

Rapport explicatif

concernant la modification de l'ordonnance sur la surveillance par poste et télécommunication (OSCPT; RS 780.11) ainsi que la modification de l'ordonnance sur les émoluments et indemnités en matière de surveillance de la correspondance par poste et télécommunication (RS 780.115.1)

1. Contexte

Le Service Surveillance de la correspondance par poste et télécommunication (SCPT) du Centre de services informatiques CSI-DFJP est chargé d'assurer la surveillance de la correspondance par poste et télécommunication ainsi que de veiller aux développements techniques que connaît ce domaine et de procéder à l'adaptation appropriée des dispositions légales. Ce domaine des prestations de services de télécommunication se caractérise par une perpétuelle évolution. Il est incontesté que ce marché s'est accru lors de la dernière décennie et que les clients se voient offrir toujours plus de possibilités de communiquer de façon variée. Ainsi, les délinquants ont recours aux nouveaux moyens sophistiqués de prestations de services de télécommunication en sachant que leurs communications ne pourront pas ou que très difficilement être surveillés. La technologie analogique de communication (téléphone, télécopie, etc.) disparaît peu à peu au profit de la technologie Internet. Eu égard à cette situation, les autorités de poursuite pénale se plaignent à juste titre que les prescriptions de l'OSCPT ne sont plus à jour et qu'une poursuite pénale efficace, comme par exemple celle menée dans la lutte contre la pédophilie, l'extrémisme, le terrorisme, la criminalité économique (escroquerie, espionnage économique) ou encore la criminalité liée au trafic de stupéfiants est rendue de par ce fait très difficile.

En outre, la Suisse a signé la convention sur la cybercriminalité du Conseil de l'Europe du 23.11.2001. Cette convention entrera en vigueur pour la Suisse le 1^{er} janvier 2012. Dite convention exige notamment la réglementation concrète en droit national du fait de recueillir des données informatiques en temps réel.

Le but de cette révision partielle de l'OSCPT est de combler ces lacunes. Pour cette raison et compte tenu de l'urgence d'adapter les dispositions de l'OSCPT, il a été décidé de procéder à cette révision partielle sans attendre l'issue de la révision actuellement en cours de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT¹). L'art. 15 LSCPT permet de procéder déjà maintenant à cette adaptation de l'OSCPT. Ce d'autant plus que cette révision partielle de l'OSCPT n'anticipe pas sur la révision totale de l'ordonnance susvisée (adaptation à la future LSCPT) qui est nécessaire et aura lieu ultérieurement. Des adaptations de l'OSCPT ont également été nécessaires en raison de l'entrée en vigueur du Code de procédure pénale suisse (CPP²) au 1^{er} janvier 2011.

¹ RS 780.1

² RS 312.0

Keine Kopfzeile

De l'avis des autorités de poursuite pénale ordonnant les mesures de surveillance et les tribunaux de mesures de contrainte qui les autorisent, la liste des mesures de surveillance ne saurait être considérée comme exhaustive. Le service SCPT et les fournisseurs de services de télécommunication sont également obligés d'exécuter les mesures de surveillance ordonnées et autorisées ne figurant pas explicitement dans l'OSCPT. Cette situation conduit à une grande insécurité juridique et, tant pour le service SCPT que les fournisseurs de services de télécommunication, à des coûts considérables lors de l'exécution de mesures de surveillance ne figurant pas expressément dans l'OSCPT. L'exécution de ces mesures spéciales, par exemple dans le domaine de la surveillance Internet, peut occasionner de lourdes dépenses de l'ordre de plusieurs centaines de milliers de francs, par l'acquisition de technologies de surveillance et par le recours à des spécialistes externes, coûts qui ont jusqu'à présent été pris en charge par le service SCPT. Cette situation ne saurait être tolérée. Confronté à l'exécution de telles mesures de surveillance, le service SCPT se voit contraint de rendre des décisions relevant du droit administratif fédéral. Ces décisions font régulièrement l'objet de recours de la part des fournisseurs de services de télécommunication. Il en découle une charge supplémentaire pour le service SCPT ainsi qu'une insécurité juridique. Ces deux points pourraient être évités si l'OSCPT venait à être complétée par l'introduction explicite des nouvelles mesures de surveillance Internet et en même temps par l'adaptation des tarifs dans l'ordonnance sur les émoluments et indemnités en matière de surveillance de la correspondance par poste et télécommunication³ (ci-après, ordonnance sur les émoluments et indemnités). En outre, la levée de l'insécurité juridique actuelle renforcerait la sécurité des investissements des fournisseurs de services de télécommunication en matière de technologies liées à la surveillance. L'art. 15 LSCPT permet de procéder à une telle révision partielle de l'OSCPT dans la mesure où les fournisseurs de services de télécommunication doivent pouvoir être en mesure de livrer non seulement des données de l'application e-mail conformément à l'actuel art. 24 OSCPT, mais également celles d'accès Internet et d'autres applications Internet.

Il est également nécessaire de formuler de façon suffisamment précise dans l'OSCPT les autres mesures de surveillance qui ont été définies par la pratique et reconnues par la jurisprudence en matière de la LSCPT. Il en est de même des émoluments et indemnités découlant desdites mesures et devant être fixés dans l'ordonnance sur les émoluments et indemnités. Il s'agit particulièrement des recherches par champ d'antennes, de la recherche et du sauvetage de personnes disparues (recherches d'urgence) ainsi que de la surveillance en relation avec l'étranger de personnes suspectées. Ces mesures, créées par les besoins des autorités de poursuite pénale et confirmées par la jurisprudence, doivent être introduites dans le cadre de la révision partielle des deux ordonnances également pour des raisons liées à la sécurité du droit.

Enfin, il y a lieu de relever que les nouvelles mesures devant être intégrées dans l'OSCPT seront, en application de l'art. 33 al.1^{bis}, règlementées dans les directives administratives et techniques du service SCPT de manière conforme aux standards

Keine Kopfzeile

internationaux (ETSI⁴). En conséquence l'exécution de la surveillance de l'Internet sera standardisée tant pour le service SCPT que pour les fournisseurs de services de télécommunication ce qui entrainera une réduction des frais étant donné que les fournisseurs de services de télécommunication devront être en mesure d'exécuter ces standards. Les autorités de poursuite pénale se verront octroyer les moyens de surveiller plus efficacement les criminels ayant recours aux technologies nouvelles de télécommunication leur permettant de communiquer par-delà les frontières.

2. Commentaire des dispositions de l'ordonnance sur la surveillance par poste et télécommunication (OSCPT; RS 780.11)

Art. 1, al. 2, let. e

Cette modification ne concerne que le texte français. La notion de "fournisseurs d'accès à Internet" a été remplacée par celle de "fournisseurs Internet". En effet, la notion "de fournisseur d'accès à Internet" ne correspond plus à la réalité technique actuelle, étant donné qu'aujourd'hui les prestations de services Internet sont offertes par de nombreux fournisseurs qui eux-mêmes ne proposent pas les accès Internet. Si la notion étroite de "fournisseur d'accès à Internet" était maintenue, le champ d'application de l'OSCPT dans le domaine de l'Internet serait trop restreint. La téléphonie classique (réseau fixe) est en train de converger vers Internet par le biais de la téléphonie VoIP⁵. Dès lors les fournisseurs de services de téléphonie, en invoquant le fait qu'ils ne font qu'utiliser la technique Internet pour la transmission des communications téléphoniques, empêcher la surveillance de la téléphonie par protocole IP. En outre, la plupart des services de télécommunication actuels, tels que par exemple Skype et les Chats, figurant parmi les canaux de communication les plus utilisés et ce également par des criminels, ne pourraient pas faire l'objet d'une surveillance. Par l'adaptation du terme « fournisseur Internet » ces insécurité juridiques seront évitées.

Art. 2 Termes et abréviations

Les termes et abréviations ont été enlevés de la liste des définitions de l'art. 2 et intégrés dans une annexe, selon le modèle déjà connu de l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT⁶).

Art. 8, al. 1

⁴ "European Telecommunication Standards Institute". Organisme européen chargé de l'harmonisation des télécommunications.

⁵VoIP (Voice over IP) : est une technique qui permet de communiquer par la voix par le biais l'Internet. Le trafic VoIP peut être acheminé sur un réseau privé contrôlé ou le réseau Internet public ou une combinaison des deux.

⁶ RS 784.104 (cf. art. 1 et annexe ORAT)

Keine Kopfzeile

En utilisant la conjonction "et" à la place de "y compris", la notion de fournisseurs de services de télécommunication est précisée dans la mesure où elle englobe les fournisseurs Internet proposant des prestations de service n'étant pas limitées à l'accès Internet.

Art. 9, al. 2

L'art. 9 al. 2 se fonde sur la réglementation actuelle relative à la sécurité des données liées à la surveillance lors de leur transfert et règlemente sans équivoque la responsabilité quant à la sécurité des données jusqu'à leur transmission au service SCPT. Cet article concrétise la pratique actuelle. Cette responsabilité se déduit de l'art. 15, al. 1 LSCPT qui prévoit que les fournisseurs de services de télécommunications sont, à la demande du service SCPT, tenus de lui transmettre les communications de la personne surveillée.

Art. 11, let. d

L'art. 4, al. 3, LSCPT a été abrogé avec l'entrée en vigueur le 1^{er} janvier 2011 du Code de procédure pénale suisse (Code de procédure pénale, CPP) et remplacé par l'art. 271, al. 1 CPP. Il s'agit donc en l'espèce d'une adaptation d'ordre formel.

Titre précédant l'art. 15

Section 4 Surveillance des services téléphoniques

Le titre actuel de cette section n'est plus adapté à la situation et doit par conséquent être modifié. En effet, la mention selon laquelle cette section ne s'applique pas à Internet est superflue et source de confusions étant donné que les nouveaux articles 24, 24a, 24b et 24c de la section 6 sont exclusivement consacrés à la surveillance Internet. Il convient de préciser que les services de téléphonie suisses de provider VoIP, qui utilisent Internet comme technologie de transmission, sont concernés par cette section. Dès lors les fournisseurs de ce type de prestations de services ont les mêmes obligations que ceux proposant des services de téléphonie classiques.

Art. 15, al. 1, let. d et i, ch. 2

L'art. 4, al. 3 et al. 4 LSCPT ont été abrogés avec l'entrée en vigueur le 1^{er} janvier 2011 du CPP et remplacés respectivement par l'art. 271, al. 1 et 271, al. 2 et 3, CPP. En conséquence, il s'agit en l'espèce d'une adaptation d'ordre formel ayant pour but de couvrir le contenu matériel des alinéas 3 et 4 de l'art. 4 LSCPT.

Art. 16 Types de surveillance (temps réel et rétroactif)

Comme dans les autres dispositions qui seront énumérées ci-après, la let. b a été complétée par l'ajout de la notion "d'identification cellulaire (Cell ID)". Le but poursuivi est que chaque fournisseur de services de téléphonie mobile livre l'identificateur réel de la cellule selon les standards internationaux. Cela permettra aux autorités de poursuite pénale d'effectuer la surveillance au moyen d'appareils

Keine Kopfzeile

techniques de surveillance au sens de l'art. 280 CPP. Il en est de même en ce qui concerne la let. c, ch. 4 et la let. f, ch. 3 de cet article⁷.

L'art. 16 a été complété par une mesure de surveillance qui s'est développée dans la pratique. Cette mesure figure à la let. e qui définit l'exécution d'une recherche par champ d'antennes. Au moyen de la recherche par champ d'antennes il est possible de recueillir rétroactivement les données relatives au trafic de la totalité des communications par téléphonie mobile qui ont eu lieu durant un laps de temps déterminé dans une cellule déterminée de l'antenne. Les données ainsi recueillies peuvent être analysées entre autre en fonction du numéro appelant et appelé. Seule la communication ayant réellement eu lieu est saisie.

Art. 16a Recherche et sauvetage de personnes disparues

L'art. 16a définit les possibilités d'effectuer des mesures de surveillance dans le cadre de la recherche et le sauvetage de personnes disparues ou de personnes se trouvant dans une situation d'urgence (recherche d'urgence) en application de l'art 3 LSCPT. Le but de la recherche d'urgence est d'établir la position de l'équipement terminal d'une personne disparue. Il existe trois formes de recherches d'urgence: la détermination du dernier lieu de localisation de l'équipement terminal de la personne disparue (N1), la transmission en temps réel des données relatives au trafic (pour la téléphonie mobile y compris la position actuelle) de l'équipement terminal de la personne disparue (N2) et la recherche ainsi que la transmission des informations relatives au trafic historiques (pour la téléphonie mobile y compris les informations relatives à la position) de l'équipement terminal mobile de la personne disparue (N3).

Pour la téléphonie mobile le fournisseur de services de télécommunication livre les informations relatives à la ou aux antenne(s) de téléphonie mobile avec laquelle/lesquelles l'équipement terminal mobile de la personne disparue est respectivement a été connecté. Ces informations peuvent être les suivantes: l'identification cellulaire (Cell ID), la position, la direction d'émission ou la bande de fréquence de l'antenne. Au moyen de ces informations il est possible d'établir de manière approximative la position de l'équipement terminal de la personne disparue et ainsi délimiter la position de la personne disparue.

Les recherches d'urgence (N2 et N3) peuvent aussi être ordonnées pour des raccordements fixes.

Une situation susceptible de mener à une recherche d'urgence N2 sur des raccordements fixes pourrait être le fait que l'autorité ordonnant la surveillance souhaiterait connaître l'endroit où se trouve une personne suicidaire et fait surveiller les raccordements fixes connus de la personne disparue.

Un exemple de recherche d'urgence N3 sur un raccordement fixe pourrait être que l'autorité ordonnant la surveillance souhaiterait savoir avec qui une personne d'humeur suicidaire a communiqué durant les dernières 4 semaines afin d'obtenir de la part des personnes contactées des informations relatives à l'endroit où pourrait se trouver cette personne.

⁷ cf. également l'art. 24a, let. b, ch. 6 et l'art. 24b, let. a, ch. 6, pour ce qui est des explications en rapport avec l'identification cellulaire Cell ID.

Keine Kopfzeile

Art. 16b Mesures de surveillance en rapport avec l'étranger

Le Tribunal fédéral a clairement déterminé dans sa décision du 10 mars 2009 (A2335/2008) qu'en vertu de l'art. 15 al. 1 LSCPT et de l'art. 16 OSPCT (ancien), la surveillance de la correspondance par télécommunication n'est pas limitée à un raccordement national avec un numéro d'appel national.

Art 16b al. 1 a pour but de préciser que les surveillances, même si elles ont un rapport avec l'étranger, correspondent à des surveillances standard selon art. 16 let. a, let. c, ch. 1, 2, 3 et 5 et let. d, ch. 1, 2 et 4.

Une surveillance a un rapport avec l'étranger si la mesure de surveillance concerne les communications de et vers une ressource d'adressage à l'étranger, une ressource d'adressage suisse à l'étranger ou une ressource d'adressage étrangère en Suisse. La correspondance par télécommunication comprend les services téléphoniques y compris les sms. Des surveillances en temps réel et des surveillances rétroactives de la correspondance par télécommunication peuvent également être ordonnées dans ces cas de figure. Ceci vaut en outre indépendamment de l'appartenance de réseau de la ressource d'adressage.

Cela étant, afin de pouvoir exécuter une surveillance de la correspondance par télécommunication en rapport avec l'étranger il est nécessaire que dite correspondance par télécommunication soit effectuée par le biais d'un réseau suisse.

Art 16b al. 2 a pour but de préciser que les surveillances selon art. 16 let. b, let. c, ch. 4 et let. d, ch. 3 et 16a constituent des surveillances standard même quand elles sont ordonnées pour un Inbound Roamer. Un Inbound Roamer est un usager de téléphonie mobile étranger se trouvant dans le réseau d'un fournisseur de services de télécommunication suisse.

Art. 17, al. 2, 4, 5, 6 et 7

L'art. 271, al. 1, CPP poursuit le même but que l'art. 4, al. 5 et 6, LSCPT. Avec l'entrée en vigueur le 1^{er} janvier 2011 du CPP, les art. 3 à 10 LSCPT ont été abrogés. Il faut dès lors procéder à une adaptation de l'art. 17, al. 2 OSCPT. Le but est d'assurer le tri des informations issues de la surveillance du raccordement d'une personne soumise au secret professionnel ne faisant pas l'objet de l'enquête en cours. D'une part les mesures de protection nécessaires doivent être prises et, d'autre part, l'autorité ayant ordonné la surveillance doit en être dûment informée par le service SCPT.

L'art. 17 al. 4 a été reformulé afin de définir l'obligation des fournisseurs de services de télécommunication de transmettre la correspondance par télécommunication de la personne surveillée. L'al. 4 autorise le service SCPT de règlementer les spécifications de cette transmission dans ses directives. Il est précisé que les directives se fondent sur les standard ETSI afin d'assurer la sécurité d'investissement des fournisseurs de services de télécommunications et d'œuvrer en vue d'une unification de la surveillance de la correspondance par télécommunication selon les standards européens.

Art. 17, al. 5 a été introduit afin de règlementer séparément les compétences du service SCPT d'ordonner aux fournisseurs de services de télécommunication

Keine Kopfzeile

d'exécuter des mesures de surveillances n'étant pas explicitement prévues par la présente ordonnance mais ayant été ordonnées par les autorités de poursuite pénale et autorisées par les tribunaux de mesures de contrainte. Il est renvoyé aux explications ci-dessus relatives à l'art. 25, al. 5.

Les al. 6 et 7 de l'art. 17 correspondent de par leur contenu aux anciens al. 5 et 6 de l'art. 17.

Art. 18, al. 3, al. 7 et al. 8

A l'al. 3, l'adverbe "également" a été ajouté pour marquer expressément l'obligation faite aux fournisseurs de services de télécommunication d'être en tout temps en mesure de recevoir des ordres de surveillance et de les exécuter dans les délais les plus brefs. Cette obligation n'est pas restreinte au temps en-dehors des heures de bureau, ainsi que le prévoyait l'ancien al. 3, mais concerne également le temps durant les heures de bureau. Par ailleurs, il est précisé que les fournisseurs de services de télécommunication doivent indiquer au service SCPT, en la forme écrite, les noms des personnes de contact responsables. Des changements relatifs à ces contacts doivent être annoncés au service SCPT sans délai et par écrit.

On a en revanche tracé l'adverbe "temporairement" à l'al. 7 de l'art. 18, car le but de cet alinéa est de donner au service SCPT la possibilité d'utiliser gratuitement les services de télécommunication, respectivement les lignes des fournisseurs de services de télécommunication, afin que l'aptitude à effectuer les surveillances puisse être vérifiée en tout temps et que des problèmes survenant durant la surveillance de la télécommunication puissent être rapidement identifiés et résolus. . D'une part l'adverbe "temporairement" n'est pas défini, mais en le gardant on risque de mettre en péril l'exécution des mesures de surveillance. En d'autres termes, si le service SCPT juge nécessaire de contrôler la manière dont sont exécutés les différents types de surveillance, il doit être en mesure de le faire sans avoir à négocier au préalable la durée de tests.

L'al. 8 a été introduit afin de réglementer l'obligation des fournisseurs de services de télécommunication de soutenir le service quant à la vérification de la conformité des données transmises lors de la surveillance avec la correspondance par télécommunication de la personne surveillée.

Titre précédant l'art. 23

Section 6 Surveillance de l'Internet

Le titre de la section 6 a été adapté en raison de l'abrogation de l'art. 24 OSCPT et la nouvelle formulation de cet article complété par les nouveaux articles 24a, 24b et 24c.

Art. 23, let. d, f et g

L'art. 23, let. d, a subi une adaptation d'ordre formel, étant donné que l'art. 4, al. 3 LSCPT a été abrogé avec l'entrée en vigueur le 1^{er} janvier 2011 du CPP et a été remplacé par l'art. 271, al. 1 CPP.

Keine Kopfzeile

La modification de la let. f concerne uniquement la version française. Le terme « fournisseur d'accès à internet » a été remplacé par « fournisseur Internet ». Ce changement de terminologie intervient également à l'art. 1 al. 2 let. e et dans l'annexe à la présente ordonnance.

Sans être exhaustive, la liste de ressources d'adressage de la let. g, ch. 1 complète la liste actuelle. Le but consiste à obtenir des autorités de poursuite pénale qu'elles fournissent les ressources d'adressage correctes afin de pouvoir exécuter les mesures de surveillance Internet qu'elles ont ordonnées.

Art. 24 Types de surveillance

L'art. 24, en sa teneur actuelle, a été complètement remanié, car il ne correspond plus au niveau actuel de la technique. La disposition en vigueur laisse croire que la communication Internet n'aurait lieu que par e-mails. Or, il est incontesté que le domaine de la technologie et des prestations de services Internet se sont continuellement développés par le passé et que cette évolution va continuer dans le futur. Dans le cadre de ce processus, la communication par e-mail ne joue qu'un rôle négligeable. Dès lors, il est impératif de procéder aux adaptations nécessaires de cette partie de l'OSCPT afin d'assurer la sécurité du droit et de permettre aux autorités de poursuite pénale de disposer d'un moyen efficace dans la lutte contre la criminalité, tout particulièrement dans le domaine de la cybercriminalité. Outre le nouvel art. 24, trois nouvelles dispositions ont été créées, à savoir les art. 24a, 24b et 24c.

Le choix de la séparation en quatre articles repose d'une part sur la volonté d'adapter la surveillance de l'Internet aux normes internationales ETSI prévalant dans le domaine de la surveillance des télécommunications et d'autre part sur la volonté de transcrire dans l'ordonnance la jurisprudence du Tribunal fédéral administratif en matière de mesures de surveillances en rapport avec l'étranger. Conformément à ce but, l'art. 24 règle la question des accès internet et applications pouvant faire l'objet d'une surveillance. Les art. 24a et 24b décrivent les différents types de surveillance. L'art. 24a règle les surveillances en temps réel et art. 24b les surveillances rétroactives. Enfin, l'art. 24c règle les mesures de surveillance en rapport avec l'étranger.

L'art. 24 décrit de manière détaillée ce que l'on entend par canal ou voie de communication Internet, en dressant à titre exemplatif une liste de différentes technologies utilisées actuellement pour transmettre des données Internet.

L'al. 1 définit une liste énonçant les canaux de communication suivants:

- a. L'accès à Internet par une ligne téléphonique moyennant un modem analogique constitue la première méthode d'accès Internet qui avait été offerte au grand public avant « l'ère de l'ADSL ». Ce type d'accès existe encore aujourd'hui pour effectuer un accès à distance sécurisé.
- b. L'accès Internet à large bande est le type d'accès le plus répandu pour le grand public. Il s'agit généralement de l'ADSL, du VDSL ou de l'accès par câble.

Keine Kopfzeile

- c. L'accès Internet par le biais d'un réseau téléphonique mobile est normalement un accès Internet effectué par ondes radio au moyen d'un téléphone mobile ou d'un autre appareil mobile, comme par exemple un laptop/notepad (ce faisant la connexion Internet est continue indépendamment du fait que l'équipement terminal change de position).
- d. L'accès Internet par le biais d'un réseau sans fil est un accès au moyen d'ondes radio. Ce genre d'accès Internet s'effectue principalement par Wi-Fi mis à disposition du public dans la plupart des endroits communément accessibles.
- e. Ce type d'accès Internet consiste en une ligne de fibre optique atteignant directement l'utilisateur final (par ex. Ethernet par Fiber To The Home). Il s'agit d'une technologie de connexion de pointe, qui deviendra commune entre 2011 et 2020.
- f. L'accès Internet mentionné à la lettre f concerne la connexion à Internet à travers un tunnel de télécommunication privé (VPN) permettant de communiquer de façon sécurisée.

L'al. 2 de l'art. 24 décrit en premier lieu les services Internet (applications) susceptibles de faire l'objet d'une surveillance. Il s'agit selon la let. a d'une part principalement de services de messagerie asynchrones, dont l'utilisateur ne peut pas recevoir l'information en temps réel, tel que les e-mails et, d'autre part, de services de messagerie synchrones, tels que l'Instant Messaging ou les Chats, où l'information est échangée simultanément.

La lettre b prévoit la possibilité de surveiller les services multimédia, tels que la transmission de messages audio et vidéo (comme par exemple dans le cas de Skype).

Art. 24a Types de surveillance (temps réel)

L'art 24a décrit quels genres d'informations sont susceptibles d'être surveillés en temps réel. Les let. a et b règlementent les types de surveillance relatifs à l'accès Internet et les let. c et d les types de surveillance relatifs aux applications Internet.

- a. Dans le type de surveillance prévu par art. 24a let. a, la mesure de surveillance est effectuée directement sur l'accès Internet. Tout le trafic passant par cet accès Internet est surveillé en temps réel.
- b. La let. b concerne en revanche toutes les autres données qui ne sont pas reliées au contenu de la communication, mais à la mise en place et à l'administration de la connexion. Ainsi, les paramètres suivants sont énoncés:

Keine Kopfzeile

1. Les paramètres conventionnels retenus par les fournisseurs de services de télécommunication concernant le début et la fin d'une session Internet, répertoriés par date et heure.
 2. Le type de connexion à Internet utilisé, tels que par exemple ADSL, UMTS.
 3. Les paramètres conventionnels relatifs à la trace laissée par l'utilisateur pour accéder à la connexion Internet, tels que le nom d'utilisateur, le mot de passe et les heures des logins effectués.
 4. Toutes les ressources d'adressage doivent être livrées, en particulier celles en relation avec l'origine de la communication. Par exemple le numéro du téléphone mobile avec lequel la liaison Internet a été établie.
 5. Les paramètres de communication de l'équipement terminal sont les paramètres directement liés à l'équipement terminal comme par exemple l'adresse MAC et le numéro IMEI. Les paramètres pour l'identification de l'utilisateur sont les caractéristiques d'identification qui sont à disposition du fournisseur de services de télécommunication, mais qui ne sont pas en relation directe avec l'équipement terminal. Comme exemple le numéro IMSI.
 6. Ce chiffre renvoie à la surveillance du trafic Internet généré par un téléphone mobile par le biais d'un réseau téléphonique mobile. Ces informations permettent d'établir la position actuelle de l'équipement terminal. Cette dernière résulte de l'ensemble des paramètres définis au ch. 6.
 7. Ce chiffre énonce les informations pouvant être demandées lors d'une liaison de communication. Dans ce cas les autorités de poursuite pénale ont la possibilité d'obtenir un rapport technique concernant tous les changements que la personne surveillée ou le fournisseur de télécommunication a engendrés. Il s'agit par exemple de changements d'abonnements ou au réseau.
- c. La let. c de l'art. 24a règlemente la surveillance du contenu d'une application, par exemple le contenu d'e-mails.
- d. La let. d concerne toutes les données ne correspondant pas au contenu d'une application mais qui sont en rapport avec l'établissement et l'administration de la connexion. Il s'agit en l'espèce des paramètres suivants :

Keine Kopfzeile

1. Les paramètres communs retenus par les fournisseurs de services de télécommunication relatifs au début et à la fin de l'utilisation d'une session Internet, définis par la date et l'heure.
2. Toutes les ressources d'adressage doivent être livrées, en particulier celles en relation avec l'origine et la destination de la communication.
3. Le chiffre 3 se réfère aux éléments concernant l'accès à un service Internet, tels que les noms d'utilisateurs et les mots de passe
4. Le chiffre 4 se réfère aux informations d'enveloppe selon le protocole SMTP. Il s'agit en l'espèce du protocole standard utilisé pour l'envoi d'e-mails.
5. Le chiffre 5 permet de demander d'autres paramètres de communication générés auprès du fournisseur Internet par l'utilisation d'un service Internet et qui sont conservés, tels que le numéro du port de l'origine et de la destination de la communication.
6. Ce chiffre traite des informations pouvant être demandées durant une communication par le biais d'un service Internet. Les autorités de poursuite pénale ont la possibilité de demander un rapport technique concernant tous les changements effectués par la personne surveillée ou le fournisseur de services de télécommunication. Il s'agit typiquement du changement de type d'abonnement ou de login.

Art. 24b Types de surveillance (rétroactif)

L'article 24b se réfère à la surveillance que l'on appelle rétroactive. Il traite donc des données qui ont été enregistrées et sauvegardées par le fournisseur Internet.

La let. a se réfère à la livraison de données relatives au trafic concernant au moins un des paramètres suivants :

1. Le chiffre 1 traite de la livraison des éléments suivants : la date et l'heure du début et de la fin de la connexion. Le terme « connexion » définit une session Internet et non pas chaque action effectuée dans le cadre d'une telle session.
2. Au chiffre 2, il est question du type de connexion ou de raccordement. Par exemple une connexion ADSL ou un raccordement analogique.
3. Le chiffre 3 concerne les données connues relatives à l'accès (noms d'utilisateurs et mots de passe).

Keine Kopfzeile

4. Le chiffre 4 a trait aux ressources d'adressage connues de l'accès Internet surveillé, en particulier de l'origine de la communication (p.ex. adresse IP, numéro de téléphone du raccordement ADSL).
5. Le chiffre 5 concerne les informations connues lors de l'utilisation d'un appareil pour l'accès à Internet. La liste du chiffre 5 n'est pas exhaustive et concerne l'accès par le biais d'un ordinateur ou d'un téléphone mobile (smartphone).
6. Parmi les informations mentionnées dans le chiffre 6, il y a celles relatives à l'identification cellulaire (Cell ID)⁸ lors d'une surveillance d'un téléphone portable ayant servi comme moyen d'accès à Internet.

La let. b se réfère en particulier à l'obtention des informations rétroactives lors d'une surveillance d'un service de messagerie asynchrone. Il s'agit typiquement de données relatives à la surveillance d'e-mails. Dans ces cas, les données énoncées aux chiffres suivants doivent pouvoir être livrés aux autorités de poursuite pénale:

1. Parmi les données énoncées au chiffre 1 figurent les données de base générées lors de l'envoi et de la réception de messages par le biais de services de messageries électroniques asynchrones : la date et l'heure de l'envoi et de la réception.
2. Le chiffre 2 mentionne les paramètres détenus par le fournisseur Internet enregistrés et conservés par lui lors de l'utilisation du protocole SMTP, nécessaire entre autre pour l'envoi d'e-mails.
3. Le chiffre 3 exige que les adresses IP utilisées lors de l'envoi et / ou de la réception des messages transmis par le biais des services de messagerie électroniques asynchrones (par exemple les e-mails), puissent être requises par les autorités de poursuite pénale.
4. Le chiffre 4 dispose que toutes autres ressources d'adressage disponibles enregistrées par le fournisseur Internet lors de l'envoi ou de la réception de messages par la personne surveillée doivent être livrées.

Art. 24c Mesures de surveillance en rapport avec l'étranger

Le Tribunal fédéral a clairement déterminé dans sa décision du 10 mars 2009 (A2335/2008) qu'en vertu de l'art. 15 al. 1 LSCPT et de l'art. 16 OSPCT (ancien), la surveillance de la correspondance par télécommunication n'est pas limitée à un raccordement national avec un numéro d'appel national. La procédure de recours à la base de cet arrêt traitait de la surveillance d'un raccordement téléphonique se

⁸ Cf. à ce propos les explications ci-dessus ad art. 16 OSCPT

Keine Kopfzeile

trouvant à l'étranger. Partant, la décision du Tribunal fédéral administratif concerne les services de téléphonie.

Cela étant, les conclusions du Tribunal fédéral administratif sont également applicables à la surveillance de l'Internet. Car le Tribunal fédéral administratif a conclu que la surveillance de la correspondance par télécommunication entre une ressource d'adressage étrangère et une ressource d'adressage quelconque se trouvant dans un réseau d'un fournisseur de services de télécommunication suisse n'était pas contraire à l'esprit de la LSCPT. Par un tel branchement la correspondance par télécommunication d'une personne précise est surveillée, tel que le prévoit l'art. 15 al. 1 LSCPT, et, ce faisant, l'objet de la surveillance est une ressource d'adressage précise exactement comme lors de la surveillance d'une ressource d'adressage nationale. Il n'est pas possible de déduire de l'art. 15 al. 1 LSCPT qu'une surveillance doit être limitée à une ressource d'adressage nationale avec un accès national.

L'art. 24c précise que les surveillances, même si elles ont un rapport avec l'étranger, demeurent des surveillances standard selon art. 24 al. 1 let. c et d, art. 24a let a et b et art. 24b let a.

Il y a rapport avec l'étranger quand une mesure de surveillance concerne le trafic par Internet de ou vers une ressource d'adressage étrangère à l'intérieur du pays, appelée Inbound Roamer. La correspondance par télécommunication comprend le trafic par internet par le biais d'un réseau téléphonique mobile suisse ou un accès sans câble en Suisse. La ressource d'adressage à surveiller peut être par exemple un numéro MSISDN ou un numéro IMSI. Des surveillances en temps réel et rétroactives de la correspondance par télécommunication peuvent être ordonnées dans ce cas de figure et ce indépendamment de l'appartenance de réseau de la ressource d'adressage. En ce qui concerne les applications il peut être fait abstraction de l'endroit de connexion de l'utilisateur.

Art. 25 Mise en œuvre de la surveillance

Cet article est désormais composé de 7 alinéas. Il a été élargi de deux alinéas, à savoir les actuels alinéas 4 et 5.

L'al. 1, let. a est maintenu dans sa forme actuelle. Seul l'al. 1 let. b est complété par l'expression "si nécessaire", afin que la compétence de décision de contacter ou non les fournisseurs Internet dans les situations mentionnées à l'al. 1, let. b demeure auprès du service SCPT. Contrairement à la version française, le terme « fournisseur Internet » n'a pas du être adapté dans la version allemande et italienne.

L'al. 2 tient compte de l'entrée en vigueur du CPP en date du 1^{er} janvier 2011 et de l'abrogation des art. 3 à 10 LSCPT. Dès lors, il renvoie à l'art. 271, al. 1, CPP qui poursuit le même but que les art. 4, al. 5 et 6, ancienne LSCPT. En outre, cet alinéa doit être adapté au fait qu'en plus du courrier électronique, il y a lieu de surveiller également l'accès Internet ainsi que les applications Internet (renvoi aux art. 24, 24a et 24b).

L'al. 3 demeure inchangé.

Keine Kopfzeile

L'art. 25 al. 4 a été inséré afin de préciser que les fournisseurs Internet ont l'obligation de transmettre la correspondance par télécommunication des personnes sous surveillance. En outre l'al. 4 autorise le service SCPT à régler les spécifications de ces transmissions dans ses directives. Il est précisé que les directives se basent sur les standards ETSI afin d'assurer la sécurité des investissements des fournisseurs de services de télécommunication et en vue d'agir vers une unification de la surveillance de la correspondance par télécommunication selon les standards européens.

Art. 25 al. 5 a été inséré suite à la longue pratique du service SCPT entérinée par les tribunaux afin de régler séparément la compétence du service d'ordonner à l'encontre des fournisseurs Internet l'exécution des mesures de surveillance ne figurant pas explicitement dans la présente ordonnance mais qui ont été ordonnées par les autorités de poursuite pénale et autorisées par les tribunaux de mesures de contrainte.

Le contenu des anciens al. 4 et 5 est réglé par les nouveaux alinéas 5 et 6.

Art. 26 Obligations des fournisseurs Internet

Cet article a été remanié et harmonisé avec l'actuel 18 OSCPT. Il comprend désormais 7 alinéas au lieu de 5.

Dans la version française la notion de fournisseurs d' "accès" Internet est remplacée par celle de « fournisseurs Internet » dans le titre ainsi que les al. 1, 3, 5 et 6. Il en est de même à l'al. 2 où la notion d' "accès" a été tracée. Ces modifications résultent de la nouvelle terminologie de l'art. 1, al. 2, let. e. Contrairement au texte français la notion de « fournisseur Internet » n'a pas du être adaptée dans la version allemande et italienne.

L'al. 1 est modifié par la suppression du renvoi à l'ancien art. 24 OSCPT. Ce dernier a été remplacé par un renvoi à la section 6. S'agissant de l'al. 2, il ne subit qu'une modification linguistique dans sa version française pour les raisons exposées dans le paragraphe précédent. Il en est de même de l'al. 3 en sa version française et il a été harmonisé avec l'art. 18, al. 3 OSCPT dont le contenu a été repris. Par ailleurs, il est précisé que les fournisseurs Internet doivent indiquer au service SCPT, en la forme écrite, les noms des personnes de contact responsables. Des changements y relatifs doivent également être signalés au service SCPT sans délai. Dans l'al. 4 le renvoi à l'ancien art. 24 a été supprimé et remplacé par un renvoi aux art. 24-24c. En outre dit alinéa a du être adapté au fait que désormais non seulement les e-mails pourront faire l'objet d'une surveillance, mais également les accès et les applications Internet (renvoi aux art 24, 24a, 24b et 24c).

L'ancien contenu de l'al. 5 a été supprimé. La raison en est que le contenu de cet alinéa traite d'un sujet de nature organisationnelle et administrative n'ayant désormais plus sa place dans l'OSCPT étant donné qu'il est réglé dans les directives organisationnelles et administratives⁹ émises par le service SCPT. Dans sa nouvelle teneur, l'al. 5 régleme l'obligation des fournisseurs Internet de

⁹ Il s'agit des directives OAR (Organisational and Administrative Requirements) du service SCPT qui sont à disposition des fournisseurs de services de télécommunication.

Keine Kopfzeile

travailler de concert quand la correspondance par télécommunication faisant l'objet d'une surveillance passe par le biais de réseaux de plusieurs fournisseurs Internet.

Le contenu de l'al. 6 de l'art. 26 correspond à celui de l'art. 18 al. 8.

Le nouvel al. 7 régit l'obligation des fournisseurs Internet de soutenir le service SCPT quand il est question de vérifier en chaque cas que les données recueillies lors de la surveillance correspondent à la correspondance par télécommunication de la personne surveillée.

Art. 27, al. 1, et al. 2

Dans l'art. 27 al. 1 le terme « fournisseur d'accès à internet » a été remplacé par « fournisseur Internet ».

L'al. 1, let. a de l'art. 27 de la version française a été adapté de sorte que cet article, en tant que disposition d'exécution de l'art. 14, al. 4 LSCPT (Identification de l'auteur d'un acte punissable commis au moyen d'Internet), ne concerne plus seulement les adresses IP attribuées de manière définitive (soit les adresses IP dites statiques), mais également l'identification d'utilisateurs d'adresses IP dynamiques. Cette disposition a été complétée par les données utilisées pour la procédure d'identification (login) et les autres adresses IP attribuées par les fournisseurs Internet aux usagers.

La modification de l'al. 1, let. b ne concerne que le texte français. Dans la version française de l'OSCPT le terme « fournisseur d'accès à Internet » a été remplacé par « fournisseur Internet » (cf. à ce propos les explications relatives à l'art. 1 al. 2 let. e).

L'al. 1, let. c de l'art. 27 a été adapté de façon à ce que l'obligation faite au fournisseur d'identifier ses clients ne soit plus limitée aux seuls services d'e-mail, mais soit étendue à tous les services de messagerie électronique dans la mesure où ils ont été aménagés par les fournisseurs Internet en vue d'une exploitation par une clientèle. L'adaptation linguistique relative au terme « fournisseur d'accès à Internet » ne concerne que la version française.

L'al. 2 ne concerne que le texte français. Contrairement à la version française de l'OSCPT le terme « fournisseur Internet » n'a pas du être adapté dans la version allemande et italienne.

Annexe Termes et abréviations

Basée sur l'art. 2, cette annexe dresse une liste de descriptifs et abréviations utilisés généralement dans le domaine de la surveillance de la télécommunication.

3. Explications sur les raisons de la modification de l'ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication (RS 780.115.1)

3.1 Introduction

La présente révision partielle de l'ordonnance a pour but d'une part de déterminer les émoluments et les indemnités des mesures de surveillance tels qu'ils sont déjà définis et reconnus dans la pratique. Cela vaut pour trois mesures, à savoir la livraison de données relatives à des mesures de surveillance en rapport avec l'étranger (projet OSCPT art. 16b), la recherche par champ d'antennes (projet OSCPT art. 16 let. e) ainsi que la recherche et le sauvetage de personnes disparues (recherche d'urgence) (projet OSCPT art. 16a). D'autre part, elle a pour but de définir les émoluments et les indemnités relatifs à la surveillance de l'Internet. L'art. 4 de l'ordonnance ne répond plus aux exigences actuelles quant à la réglementation des émoluments. De par ce fait, deux nouveaux articles ont été créés afin de pallier à cette insuffisance. En outre de petits changements ont été effectués au texte de l'ordonnance afin d'écartier certaines imprécisions.

3.2 Commentaire des dispositions

Titre

Le titre de l'ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication est modifié comme suit : ordonnance sur les émoluments et indemnités en matière de surveillance de la correspondance par poste et télécommunication (OEI-SCPT).

Art. 1, al. 2^{bis}

En ce qui concerne le nouvel al. 2^{bis}, il prévoit que la surveillance d'une ressource d'adressage, de format suisse ou étranger, n'implique qu'une seule indemnisation ainsi qu'une seule facturation.

Art. 2 Emoluments et indemnités

A. Services à commutation de circuits

En premier lieu, il convient de relever que la nomenclature des différents types de surveillance basés sur les art. 16, 16a et 16b OSCPT (raccordements de télécommunication de circuits [Circuit Switched, CS]), ou sur les articles 24, 24a et 24b (raccordements Internet à commutation de paquets [Packet Switched, PS]) demeure inchangée. Les émoluments et indemnités relatifs aux mesures de surveillance figurant déjà dans l'ordonnance actuelle n'ont pas été modifiés. Dans le domaine CS, seuls ont été introduits les nouveaux articles 16, let. e, 16a et 16b. L'introduction de ces dispositions n'a pas entraîné d'adaptations des émoluments et indemnités relatifs aux autres mesures de surveillance inscrites au tableau. Seule la pratique d'indemnisation menée depuis des années par le service SCPT a été intégrée. Cela concerne donc les rubriques CS 5 et CS 6 ainsi que la recherche et sauvetage de personnes disparues (recherche d'urgence : N1-3).

Keine Kopfzeile

B. Services à commutation de paquets

1. Remarques introductives

Selon le droit en vigueur, les rubriques PS 1-5 et 8 ne traitent que de la surveillance d'e-mails. Comme décrit au début du présent rapport explicatif, sous le chiffre 1 ("Contexte"), la révision partielle de l'OSCPT a entre autres pour but de réglementer la surveillance Internet au sens large. Par conséquent, une grande partie des rubriques figurant sous la lettre B ont dû être supprimées ou adaptées aux modifications apportées dans la section 6 de l'OSCPT.

2. Rubriques PS 1-4

Suite à la nouvelle structure de la section 6, et tout particulièrement des articles 24, 24a, 24b et 24c il est prévu de séparer la surveillance de l'accès à Internet de la surveillance de chaque application Internet. Par ailleurs, une distinction est clairement faite entre la surveillance en temps réel de l'accès à Internet et des applications Internet d'une part (art. 24a) et de la surveillance rétroactive de l'accès à Internet et des messageries électronique asynchrones d'autre part (art. 24b).

Concrètement, les mesures de surveillance de l'art. 24a sont représentées sous les rubriques PS 1-4 et les mesures de surveillance de l'art. 24b sont reproduites sous les rubriques PS 5-6.

Pour ces mêmes raisons, la troisième colonne consacrée à ce jour aux ressources d'adressage à surveiller doit être remplacée par les informations relatives à l'accès et aux applications Internet respectivement des services de messagerie électronique asynchrones qui doivent pouvoir faire l'objet d'une surveillance. Toujours dans cette même colonne, une différence est faite dans les rubriques PS 1-4 en fonction de l'ampleur des informations que les fournisseurs Internet doivent livrer; à savoir:

- soit **le contenu des communications et les données relatives au trafic** (PS 1) ou **seulement les données relatives au trafic** d'un accès Internet (PS 2),
- soit **le contenu des communications et les données relatives au trafic** (PS 3) ou **seulement les données relatives au trafic** d'une application Internet (PS 4).

La rubrique PS 1 comprend nouvellement la surveillance en temps réel de l'accès à Internet et la livraison des données relatives au trafic.

Le total des émoluments pour une telle prestation de services est fixé à 6'160 francs.

Ce montant est constitué de la part revenant au service SCPT et qui est de 1'080 francs (cf. CS 1-3) et de la part des indemnités revenant aux fournisseurs Internet fixée à 1'330 francs. Cette indemnisation se base également sur celle relative à l'exécution d'une mesure de surveillance selon CS 1-3 de l'actuelle ordonnance sur les émoluments et indemnités. La différence entre ce montant de base (2'410 francs) et le montant global de 6'160 francs s'explique par la nécessité de conserver les données dans le centre de traitement du service SCPT et les frais y relatifs.

Ainsi, on compte 50 francs par année et par gigabyte (GByte) de données (sur un système de stockage à haute disponibilité et redondant) et on estime qu'une mesure de surveillance induit 20 GByte supplémentaires chaque mois et ce sur une durée

Keine Kopfzeile

moyenne de 9 mois. On arrive ainsi à un montant de 3'750 francs par mesure de surveillance en procédant au calcul suivant:

$$20 \text{ GByte} \times \frac{9(9+1)}{2} \text{ mois} \times \frac{50 \text{ frs.}}{12 \text{ mois} \times \text{GByte}} = 3'750 \text{ frs.}$$

La rubrique PS 2 correspond au paiement de l'indemnité relative à une demi-journée de travail (quatre heures de travail) d'un employé d'un fournisseur Internet et à une heure de travail d'un employé du service SCPT. Une heure de travail est facturée à 160 francs, tant pour un employé d'un fournisseur Internet que pour un employé du service SCPT. La même base de calcul s'applique pour le prélèvement de l'émolument et de l'indemnité de la rubrique PS 4.

La rubrique PS 3 traite de la surveillance en temps réel d'une application Internet et de la livraison des données relatives au trafic. Cela correspond à la charge de travail mentionnée aux rubriques actuelles PS 1-5 qui comprennent la surveillance en temps réel d'un e-mail (contenu et données relatives au trafic).

3. Rubriques PS 5 et 6

La rubrique PS 5 correspond aux actuelles rubriques PS 6 et 7. Les données relatives au trafic demandées correspondent à celles de l'art. 24, let. f et de l'art. 16, let. d (CS 4), en ce qui concerne l'accès Internet par le biais d'un réseau mobile.

La rubrique PS 6 correspond à l'actuelle rubrique PS 8. Les renseignements demandés correspondent à ceux figurant à l'actuel art. 24, let. h OSCPT avec l'ajout que ces données doivent pouvoir être livrées pour toutes les messageries électroniques asynchrones.

Au vu de ces explications, les émoluments et indemnités demeurent conformes à la pratique actuelle et aux montants figurant dans l'actuelle ordonnance sur les émoluments et indemnités.

4. Rubriques A0.1 et A0.2

La rubrique A0.1 correspond à l'actuelle rubrique A.0 avec le maintien des émoluments et indemnités. Le seul changement apporté concerne le fait que jusqu'à présent l'identification d'un utilisateur d'une adresse dynamique selon l'art. 14, al. 4 LSCPT a été exécutée sous la rubrique PS 6 (cf. à ce propos les explications relative à l'art. 27, al. 1, let. a). C'est pourquoi la rubrique d'information A0.2 a été créée, avec le maintien des mêmes émoluments et indemnités.

Art. 3, phrase introductive Forfaits supplémentaires pour des prestations fournies en dehors des heures normales de travail

Il s'agit ici d'une simple adaptation relative à l'actuelle dénomination du service SCPT.

Dans le cas de l'application du forfait pour prestations fournies en dehors des heures normales de travail, le terme « mesure de surveillance » est remplacé par le terme

Keine Kopfzeile

« ordre ». Pour chaque ordre, le montant forfaitaire pour prestations fournies en dehors des heures normales de travail n'est facturé qu'une seule fois par fournisseur de services de télécommunication, étant précisé qu'un ordre peut contenir plusieurs mandats (surveillances ou demandes de renseignements).

Donc, par exemple, si le service reçoit à 23:30h d'une autorité de poursuite pénale un ordre contenant 10 mandats (surveillances et demandes de renseignements) et à 01:15, toujours de la même autorité de poursuite pénale, un ordre ne contenant qu'un seul mandat de surveillance, le montant forfaitaire de CHF 250.00 sera facturé deux fois à dite autorité de poursuite pénale.

Art. 3a Autres prestations de services

Cet article consacre une pratique longue et incontestée du service SCPT selon laquelle un montant forfaitaire de 125 francs est facturé à l'autorité de poursuite pénale désireuse d'obtenir une copie supplémentaire d'un DVD ou d'un disque dur.

Art. 4 Emoluments pour des prestations ne figurant pas dans l'OSCP

L'al. 1 permet au service SCPT de percevoir des émoluments pour des prestations de service ne figurant pas sur la liste de la présente ordonnance. L'al. 1 correspond à la deuxième phrase de l'art. 4 al. 2 actuellement en vigueur qui fixe le taux horaire. Le montant de 160 francs équivaut à une moyenne du tarif horaire du personnel du service SCPT et prend en considération la formation et les connaissances requises dudit personnel. Il correspond en outre à la pratique de facturation courante du service SCPT qui a également été confirmée par le Tribunal fédéral (cf. Tribunal fédéral, arrêt du 20 mars 2007, 1A.255/2006). Il est aussi tenu compte des tarifs prévus par certaines ordonnances de la Confédération sur les émoluments¹⁰. Il est en outre pris en considération que le nombre annuel des surveillances auxquelles le service SCPT doit donner suite est supérieur à 10'000. Comme chaque mesure de surveillance nécessite l'engagement d'un ou plusieurs employés du service SCPT (juristes, ingénieurs, personnel administratif), il n'est pas possible de calculer séparément les tarifs horaires de tous les différents employés du service SCPT intervenant dans le cadre de l'exécution d'un ordre de surveillance. Un calcul séparé des différents tarifs horaires lors de l'établissement des émoluments entraînerait une surcharge administrative considérable pour le service SCPT. L'al. 3 définit la base de calcul pour la répartition des dépenses liées à l'acquisition d'appareils et des charges découlant du travail technique nécessaire. La facture d'émoluments, selon la pratique actuelle du service SCPT, comprend tant l'indemnisation du fournisseur de services de télécommunication que l'indemnisation du service SCPT pour chaque ordre de surveillance. Le taux horaire de 160 francs vaut pour les employés des fournisseurs de services de télécommunications ainsi que pour ceux du service SCPT.

¹⁰ En particulier l'ordonnance sur les émoluments du Contrôle des finances (RS 172.041.17) et l'ordonnance sur les émoluments pour les prestations de l'Office fédéral de la justice (RS 172.041.14)

Keine Kopfzeile

Art. 4a Emoluments pour des prestations non prévues par l'OSCPT

L'al. 1 est le pendant de l'al. 1 de l'art. 4 quant aux indemnités ne figurant pas dans la liste de la présente ordonnance octroyées aux fournisseurs de services de télécommunication. En outre il précise que l'indemnité est partie intégrante de l'émolument perçu auprès des autorités de poursuite pénale, soit que l'émolument est composé d'une indemnisation destinée au service SCPT ainsi qu'une indemnisation destinée aux fournisseurs de services de télécommunication. Pour les prestations de services prévues par la présente ordonnance on obtient le montant de l'indemnité destinée au service SCPT par la soustraction du montant de l'indemnité destinée aux fournisseurs de service.

L'al. 2 de l'art. 4a fixe le taux horaire à 160 francs (cf. explications relatives à l'art. 4).

L'al. 3 définit les démarches susceptibles d'être facturées par les fournisseurs de services postaux et de télécommunication afin de permettre une indemnisation correcte de leurs dépenses conformément à l'art. 4a.

L'al. 4 fixe à 80% le pourcentage de la couverture des indemnités par rapport à l'ensemble des dépenses¹¹.

Art. 5a Emoluments pour des mesures non autorisées

L'art. 5a établit le principe selon lequel des émoluments et des indemnités seront également facturés si une mesure de surveillance ordonnée et exécutée n'a pas été autorisée par la suite ou n'a pas permis d'obtenir le succès d'enquête escompté.

Art. 5b Application de l'ordonnance générale sur les émoluments

Il s'agit ici d'une référence globale à l'ordonnance générale sur les émoluments¹².

4. Conséquences financières et personnelles

Selon toute vraisemblance, ces deux projets de révision d'ordonnances n'auront pas, dans une première phase, de conséquences financières ou personnelles pour la Confédération.

En vertu des articles 15 et 16 LSCPT en relation avec les articles 18 et 26 OSCPT, les fournisseurs de services de télécommunication doivent assumer les frais d'investissement nécessaires pour garantir l'exécution des mesures de surveillance. Après l'entrée en vigueur de la révision partielle de l'OSCPT, lesdits fournisseurs devront également prendre à leur charge les frais d'investissement liés à la capacité d'effectuer la surveillance des nouvelles technologies de télécommunication qu'ils ont mis et mettront sur le marché (surveillance Internet).

¹¹ Il s'agit en l'occurrence d'un pourcentage correspondant à la pratique instaurée par le DETEC et ayant prévalu à ce jour.

¹² RS 172.041.1

Keine Kopfzeile

L'effet à moyen terme sera que le service SCPT devra exécuter moins de "mesures spéciales" à savoir qu'il pourra également passer par des processus standardisés pour la surveillance de l'Internet. Cela aura entraîné à moyen terme une réduction des dépenses du service SCPT relatives à l'acquisition de matériel dans le domaine de la surveillance de l'Internet.

Dans le domaine du personnel il n'y a pas de possibilités d'effectuer des économies. Cela étant, les présents projets de révision partielle n'entraîneront aucune augmentation du besoin en personnel du service SCPT.

Quant aux autorités de poursuite pénale de la Confédération et des cantons, elles se voient offrir des nouvelles possibilités d'investigation dans un domaine de télécommunication en pleine expansion et qui nécessite un grand engagement dans le domaine de la lutte contre la cybercriminalité. Cette lutte incontournable contre ces nouvelles formes de criminalité va occasionner des frais, mais ces derniers devraient demeurer dans une proportion raisonnable au regard de l'efficacité des possibilités d'investigation que les nouvelles mesures de surveillance vont apporter.