit être soumise à l'autorisation du tribunal des mesures de contrainte. Les caractéristiques du procédé de surveillance considéré impliquent également que c'est expressément qu'une telle surveillance ordonnée doit être autorisée par le tribunal des mesures de contrainte, conformément à l'art. 274, al. 4, let. c du code de procédure pénale[162], qui est une disposition nouvelle, introduite par la nouvelle LSCPT.

Art. 270ter Utilisation de systèmes de localisation *(nouveau)*

L'*al. 1* constitue la base légale expresse pour l'utilisation, par la police, sur ordre du ministère public, d'appareils particuliers, dans le but de garantir la sécurité publique. Ces appareils servent à déterminer des données spécifiques permettant l'identification d'un appareil de téléphonie mobile utilisé, comme par exemple le numéro d'identification international de celui-ci (numéro IMEI) ou le numéro de la carte d'identification de l'usager utilisé (numéro SIM). Ils servent également à localiser les appareils de téléphonie mobile.

L'"IMSI-catcher", en particulier, est un appareil visé par l'*al. 1*. Cet appareil 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. Ceci 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 l'identification du numéro d'identification international (numéro IMSI), jusqu'ici inconnu, d'une personne donnée.

Le service et les fournisseurs de services de télécommunication n'assument, respectivement, ni tâches ni obligations particulières dans la mise en œuvre du procédé de surveillance considéré. Ce procédé de surveillance doit à cet égard en particulier être distingué du type de surveillance qui vise à obtenir des fournisseurs

159 RS ... (FF **2007** 6583)
160 RS ... (FF **2007** 6583)
161 RS ... (FF **2007** 6583)
162 RS ... (FF **2007** 6583)

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 précis 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. Au vu des caractéristiques du procédé de surveillance visé par l'*art. 270*^{ter}, le recours à celui-ci ne doit donc pas être régi dans la nouvelle LSCPT mais dans le code de procédure pénale[163].

Les appareils utilisés par la police mentionnés à l'*al. 1* sont susceptibles de perturber les télécommunications. L'*al. 1* prévoit donc en outre, en substance, 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, se fonde sur l'art. 32*a* de la loi du 30 avril 1997 sur les télécommunications[164] et sur les art. 49 ss de l'ordonnance du 9 mars 2007 sur la gestion des fréquences et les concessions de radiocommunication[165]. Concrètement, pour obtenir cette autorisation, l'autorité qui souhaite utiliser un appareil visé par l'*al. 1* doit déposer une demande auprès de l'Office fédéral de la communication. 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'Office fédéral de la communication évaluera donc le danger de perturbation des télécommunications, en particulier des réseaux de téléphonie mobile, induit par l'utilisation de l'appareil considéré. Une fois l'autorisation de l'Office fédéral de la communication 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.

L'*al. 2* prévoit que, comme toute mesure de surveillance ordonnée, celle qui fait l'objet de l'al. 1 doit être soumise à l'autorisation du tribunal des mesures de contraintes. Les caractéristiques du procédé de surveillance considéré impliquent également que c'est expressément qu'une telle surveillance ordonnée doit être autorisée par le tribunal des mesures de contrainte, conformément à l'art. 274, al. 4, let. d du code de procédure pénale[166], qui est une disposition nouvelle, introduite par la nouvelle LSCPT.

Art. 271, al. 1 et 2

L'*art. 271* est précisé en ses al. 1 et 2.

L'*al. 1* s'inspire de l'actuel al. 1. Pour des raisons de clarté cependant, au vu du fonctionnement actuel du système géré par le service, la 1ère phr. de l'actuel al. 1 est complétée, de manière à ce qu'il soit explicitement dit que les autorités de poursuite pénale ne peuvent, dans le cas de figure visé par l'*al. 1* et afin de sauvegarder le secret professionnel, accéder directement aux informations recueillies dans le cadre de la surveillance effectuée, contrairement à ce qui est en principe le cas. Ce n'est donc qu'une fois que le tri visé par l'*al. 1* a été effectué que les autorités de poursuite pénale peuvent prendre connaissance des informations qui n'ont pas été écartées en

163 RS ... (FF **2007** 6583)
164 RS **784.10**
165 RS **784.102.1**
166 RS ... (FF **2007** 6583)

vertu de ce tri. Il va de soi que le fait qu'un tri doive avoir lieu implique que la surveillance ne peut être exécutée par branchement direct (voir commentaire de l'al. 2).

L'*al. 2* reprend en substance l'actuel al. 2. Il explique toutefois le cas de figure visé par celui-ci sous un autre angle, 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 ces cas de figure, d'une part, les autorités de poursuite pénale peuvent accéder directement, par le biais du système géré par le service, aux informations recueillies dans le cadre de la surveillance effectuée et que, d'autre part, la surveillance considérée peut être exécutée par branchement direct (Direktschaltung). Les caractéristiques du branchement direct – notion qu'il ne faut pas confondre avec celle de surveillance en temps réel (Echtzeit-Überwachung) – rendent en effet matériellement impossible le tri visé par l'al. 1 (voir commentaire de l'art. 16, let. d AP). Il sied de préciser que, à teneur 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 fait l'objet en tant que tiers, au sens de l'art. 270, let. b du code de procédure pénale[167].

Art. 273, al. 3

La période sur laquelle les données dites secondaires peuvent être demandées avec effet rétroactif, au sens de l'art. *273, al. 3*, passe de six mois 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 dites secondaires (art. 19, al. 2 et art. 23 AP). Pour le surplus, voir ch. 1.4.5.

Art. 274, al. 4, let. c et d (nouveaux)

L'art. *274, al. 4, let. c* renvoie au procédé de surveillance faisant l'objet de l'art. 270bis du code de procédure pénale[168], qui est une disposition nouvelle, introduite par la nouvelle LSCPT. Les caractéristiques du procédé de surveillance visé à l'art. précité (voir commentaire de l'art. 270bis du code de procédure pénale[169]) impliquent qu'une telle surveillance ordonnée doit être expressément autorisée par le tribunal des mesures de contrainte, ce que prévoit l'*art. 274, al. 4, let. c*.

L'art. *274, al. 4, let. d* renvoie au procédé de surveillance faisant l'objet de l'art. 270ter du code de procédure pénale[170], qui est une disposition nouvelle, introduite par la nouvelle LSCPT. Les caractéristiques du procédé de surveillance visé à l'art. précité (voir commentaire de l'art. 270ter du code de procédure pénale[171]) impliquent qu'une telle surveillance ordonnée doit être expressément autorisée par le tribunal des mesures de contrainte, ce que prévoit l'*art. 274, al. 4, let. d.*

167 RS ... (FF **2007** 6583)
168 RS ... (FF **2007** 6583)
169 RS ... (FF **2007** 6583)
170 RS ... (FF **2007** 6583)
171 RS ... (FF **2007** 6583)

Art. 278, al. 1bis

Le renvoi contenu à l'*art. 278, al. 1bis*, qui est une disposition introduite par la loi fédérale sur l'organisation des autorités pénales de la Confédération[172], doit être modifié et complété. Le renvoi à l'art. 3 de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[173] doit être remplacé par le renvoi à l'art. 27 de la nouvelle LSCPT (voir commentaire de l'art. 27 AP). Il y a également lieu d'opérer un renvoi à l'art. 28 de la nouvelle LSCPT, dès lors que cet article ne vise pas, à l'instar de l'art. 27 de la nouvelle LSCPT, une procédure pénale en cours (voir commentaire de l'art. 28 AP) et que des découvertes fortuites peuvent également avoir lieu dans une situation visée par cet article.

Procédure pénale militaire du 23 mars 1979[174]

Art. 70a, let. b, ch. 1 (texte en français)

Le commentaire relatif à l'art. 270, let. b, ch. 1 du code de procédure pénale[175] s'applique par analogie à l'*art. 70a, let. b, ch. 1*, qui est une disposition introduite par le code de procédure pénale[176].

Art. 70abis Interception et décryptage de données *(nouveau)*

Le commentaire relatif à l'art. 270bis du code de procédure pénale[177] s'applique par analogie à l'*art. 70abis*. L'art. 70*e*, al. 4, lit. c, qui est une disposition nouvelle, introduite par la nouvelle LSCPT, est l'équivalent dans la procédure pénale militaire[178] de l'art. 274, al. 4, let. c du code de procédure pénale[179].

Art. 70ater Utilisation de systèmes de localisation *(nouveau)*

Le commentaire relatif à l'art. 270ter du code de procédure pénale[180] s'applique par analogie à l'*art. 70ater*. L'art. 70*e*, al. 4, lit. d, qui est une disposition nouvelle, introduite par la nouvelle LSCPT, est l'équivalent dans la procédure pénale militaire[181] de l'art. 274, al. 4, let. d du code de procédure pénale[182].

Art. 70b

Le commentaire relatif à l'art. 271, al. 1 et 2 du code de procédure pénale[183] s'applique par analogie à l'*art. 70b, al. 1 et 2*, qui est une disposition introduite par le code de procédure pénale[184]. Le renvoi à l'art. 75, let. a et c contenu à l'*al. 3 de l'art.*

172 RS ... (FF **2008** 7371)
173 RS **780.1**
174 RS **322.1**
175 RS ... (FF **2007** 6583)
176 RS ... (FF **2007** 6583)
177 RS ... (FF **2007** 6583)
178 RS **322.1**
179 RS ... (FF **2007** 6583)
180 RS ... (FF **2007** 6583)
181 RS **322.1**
182 RS ... (FF **2007** 6583)
183 RS ... (FF **2007** 6583)
184 RS ... (FF **2007** 6583)

70b, qui est également une disposition introduite par le code de procédure pénale[185], 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 du code de procédure pénale[186], 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. 70d, al. 3

La période sur laquelle les données dites secondaires peuvent être demandées avec effet rétroactif, au sens de l'*art. 70d, al. 3*, qui est une disposition introduite par le code de procédure pénale[187], passe de six mois 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 dites secondaires (art. 19, al. 2 et art. 23 AP). Pour le surplus, voir ch. 1.4.5.

Art. 70e, al. 4, let. c et d (nouveaux)

L'*art. 70e, al. 4, let. c* renvoie au procédé de surveillance faisant l'objet de l'art. 70a^{bis} de la procédure pénale militaire du 23 mars 1979[188], qui est une disposition nouvelle, introduite par la nouvelle LSCPT. Les caractéristiques du procédé de surveillance visé à l'art. précité (voir commentaire de l'art. 70a^{bis} de la procédure pénale militaire du 23 mars 1979[189]) impliquent qu'une telle surveillance ordonnée doit être expressément autorisée par le tribunal des mesures de contrainte, ce que prévoit l'*art. 70e, al. 4, let. c*.

L'*art. 70e, al. 4, let. d* renvoie au procédé de surveillance faisant l'objet de l'art. 70a^{ter} de la procédure pénale militaire du 23 mars 1979[190], qui est une disposition nouvelle, introduite par la nouvelle LSCPT. Les caractéristiques du procédé de surveillance visé à l'art. précité (voir commentaire de l'art. 70a^{ter} de la procédure pénale militaire du 23 mars 1979[191]) impliquent qu'une telle surveillance ordonnée doit être expressément autorisée par le tribunal des mesures de contrainte, ce que prévoit l'*art. 70e, al. 4, let. d*.

Loi sur les télécommunications du 30 avril 1997[192]

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

L'*art. 6a* prévoit expressément une obligation de blocage par les fournisseurs de services de télécommunication de l'accès à la téléphonie mobile et à Internet, aux conditions mentionnées. Ceci évite de devoir fonder cette obligation sur une interprétation extensive de l'art. 20, al. 2 AP. Dite obligation a pour but de contribuer à identifier les personnes qui accèdent à la téléphonie mobile ou à Internet sans avoir

185 RS ... (FF **2007** 6583)
186 RS ... (FF **2007** 6583)
187 RS ... (FF **2007** 6583)
188 RS **322.1**
189 RS **322.1**
190 RS **322.1**
191 RS **322.1**
192 RS **784.10**

souscrit d'abonnement, respectivement au moyen, par exemple, de cartes SIM à prépaiement et de cartes "wireless" à prépaiement. Pour des raisons de praticabilité, l'obligation de blocage précitée se limite à la situation dans laquelle les clients des fournisseurs de services de télécommunication ont, lors de l'ouverture et de l'enregistrement de la relation commerciale (voir commentaire de l'art. 20, al. 2, AP), utilisé l'identité d'une personne qui n'existait pas ou qui n'a pas au préalable consenti à l'ouverture de cette relation, c'est-à-dire à une situation qui se présente dans le cas où le contrôle préalable à l'ouverture de dite relation n'a pas eu lieu conformément aux prescriptions (voir commentaire de l'art. 20, al. 2, AP). Exiger, suite à un contrôle d'identité qui a eu lieu conformément aux prescriptions, le blocage de l'accès à la téléphonie mobile et à Internet lorsque les clients considérés 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, par exemple, un téléphone portable muni d'une carte SIM à prépaiement peut 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 dans un contexte délictueux. 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 considérée 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.

Art. 37 Disposition transitoire

L'*art. 37* ne prévoit pas de réglementation transitoire particulière. La nouvelle LSCPT s'applique entièrement dès son entrée en vigueur, y compris aux surveillances en cours ordonnées avant son entrée en vigueur.

Art. 38 Référendum et entrée en vigueur

L'*al. 1* précise que la nouvelle LSCPT est soumise au référendum.

L'*al. 2* précise que le Conseil fédéral décide de la date d'entrée en vigueur de la nouvelle LSCPT.

3 Conséquences en matière de finances et de personnel

3.1 Conséquences pour la Confédération

Les nouvelles tâches attribuées au service engendreront des coûts supplémentaires pour la Confédération, y compris en matière de personnel. Cette augmentation doit bien entendu être mise en rapport avec l'amélioration que la nouvelle LSCPT permettra d'obtenir dans la poursuite des infractions. Il appartient au Conseil fédéral de décider si ces coûts supplémentaires doivent financièrement être compensés – en vertu du programme de consolidation (PCO) 2011-2013[193] mis en consultation par le Conseil fédéral le 14 avril 2010 (voir ch. 1.4.6) et, surtout, du moratoire en matière de dépenses adopté par le Conseil fédéral le 30 septembre 2009 – ou si cela

[193] http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf

n'est pas nécessaire. Si ces coûts doivent être compensés, il y aura lieu de décider des modalités pour ce faire. Sont notamment envisageables une compensation interne au DFJP en termes de personnel ou une augmentation du montant des émoluments (voir commentaire de l'art 30, al. 2 AP).

L'influence de l'avant-projet sur les finances de la Confédération, sous l'angle du personnel du service et des frais de fonctionnement de celui-ci, est estimée comme suit:

- Les art. 6 à 13 AP impliquent une augmentation de 6.0 postes, de CHF 2.5 millions par an au titre de frais d'exploitation (y compris les frais de personnel) et un investissement de CHF 1.6 millions. Ce qui précède est tout d'abord lié au fonctionnement en tant que tel du nouveau système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication exploité par le service. Ce système devra en effet permettre la conservation dans des conditions optimales d'une très grande quantité de données pendant une longue période. Cette influence estimée sur les finances de la Confédération est également liée aux tâches qu'assumera le service dans l'exploitation de ce nouveau système, notamment dans les domaines de l'administration de l'accès aux données contenues dans le système et du contrôle de la durée de conservation de celles-ci dans le système. Il sied de noter que les informations précitées tiennent compte des économies liées au passage de l'ancien au nouveau système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication.
- L'art. 17 AP implique une augmentation de 0.5 poste et de CHF 100'000.-- par an au titre de frais d'exploitation (y compris les frais de personnel).
- Les art. 18 et 24 AP impliquent une augmentation de 3.5 postes et de CHF 700'000.-- par an au titre de frais d'exploitation (y compris les frais de personnel).
- L'art. 21, al. 4 AP implique une augmentation de 2.5 postes et de CHF 900'000.-- par an au titre de frais d'exploitation (y compris les frais de personnel).
- L'art. 23 AP implique une augmentation de 0.25 poste, de CHF 750'000.-- par an au titre de frais d'exploitation (y compris les frais de personnel) et un investissement de CHF 100'000.--, étant entendu que le service enregistre les données considérées que les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la LSCPT doivent conserver non plus durant six mois mais durant douze mois.
- L'art. 25 AP implique une augmentation de 1 poste et de CHF 200'000.-- par an au titre de frais d'exploitation (y compris les frais de personnel).
- L'art. 28 AP implique une augmentation de 0.25 poste et de CHF 50'000.-- par an au titre de frais d'exploitation (y compris les frais de personnel).

En résumé, les conséquences précitées du présent avant-projet sont estimées comme suit:

- augmentation de 14 postes;
- CHF 1.7 millions de frais d'investissement;
- augmentation de CHF 5.2 millions par an au titre de frais d'exploitation, y compris de personnel.

Il y a lieu de ne pas perdre de vue que l'estimation précitée se fonde sur la situation tenant déjà compte des conséquences – bénéfiques pour les finances de la Confédération – qui découlent de la suppression de l'indemnisation des personnes qui exécutent des surveillances en vertu de la LSCPT. En effet, cette suppression est une mesure qui fait partie du programme de consolidation (PCO) 2011-2013[194] déjà mis en consultation par le Conseil fédéral le 14 avril 2010 (voir ch. 1.4.6).

Il sied de préciser, en guise de remarque, que l'acquisition du nouveau système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication exploité par le service n'est pas régi par le présent avant-projet. Les moyens supplémentaires pour l'introduction de ce nouveau système sont déjà prévus (décision du Conseil fédéral du 17 juin 2009).

3.2 Conséquences pour les cantons

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

Le passage au nouveau système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication est susceptible d'entraîner une baisse des coûts pour les cantons pour ce qui concerne l'équipement (voir ch. 1.4.2). Concernant les émoluments, voir le commentaire de l'art. 30 AP.

3.3 Conséquences pour l'économie

Le présent avant-projet engendrera des coûts supplémentaires pour les personnes soumises à la LSCPT, c'est-à-dire pour les personnes qui exécutent des surveillances en vertu de cette loi. Pour ce qui concerne les fournisseurs de services de télécommunication, en particulier, cette augmentation est toutefois à relativiser, au vu du fait que le coût des surveillances ne représente qu'une faible partie de leur chiffre d'affaire. L'augmentation considérée doit également être relativisée au vu du gain en efficacité dans la poursuite des infractions qui sera obtenu grâce à la nouvelle LSCPT.

4 Lien avec le programme de législature

Le présent avant-projet n'est pas prévu dans le message du 23 janvier 2008 sur le programme de la législature 2007 à 2011[195] ni dans l'arrêté fédéral du 18 septembre 2008 sur le programme de la législature 2007 à 2011[196]. Cela provient du fait que, au moment de l'élaboration du message relatif au programme de la législature précitée, il n'était pas assez avancé pour être repris dans ledit message.

194 http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf
195 FF **2008** 639
196 FF **2008** 7745

5 Aspects juridiques

La nouvelle LSCPT se fonde sur les art. 92, al. 1, et 123, al. 1, de la Constitution fédérale du 18 avril 1999 de la Confédération suisse[197], qui, respectivement, attribuent à la Confédération la compétence en matière de services postaux et de télécommunications et en matière de législation relative au droit pénal ainsi qu'à la procédure pénale.

Elle contient des délégations législatives au Conseil fédéral et aux cantons.

La nouvelle LSCPT ne pose pas de problèmes en relation avec le droit international.

[197] RS **101**