Rapport explicatif

relatif à la révision totale de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT; RS 780.11)

A. Contexte

La révision totale de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[1] (LSCPT) implique une révision totale de ses ordonnances d'application, et donc, entre autres, de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT).

La nouvelle ordonnance reprend la structuration traditionnelle: dispositions générales (chapitre 1), correspondance postale (chapitre 2), télécommunications (chapitre 3) et dispositions finales (chapitre 4). Pour répondre à la demande d'une plus grande sécurité du droit, l'ordonnance décrit de manière très détaillée les droits et les devoirs des uns et des autres. Elle ne se contente plus, par exemple de distinguer les types de surveillance en temps réel et rétroactive, mais elle contient pour chaque service proposé des dispositions propres qui décrivent – lorsqu'il y a lieu – la manière dont le service en question est surveillé en temps réel et de manière rétroactive. Il s'ensuit que les différentes conditions d'un type de renseignement ou de surveillance sont aussi fixées en détail.

La forte densité normative vise à renforcer la sécurité du droit, mais aussi à standardiser le plus possible les types de demandes de renseignements et de surveillances, afin de favoriser l'automatisation des procédures.

Une autre différence par rapport à l'OSCPT dans sa teneur du 31 octobre 2001 est que l'OSCPT entièrement révisée ne fait plus la distinction entre la commutation de circuits et la commutation de paquets. Avec l'évolution de la technologie, cette distinction n'est en effet plus actuelle. La téléphonie, par exemple, passe de plus en plus souvent par internet. En revanche, les différents types de surveillance sont désormais séparés entre la surveillance des services d'accès au réseau (section 8 et art. 60) et la surveillance d'applications (section 9 et art. 61 à 66).

À l'occasion de la révision totale de la LSCPT, le cercle des personnes tenues de coopérer a par ailleurs été élargi. Avec l'ancienne législation, par exemple, il n'était pas possible d'imposer des obligations en matière de surveillance aux fournisseurs de services de télécommunication non soumis à l'obligation d'annoncer, ou à ceux qui offrent leurs services de communication via internet mais sans être eux-mêmes fournisseurs d'accès. Dans le nouveau droit, l'art. 2, let. c, LSCPT inclut dans le champ d'application à raison des personnes les fournisseurs de services de communication dérivés, c'est-à-dire les fournisseurs de services qui se fondent sur des services de télécommunication et qui permettent une communication unilatérale (par ex. mise en ligne d'un document) ou multilatérale (par ex. messagerie instantanée ou service de chat). Par ailleurs, dans la nouvelle loi, le champ d'application à raison des personnes n'est plus lié à l'obligation d'annoncer prévue à l'art. 4 de la loi sur les télécommunications[2].

---

1 RS **780.1**
2 RS **784.10**

On pourrait ainsi s'attendre à ce que le nombre de personnes tenues de collaborer et d'exécuter activement des obligations de renseignement et de surveillance augmente. Or ce nombre, selon toute vraisemblance, devrait au contraire diminuer, car le Conseil fédéral a fait usage de la possibilité que lui confère la loi de dispenser des fournisseurs de services de télécommunication de certaines obligations légales de surveillance, en particulier ceux qui offrent des services de télécommunication de faible importance économique ou dans le domaine de l'éducation. Il faut partir du principe que le nombre de fournisseurs de services de télécommunication (FST) actifs soumis à l'obligation de surveiller passera de 600 environ selon le droit en vigueur à 30 voire 20 avec la nouvelle ordonnance. Il y a lieu de noter que cette libération de certaines obligations ne compromet en aucune manière la surveillance des télécommunications. De fait, les surveillances peuvent aussi être mises en œuvre auprès des FST ayant des obligations restreintes en matière de surveillance, puisque ces fournisseurs ont une obligation de tolérer des surveillances et une obligation de collaborer. Le Service SCPT doit prendre les mesures nécessaires pour que la surveillance puisse être mise en œuvre (art. 17, let. e, LSCPT; voir commentaire de l'art. 51).

Les fournisseurs de services de communication dérivés, qui doivent en principe tolérer une surveillance, peuvent en revanche être soumis à des obligations plus étendues en matière de fourniture de renseignements et de surveillance, notamment s'ils offrent des services d'une grande importance économique ou à un grand nombre d'utilisateurs (art. 27, al. 3, LSCPT). Le Conseil fédéral a là aussi précisé cette disposition, à l'art. 52. Les conditions étant très strictes, peu de fournisseurs de services de communication dérivés devront activement mettre en œuvre une surveillance (voir commentaire de l'art. 52) et un grand nombre de fournisseurs de services de télécommunication qui étaient jusqu'ici soumis à cette obligation ne le seront plus à l'avenir. La plupart des fournisseurs de services de télécommunication seront simplement tenus, le cas échéant, de tolérer une surveillance, qui sera exécutée par le Service de surveillance de la correspondance par poste et télécommunication (Service SCPT) ou par des tiers qu'il aura mandatés. À cette fin, les fournisseurs concernés doivent garantir sans délai l'accès à leurs installations et fournir les informations nécessaires à l'exécution de la surveillance. Ils doivent en outre supprimer les cryptages qu'ils ont opérés et livrer les données secondaires de télécommunication en leur possession (pour des précisions sur la notion de *données secondaires*, voir le commentaire introductif de la section 10 du chapitre 3). Donc comme évoqué ci-dessus, il n'existe pas de risque de lacunes dans la surveillance. Par ailleurs, la révision totale de la LSCPT a donné explicitement à certains services de la Confédération la possibilité de présenter au Service SCPT une demande de renseignements ou un ordre de surveillance (voir commentaire de l'art. 1). Le Secrétariat d'État à l'économie (SECO) pourra ainsi exercer plus simplement son droit de déposer une plainte pénale et combattre plus efficacement les appels publicitaires non désirés, puisqu'il pourra demander au Service SCPT des renseignements sur les raccordements concernés. Le Service de renseignement de la Confédération (SRC) pourra lui aussi demander tous types de renseignements au Service SCPT (cf. art. 15 LSCPT).

C'est désormais aussi la qualité des données relatives aux renseignements et aux surveillances qui doit pouvoir être contrôlée, afin de ne pas entraver le bon déroulement des surveillances. L'ordonnance indique dans quelles conditions la qualité des données est garantie et qui est chargé d'assurer la qualité requise (voir commentaire de l'art. 29). Le Service SCPT joue ici le rôle d'une autorité de surveillance et peut, en cas de non-respect des dispositions légales, par exemple des

dispositions sur la qualité, engager une procédure administrative, voire pénale, pour sanctionner le fournisseur concerné, conformément aux art. 41 ou 39, al. 1, let. a, LSCPT.

Afin de garantir la bonne exécution des surveillances ordonnées et la fourniture des renseignements demandés, la procédure déjà appliquée par le Service SCPT pour vérifier que les fournisseurs de services de télécommunication respectent leurs obligations (« compliance ») est désormais inscrite dans la loi. La procédure de contrôle de la garantie de la disponibilité à renseigner et à surveiller est décrite aux art. 31 à 34 LSCPT. Il s'agit de pouvoir vérifier que les fournisseurs soumis à des obligations en matière de surveillance et de fourniture de renseignements sont bien en mesure d'exécuter des surveillances et de livrer des renseignements conformément aux dispositions légales en vigueur (voir le ch. 2.7 du message relatif à la LSCPT[3] et le commentaire des art. 31 à 34).

3 FF **2013** 2442 ss

B. Commentaire article par article

Chapitre 1 Dispositions générales
Section 1 Introduction

Art. 1 Objet et champ d'application

L'*art. 1, al. 1*, correspond à l'art. 1, al. 1, de l'OSCPT du 31 octobre 2001[4] (état le 1er janvier 2012).

L'*al. 2* précise le champ d'application à raison des personnes selon l'art. 2 LSCPT. Comme dans l'art. 1 de l'OSCPT en vigueur, il mentionne en tant que destinataires des dispositions les autorités habilitées à ordonner une surveillance et celles qui dirigent la procédure (en règle générale, les ministères publics; *let. a*), ainsi que les autorités habilitées à autoriser une surveillance (en règle générale, les tribunaux des mesures de contrainte; *let. b*). La mention des autorités de police de la Confédération, des cantons et des communes (*let. c*) vise à permettre de tenir une liste exhaustive de tous les services autorisés à obtenir des renseignements. La liste des destinataires a aussi été étendue par rapport à l'OSCPT du 31 octobre 2001[5] pour tenir compte de l'art. 15, al. 2, let. a et b, LSCPT: le Service de renseignement de la Confédération (*let. d*) et le Secrétariat d'État à l'économie (SECO; *let. e*) figurent désormais dans l'énumération des services autorisés à obtenir des renseignements. Viennent s'y ajouter les autorités fédérales et cantonales visées à l'art. 15, al. 1, let. a, LSCPT qui sont compétente pour régler les affaires relevant du droit pénal administratif (*let. f*), sans oublier, naturellement, le Service de surveillance de la correspondance par poste et télécommunication (Service SCPT; *let. g*).

Une des principales nouveautés la LSCPT entièrement révisée est l'extension du cercle des **personnes dites obligées de collaborer**, c'est-à-dire des personnes qui sont soumises à la LSCPT et qui ont des obligations en vertu de celle-ci, qu'il s'agisse d'obligations actives, comme la disponibilité à surveiller (voir l'art. 32 LSCPT), ou d'obligations passives, comme l'obligation de tolérer une surveillance (voir art. 26, al. 2 et 6, 27, al. 1 et 2, 28 et 29 LSCPT). Les catégories de personnes obligées de collaborer sont énumérées à l'al. 2, let. h à m:

- *let. h:* les fournisseurs de services postaux (FSP) au sens de la loi sur la poste (LPO)[6] du 17 décembre 2010[7];

- *let. i:* les fournisseurs de services de télécommunication (FST) au sens de l'art. 3, let. b, de la loi du 30 avril 1997 sur les télécommunications (LTC)[8];

---

4 RS **780.11**
5 RS **780.11**
6 RS **783.0**
7 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. a, FF **2013** 2402 in fine
8 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. b (en particulier abandon du critère d'être soumis à concession ou à l'obligation d'annoncer), FF **2013** 2403

- *let. j:* les fournisseurs de services qui se fondent sur des services de télécommunication et qui permettent une communication unilatérale ou multilatérale (fournisseurs de services de communication dérivés)[9];

- *let. k:* les exploitants de réseaux de télécommunication internes[10];

- *let. l:* les personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers[11];

- *let. m:* les revendeurs professionnels de cartes ou de moyens semblables qui permettent l'accès à un réseau public de télécommunication[12].

Le Service SCPT tiendra une liste, qu'il actualisera régulièrement, des fournisseurs de services de communication dérivés au sens de l'art. 1, al. 2, let. j.

Art. 2 Termes et abréviations

L'art. 2 se fonde sur l'art. 2 de l'OSCPT du 31 octobre 2001[13] et renvoie à une annexe pour la définition des nombreux termes et abréviations utilisés dans le texte de l'ordonnance.

Section 2 Ordre de surveillance

Art. 3 Transmission au Service SCPT

L'*al. 1* définit les moyens de transmission que les autorités compétentes peuvent utiliser pour transmettre un ordre de surveillance, ainsi que les ordres de prolongation et de levée de la mesure, au Service SCPT et lui indiquer les droits d'accès à configurer.

Les droits d'accès au système de traitement du Service SCPT sont valables pour la mesure de surveillance pour laquelle ils ont été demandés et pour les membres des autorités de poursuite pénale désignés par l'autorité ayant ordonné la mesure qui sont chargés du dossier et qui doivent, pour les besoins de l'enquête pénale, traiter les données collectées. Les droits d'accès au système de traitement font habituellement l'objet d'une gestion à deux niveaux: généralement, chaque autorité de poursuite pénale associée à des mesures de surveillance désigne en son sein une personne chargée de gérer les utilisateurs et leurs droits d'accès respectifs pour chaque mesure de surveillance. Cette personne a la fonction d'administrateur de l'organisation (rôle OrgAdmin). Le Service SCPT donne quant à lui au détenteur du rôle OrgAdmin concerné les autorisations nécessaires pour la mesure de surveillance, selon les indications faites par l'autorité dans l'ordre de surveillance (voir l'art. 49). Le détenteur du rôle OrgAdmin gère ensuite de manière autonome dans le système de

---

9 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. c, FF **2013** 2403 in fine

10 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. d, FF **2013** 2404 in fine

11 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. e, FF **2013** 2405

12 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. f, FF **2013** 2405

13 RS **780.11**

traitement les droits d'accès des membres de son organisation pour les différentes mesures de surveillance, conformément aux indications de l'autorité qui les a ordonnées (cf. à cet égard les art. 8 et 9 de l'ordonnance du 15 novembre 2017 sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication[14] [OST-SCPT]).

Les autorités de poursuite pénale ont aussi la possibilité de confier, pour chaque mesure de surveillance, la gestion des droits de leurs utilisateurs au Service SCPT. Si l'autorité opte pour cette solution, le Service SCPT administre alors les droits d'accès des utilisateurs de l'autorité concernée pour la mesure en question, conformément aux indications figurant sur l'ordre de surveillance (voir l'art. 49).

En cas de changements qui affectent la mesure de surveillance (par ex. modification du type de surveillance ou ajout d'un nouveau type, modification de la ressource d'adressage surveillée en raison d'une erreur d'écriture des autorités de poursuite pénale), l'autorité qui a ordonné la surveillance doit transmettre au Service SCPT un nouvel ordre de surveillance soumis à émolument. Si le Service SCPT ou l'autorité de poursuite pénale se rend compte de l'erreur avant que le mandat n'ait été transmis au fournisseur, seul le mandat correct est facturé. Aucun nouvel émolument n'est par ailleurs perçu pour des modifications des droits d'accès.

Sont des moyens de transmission sûrs autorisés par le Service SCPT au sens de la *let. a*, par exemple, une interface électronique répondant aux normes de l'Institut européen des normes de télécommunication (ETSI) ou les solutions de chiffrement des courriels utilisées par le Service SCPT. Le département fixe les prescriptions s'y rapportant dans l'ordonnance du Département fédéral de justice et police (DFJP) du 15 novembre 2017 sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT; voir aussi le commentaire de l'art. 68).

La *let. b* autorise une transmission des données exposées ci-dessus par poste ou télécopie (au moyen des formulaires mis à disposition à cette fin par le Service SCPT), mais uniquement dans les cas où l'utilisation d'un moyen de transmission selon la let. a n'est pas possible pour des raisons techniques. Les autorités de poursuite pénale. doivent donc transmettre les documents au Service SCPT en priorité conformément à la let. a. Elles doivent en particulier tout mettre en œuvre pour être en mesure de le faire.

La *let. c* dispose que lorsque la surveillance est ordonnée par téléphone, ce qui n'est autorisé qu'en cas d'urgence (par ex. pour rechercher des personnes disparues ou des personnes condamnées ou pour faire exécuter une surveillance en dehors des heures normales de travail), l'ordre proprement dit doit ensuite être transmis à l'aide d'un moyen visé aux let. a ou b.

L'*al. 2* prévoit le remplacement des moyens de transmission selon l'al. 1, let. a, par un accès en ligne au système de traitement du Service SCPT. Cet accès facilitera considérablement la communication des ordres par les autorités habilitées à ordonner des surveillances. C'est au Service SCPT qu'il appartient de fixer la date à partir de laquelle la transmission ne pourra plus se faire qu'au moyen de l'accès en ligne.

14 RS **780.12**

Art. 4 Mise en œuvre de la surveillance

Correspondant pour l'essentiel à l'art. 17, al. 1 et 6, de l'OSCPT dans sa teneur du 31 octobre 2001[15], l'*art. 4* règle la mise en œuvre de la surveillance.

L'*al. 1* reprend la réglementation en vigueur.

Si une personne obligée de collaborer est empêchée, pour des problèmes d'exploitation technique, de remplir ses obligations en matière de surveillance de la correspondance par poste et télécommunication, elle est désormais tenue, en application de l'*al. 2*, non seulement d'aviser immédiatement le Service SCPT, mais aussi de lui transmettre une justification écrite. Le terme problèmes d'exploitation couvre des problèmes de nature aussi bien technique qu'organisationnelle. Ces problèmes peuvent avoir des conséquences pour les fournisseurs concernés (par ex. art. 33, al. 5, et 34, al. 1, LSCPT).

Il est important que les personnes obligées de collaborer informent sans délai le Service SCPT de tout problème susceptible de retarder la mise en œuvre d'une surveillance. Cette communication doit se faire immédiatement par téléphone au point de contact compétent au sein du Service SCPT. Concrètement, lorsqu'elle ne peut pas exécuter un ordre de surveillance ou remplir ses obligations concernant une surveillance en temps réel, la personne obligée de collaborateur appelle le numéro central du secteur d'activité concerné si le problème survient pendant les heures de travail normales ou le numéro du service de piquet si le problème se produit en dehors des heures de bureau. Elle transmet ensuite au Service SCPT le jour ouvré suivant une annonce de dérangement écrite indiquant la durée exacte du dérangement, la nature du problème, un déroulé chronologique des mesures engagées et le statut du problème. Si le dérangement n'a pas encore pu être levé le jour ouvré suivant, elle doit faire parvenir au Service SCPT une communication écrite similaire une fois le problème réglé. Le Service SCPT doit lui aussi informer sans délai les personnes obligées de collaborer s'il n'est pas en mesure d'exécuter les surveillances qui sont de son ressort en raison de problèmes d'exploitation.

L'*al. 3* prévoit que quelle soit l'origine du problème, la personne obligée de collaborer doit enregistrer, pendant la durée fixée par le DFJP dans les prescriptions techniques, au moins les données secondaires issues de la surveillance en temps réel et les livrer ensuite dès que possible (pour des précisions sur la notion de *données secondaires issues de la surveillance en temps réel*, voir le commentaire introductif de la section 10 du chapitre 3). Si ces données ne devaient plus être disponibles ou qu'elles étaient incomplètes, la personne obligée de collaborer est tenue de livrer sans délai au Service SCPT les données secondaires correspondantes issues de la surveillance rétroactive (pour des précisions sur la notion de *données secondaires issues de la surveillance rétroactive*, voir le commentaire introductif de la section 10 du chapitre 3).

Art. 5 Protection du secret professionnel et du secret de fonction

L'*art. 5* correspond aux art. 17, al. 2 (surveillance des services téléphoniques) et 25, al. 2 (surveillance de l'Internet), OSCPT dans sa teneur du 31 octobre 2001[16]. Il a pour objet la protection du secret professionnel et du secret de fonction. Il y a lieu de

15 RS **780.11**
16 RS **780.11**

noter que cette disposition ne s'applique qu'aux cas dans lesquels le Service SCPT constate que la surveillance concerne une personne astreinte au secret professionnel ou au secret de fonction et qu'aucune mesure de protection selon l'art. 271 CPP ou l'art. 70*b* PPM n'a été ordonnée (*let. a et b*).

L'art. 16, let. e, LSCPT dispose que le Service SCPT met en œuvre les mesures visant à protéger le secret professionnel et le secret de fonction qui ont été ordonnées par l'autorité qui a autorisé la surveillance. « Cette tâche est étendue à la surveillance de la correspondance par poste, étant donné qu'elle a également tout son sens dans ce domaine. Cette disposition est à mettre en relation avec les art. 271 et 274, al. 4, let. a, CPP et les art. 70*b* et 70*e*, al. 4, let. a, PPM. Ces articles mentionnent le régime applicable à la surveillance considérée, lorsqu'il s'agit de protéger un secret professionnel, dont l'autorité de poursuite pénale ne doit pas avoir connaissance (voir commentaire des art. 271 CPP et 70*b* PPM). Le service prend les dispositions nécessaires permettant la mise en œuvre des mesures décidées dans le cadre des articles précités; mais il ne procède pas lui-même au tri dont il est fait mention dans ces articles (art. 271, al. 1 CPP[17] et art. 70*b*, al. 1 PPM[18]) »[19].

Aux termes des art. 15, let. j et k (correspondance par poste), et 49, al. 1, let. k et l (correspondance par télécommunication), l'ordre de surveillance transmis au Service SCPT doit, le cas échéant, contenir une mention indiquant que des personnes sont tenues au secret professionnel ou au secret de fonction selon l'art. 271, al. 1, CPP ou de l'art. 70*b* PPM et préciser les mesures visant à les protéger; voir aussi l'art. 9, al. 2, let. i, qui dispose que le dossier de surveillance doit contenir l'indication des mesures de protection particulières ordonnées.

En vertu de la LSCPT, le Service SCPT peut non seulement effectuer un examen formel des ordres de surveillance qui lui sont transmis, mais aussi les soumettre à un examen matériel sous l'angle du droit administratif[20]. Le Service SCPT peut constater, dans le cadre de cet examen, que la désignation de la profession d'une personne indique qu'elle est tenue au secret professionnel alors qu'aucune mesure de protection n'a été ordonnée.

Si la surveillance vise par exemple un médecin, lequel est astreint, par définition, au secret professionnel, et qu'aucune mesure de protection particulière au sens de l'art. 271 CPP ou de l'art. 70*b* PPM n'a été ordonnée, le Service SCPT exécute la surveillance, mais ne donne pas accès dans un premier temps aux données collectées à l'autorité qui a ordonné la mesure. Il en informe cette dernière et l'autorité qui a autorisé la surveillance, laquelle a la possibilité d'approuver la surveillance en l'assortissant de la condition d'opérer un tri des informations conformément aux art. 271, al. 1, et 274, al. 4, let. a, CPP ou 70*b* et 70*e*, al. 4, let. a, PPM. L'autorité habilitée à autoriser la surveillance peut désigner un responsable chargé de consulter préalablement les données collectées et de les trier. Le Service SCPT attribue à cette personne les autorisations pour se connecter au système de traitement ou lui donne un accès direct aux données qui y sont enregistrées. L'autorité habilitée à autoriser la surveillance indique ensuite au Service SCPT quelles sont les données que peut

17 RS **312.0**
18 RS **322.1**
19 FF **2013** 2421 ; voir aussi le commentaire des art. 271 CPP et 70*b* PPM dans le message concernant la LSCPT
20 FF **2013** 2392, ch. 1.4.5

consulter l'autorité qui a ordonné la surveillance. Lorsqu'un tri est ordonné, l'autorité habilitée à autoriser la surveillance transmet périodiquement au Service SCPT une liste des données qui peuvent être transmises et charge le service de procéder au tri dans le système de traitement. Concrètement, l'autorité qui a ordonné la surveillance ne peut accéder qu'aux seules données sélectionnées par l'autorité habilitée à autoriser la surveillance. Le Service SCPT supprime toutes les autres données[21]. Cette procédure vaut pour toute la durée de la surveillance.

La *let. c* précise que la disposition de l'alinéa précédent s'applique par analogie au Service de renseignement de la Confédération en sa qualité d'autorité habilitée à ordonner une surveillance. Dans ce cas, l'autorité chargée d'autoriser la mesure est le Tribunal administratif fédéral.

Art. 6 Obligation de garder le secret

L'*art. 6* reprend les dispositions des art. 17, al. 7, et 25, al. 7, de l'OSCPT dans sa teneur du 31 octobre 2001[22]. Il réglemente l'obligation de garder le secret.

Le secret doit être gardé en toutes circonstances. Il y va non seulement du résultat des mesures de surveillance et des demandes de renseignements, mais aussi de la protection des droits de la personnalité des personnes concernées. Ni ces dernières, ni aucun tiers non autorisé ne doivent obtenir d'indices directs ou indirects sur des surveillances ou des fournitures de renseignements (voir aussi l'art. 320 CP et l'art. 39, al. 1, let. d, LSCPT).

Art. 7 Tri des données (filtrage)

L'*art. 7* explicite l'art. 17, let. g, LSCPT.

Le tri prévu se distingue de celui visé à l'art. 271 CPP ou 70*b* PPM pour protéger le secret professionnel et le secret de fonction (voir le commentaire de l'art. 5).

Le tri technique des données (filtrage) consiste à réduire, au moyen d'une procédure automatisée et selon les instructions documentées de l'autorité qui a ordonné la surveillance, la quantité de données à traiter, dans le but par exemple de faciliter l'analyse de grands volumes d'informations. Les données qui ne sont pertinentes pour l'enquête et qui n'apportent aucun renseignement utile aux autorités de poursuite pénale, comme celles concernant la télévision par internet, sont filtrées et retirées du flux de données avant même d'arriver dans le système de traitement.

Cette disposition ne vise pas les situations dans lesquelles la surveillance touche un grands nombre de tiers non concernés (par ex. surveillance du numéro de téléphone central d'une entreprise). En pareil cas, le Service SCPT prend aussi contact avec l'autorité qui a ordonné la mesure (par analogie avec la procédure prévue à l'art. 5).

Le Service SCPT filtre gratuitement les données à condition que la procédure puisse être automatisée et qu'elle n'entraîne pas une charge disproportionnée, c'est-à-dire que le Service SCPT puisse prendre les mesures nécessaires à cette fin dans le cadre de ses ressources en personnel et de ses moyens financiers et techniques. S'il constate que le filtrage demandé n'est techniquement pas possible ou que sa réalisation

21 Message du 21 décembre 2005 relatif à l'unification du droit de la procédure pénale, FF **2006** 1231

22 RS **780.11**

implique des efforts ou des coûts disproportionnés, le Service SCPT en avertit sans délai l'autorité qui a ordonné la surveillance en justifiant sa décision.

C'est aux autorités de poursuite pénale qu'il appartient de configurer les possibilités de filtrage définies par le Service SCPT, qui les conseille à cette fin. Compte tenu des exigences élevées posées à la mise en œuvre de ces filtrages, seules entrent en ligne de compte des procédures automatisées. Les autres types de tri sont en effet très compliqués, voire impossibles à réaliser[23]. Avant de demander un tri technique des données, l'autorité qui ordonne la surveillance prend contact avec le service SCPT pour s'assurer de la faisabilité du filtrage.

Art. 8 Enregistrement des communications téléphoniques à des fins probatoires

L'*art. 8, al. 1*, autorise le Service SCPT à enregistrer à des fins probatoires les appels téléphoniques en lien avec l'exécution de ses tâches. Il arrive fréquemment que les autorités qui ordonnent une surveillance transmettent l'ordre oralement (par ex. dans les situations d'urgence; voir l'art. 3, al. 1, let. c) ou fournissent ultérieurement des explications par téléphone. Ces cas ont parfois conduit par le passé à des divergences dans les déclarations des collaborateurs du Service SCPT et des collaborateurs de l'autorité qui avait ordonné la surveillance. Or il est indispensable de pouvoir établir les faits avec précision dans une enquête, d'où l'importance de disposer d'un tel outil d'administration des preuves.

Toutes les communications *écrites* – par exemple des ordres ou des décisions, les mandats de surveillance et la correspondance s'y rapportant, voir l'art. 9 (dossier de surveillance) – échangées entre le Service SCPT, les autorités et les personnes obligées de collaborer sont aujourd'hui déjà conservées. Il était donc nécessaire de prévoir la même réglementation pour les communications téléphoniques.

Seuls sont enregistrés les appels passés via les numéros de téléphone (y compris le numéro du service de piquet) de l'unité Gestion de la surveillance du Service SCPT.

Seul le préposé à la protection des données du Service SCPT est habilité, le cas échéant, à exploiter les enregistrements (*al. 2*).

Le Service SCPT ne peut conserver les communications téléphoniques enregistrées que pendant deux ans au plus (al. 3). Passé ce délai, les enregistrements doivent être détruits.

Art. 9 Dossier de surveillance

L'*art. 9* prévoit l'établissement d'un dossier de surveillance par le Service SCPT et en définit le contenu de manière exhaustive.

Le Service SCPT est tenu, conformément à l'*al. 1*, d'établir un dossier dans le système de traitement selon l'OST-SCPT pour chaque ordre de surveillance, sachant qu'un même ordre peut englober plusieurs mesures de surveillance.

L'*al. 2* énumère quant à lui les documents qu'il y a lieu de conserver dans le dossier, à savoir l'ordre de surveillance et ses annexes éventuelles, le ou les mandats de surveillance destinés aux personnes obligées de collaborer, accompagnés de la confirmation indiquant la date de transmission par le Service SCPT, la confirmation

23 FF **2013** 2424

d'exécution du ou des mandats par les personnes obligées de collaborer (avec indication de la date et de l'heure), les décisions de l'autorité habilitée à autoriser la surveillance et les éventuelles décisions sur recours, d'éventuels ordres de prolongation de la surveillance et les autorisations correspondantes de l'autorité compétente, l'ordre de lever la ou les surveillances, la correspondance (courriels, etc.) éventuellement échangée au sujet de la mesure, le cas échéant les mesures de protection particulières ordonnées (par ex. tri des données), ainsi que les documents de facturation.

C'est sur ce dossier que se fonde la perception des émoluments dus par l'autorité qui a ordonné la surveillance et le versement des indemnités aux personnes obligées de collaborer qui l'ont exécutée.
Le but est de pouvoir conserver les dossiers de surveillance sous une forme électronique, idéalement dans le système de traitement.
L'*al. 3* règle la conservation des données conformément à l'art. 11 LSCPT et leur destruction conformément à l'art. 14 OST-SCPT.

Section 3 Heures de travail et service de piquet

Art. 10 Heures normales de travail et jours fériés

L'*art. 10* est nouveau. Il définit à l'*al. 1* les heures de travail normales, qui correspondent à la pratique actuelle. Les heures sont indiquées par rapport à la Suisse.

L'*al. 2* énumère les jours fériés. Ceux-ci correspondent à ceux de la liste figurant à l'art. 66, al. 2, de l'ordonnance du 3 juillet 2001 sur le personnel de la Confédération[24].

Art. 11 Prestations en dehors des heures normales de travail

Bien que nouveau, l'*art. 11* ne fait que donner un cadre formel à la pratique actuelle du Service SCPT concernant les prestations fournies – par lui et par les personnes obligées de collaborer – pendant le service de piquet. En dehors des heures normales de travail, les mandats urgents doivent être annoncés par téléphone au Service SCPT via le numéro prévu pour le service de piquet.

L'*al. 1* contient une liste exhaustive des prestations fournies par le Service SCPT durant le service de piquet.

Pendant la durée du service de piquet, il n'est pas possible en particulier d'exécuter des ordres concernant des cas dits spéciaux, c'est-à-dire des surveillances ou des demandes de renseignements qui ne relèvent d'aucun des types définis dans l'ordonnance (surveillances ou renseignements qui n'ont pas fait l'objet d'une standardisation); voir aussi à ce sujet le commentaire des art. 23 et 26. En dehors des heures normales de travail et les jours fériés, le Service SCPT n'assure aucune formation et ne peut fournir des conseils que dans une mesure restreinte.

L'*al. 2* définit quels sont les fournisseurs qui sont tenus d'apporter leur soutien au Service SCPT en dehors des heures normales de travail. Concrètement, il s'agit des

24 RS **172.220.111.3**

FST et des fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 51. Dans un souci de proportionnalité, les FST ayant des obligations restreintes en matière de surveillance (art. 50), de même que les fournisseurs de services de communication dérivés qui n'ont pas d'obligations étendues en matière de surveillance (c'est-à-dire ceux qui ne remplissent pas les conditions de l'art. 51) et les fournisseurs de services postaux ne sont pas tenus de fournir des prestations durant le service de piquet. Aucun ordre les concernant ne pourra donc être exécuté pendant ce laps de temps.

Les surveillances et les renseignements visés à l'art. 25 qui ne relèvent pas des types ayant fait l'objet d'une standardisation sont des mesures spéciales que le Service SCPT exécute lui-même ou fait exécuter par des tiers. Comme l'exécution de ces mandats complexes requiert davantage de temps et nécessite, le plus souvent, la collaboration de plusieurs personnes, l'*al. 3* précise que les ordres de ce type ne sont ni transmis, ni exécutés en dehors des heures normales de travail.

Section 4 Statistiques

Art. 12 Statistique des mesures de surveillance et des renseignements

Le Service SCPT a la tâche d'établir une statistique des mesures de surveillance. La base légale se trouve à l'art. 11, al. 1, let. f, de la LSCPT du 6 octobre 2000 pour la surveillance de la correspondance postale et à l'art 13, al. 1, let. j, de la LSCPT du 6 octobre 2000 pour la surveillance de la correspondance par télécommunication. Les dispositions transitoires de l'OSCPT révisée (art. 74, al. 6, let. a) donnent la possibilité au Service SCPT de continuer à établir la statistique (art. 12) selon l'ancien droit pendant la durée de la phase transitoire. C'est pourquoi ces dispositions sont encore mentionnées ici.

Introduit par le Conseil des États le 10 mars 2014, l'art. 16, let. k, de la LSCPT entièrement révisée du 18 mars 2016 charge le Service SCPT de tenir une statistique des surveillances.

La nouvelle LSCPT contient d'autres dispositions concernant les statistiques à ses art. 35, al. 3 (recherche en cas d'urgence), et 36, al. 2 (recherche de personnes condamnées). L'OSCPT du 31 octobre 2001 en revanche ne contient encore aucune disposition à ce sujet. Il est possible de consulter les statistiques des surveillances depuis 2010 sur le site internet du Service SCPT (www.li.admin.ch > Thèmes > Statistiques). Sont présentés, notamment, les chiffres relatifs aux mesures ordonnées dans le cadre de procédures pénales et ceux concernant les recherches de personnes disparues.

Il est apparu, pendant les travaux de révision de l'OSCPT, qu'il était nécessaire d'inscrire la pratique actuelle dans l'ordonnance, en y intégrant une série de nouveautés. Il y a un intérêt public à connaître le nombre et le type de surveillances qui sont ordonnées tous les ans, ainsi que les coûts qu'elles génèrent.

Conformément à l'*al. 1*, les statistiques sont publiées une fois par an, généralement en début d'année, sur le site internet du Service SCPT (www.li.admin.ch). Une diffusion dans d'autres médias (télévision, radio, presse écrite, etc.) est aussi possible.

L'*al. 2* détermine le contenu des statistiques. Les *let. a* à *c* consacrent la pratique actuelle. Seule a été ajoutée la recherche de personnes condamnées à la let. c. Les *let. d* à *f* énumèrent quant à elles des nouveautés. La *let. b* mentionne la Principauté

de Liechtenstein, car ses autorités peuvent être considérées comme une autorité habilitée à ordonner une surveillance au sens de l'art. 35 LSCPT dès lors qu'il s'agit de retrouver une personne disparue (voir le ch. 3 de l'échange de notes du 27 octobre 2003[25]). L'*al. 2* ne contient pas finalement de disposition concernant le nombre de surveillances qui n'ont pas été autorisées (comme demandé par les conseillers aux États ANITA FETZ et STEFAN ENGLER le 10 mars 2014; BO 2014 E 112). Actuellement, seuls les tribunaux des mesures de contrainte pourraient fournir ce type de statistique. Le Service SCPT, lui, n'a connaissance que des surveillances qui sont refusées après qu'elles lui ont déjà été transmises. Il est cependant vraisemblable que les tribunaux rejettent un nombre non négligeable de surveillances avant que l'ordre correspondant soit transmis au Service SCPT, qui ne peut dès lors pas être au courant.

Le Service SCPT n'est pas non plus en mesure de fournir des indications sur l'efficacité des surveillances (voir la question de la conseillère nationale ALINE TREDE 15.5191 « Surveillance de la correspondance par poste et télécommunication. Efficacité de la surveillance rétroactive » et la réponse du Conseil fédéral du 16 mars 2015).

La question s'est posée de savoir, lors de la rédaction de cet article, s'il fallait comptabiliser les surveillances ordonnées ou plutôt les surveillances menées à leur terme au cours de l'année écoulée. Il a été décidé de poursuivre la pratique en vigueur et de comptabiliser les surveillances ordonnées. Un problème se pose toutefois pour calculer la durée des surveillances (*al. 2, let. d*) à cheval sur deux années civiles. Il n'est pas possible en effet de connaître, au moment de l'établissement des statistiques, en début d'année, la durée totale de surveillances ordonnées l'an dernier et qui ne sont pas encore terminées. Il faudra régler ce problème dans la pratique.

Art. 13 Statistique des mesures de surveillance ayant nécessité l'utilisation de dispositifs techniques ou de programmes informatiques spéciaux

L'art. 13 met en œuvre les nouveaux art. 269*bis*, al. 2, et 269*ter*, al. 4, CPP, s'agissant des ministères publics, et les nouveaux art. 70*bis*, al. 2, et 70*ter*, al. 4, PPM, s'agissant des juges d'instruction militaires, pour ce qui est du recours à des dispositifs techniques spéciaux (tels que les IMSI-catchers) et à des programmes informatiques spéciaux (« GovWare »). Ces nouvelles dispositions chargent le Conseil fédéral de régler les modalités. Celles-ci devraient par principe figurer dans les dispositions d'exécution du CPP et de la PPM (par ex. dans l'ordonnance concernant la justice pénale militaire, OJPM[26]). Il n'existe toutefois pas d'ordonnance générale concernant la procédure pénale et en édicter une à ce seul effet aurait été disproportionné. Vu que les dispositifs techniques spéciaux et les programmes informatiques spéciaux touchent, au sens large, à la matière de la surveillance qui est réglementée dans la LSCPT et l'OSCPT, il apparaît opportun d'intégrer à l'*art. 13* de l'ordonnance les dispositions régissant l'utilisation de ces outils.

L'établissement des statistiques est du ressort des autorités cantonales de poursuite pénale, des procureurs fédéraux et des juges d'instruction militaires. Ces derniers les

25 Échange de notes entre la Confédération suisse et la Principauté de Liechtenstein relatif à la collaboration dans le domaine de la surveillance transfrontalière des télécommunications, RS **0.780.151.41**

26 RS **322.2**

communiquent à l'Office de l'auditeur en chef. L'*al. 2* dispose que les statistiques établies par les différentes autorités publiques doivent être transmises au Service SCPT. Concrètement, ce sont les ministères publics cantonaux, le Ministère public de la Confédération et l'Office de l'auditeur en chef qui sont chargés de faire parvenir les statistiques au Service SCPT pendant le premier trimestre de l'année suivante, afin qu'elles puissent être compilées et publiées dans un délai utile.

La publication des statistiques avait initialement donné lieu à quelques réserves. La crainte était que la diffusion de ces informations compromette le bon déroulement des enquêtes, car les mesures de surveillance spéciales faisant appel à des équipements techniques particuliers, comme les GovWare, sont nettement moins nombreuses que les surveillances ordinaires. On redoutait en outre que la publication des statistiques cantonales puisse donner des indices sur la procédure pénale concernée, notamment dans le cas des petits cantons. Face à ces craintes justifiées, l'*al. 2* prévoit, à la *deuxième phrase*, que les statistiques qui sont publiées n'incluent pas les surveillances recourant à des dispositifs techniques spéciaux ou à de programmes informatiques spéciaux qui sont encore en cours. Les autorités de poursuite pénale ou le Ministère public de la Confédération informent le Service SCPT sitôt la mesure levée, afin qu'elle puisse être prise en compte dans la prochaine statistique.

Conformément à l'*al. 3*, une statistique consolidée est publiée tous les ans. Pour ne pas compromettre des enquêtes en cours ou des investigations futures, la statistique publiée n'indiquera pas le canton des autorités à l'origine des mesures ou, pour la Confédération, ne précisera pas de quelle autorité il s'agit.

Aucun émolument n'est perçu ni aucune indemnité n'est versée dans le cas de mesures nécessitant l'utilisation de dispositifs techniques et de programmes informatiques spéciaux. Les possibilités envisageables pour indiquer ces coûts ont fait l'objet d'un examen. Après leur acquisition, les programmes informatiques de ce type doivent régulièrement être adaptés aux spécificités de la procédure. Dans d'autres cas, des développements spécifiques sont nécessaires. En fonction du modèle de coûts des frais de licence viennent s'ajouter, pour chaque utilisation, au prix d'achat et aux coûts d'exploitation récurrents, sans oublier les coûts concernant notamment le personnel nécessaire pour préparer l'installation de GovWare (policiers, informaticiens, traducteurs, etc.). Au vu de la difficulté de signaler correctement les coûts induits par chaque utilisation, il a été décidé de ne pas indiquer les coûts liés à ces outils spéciaux.

Chapitre 2 Correspondance par poste

Art. 14 Obligation des FSP

L'*art. 14* reprend pour l'essentiel les dispositions de l'art. 14 OSCPT dans sa teneur du 31 octobre 2001[27]. Il définit les obligations des fournisseurs de services postaux (FSP); voir aussi à ce sujet les art. 19 (obligations des fournisseurs de services postaux) et 20 (informations préalables à un ordre de surveillance) LSCPT et leur

27 RS **780.11**

commentaire dans le message relatif à la LSCPT[28], ainsi que le commentaire de l'art. 16 ci-après.

L'*al. 1* fixe les types de surveillance que les FSP sont tenus d'exécuter, tandis que l'al. 2 définit avant tout les heures durant lesquelles ceux-ci doivent être joignables.

Art. 15 Ordre de surveillance

L'*art. 15* reprend en substance les dispositions de l'art. 11 OSCPT dans sa teneur du 31 octobre 2001[29]. Il définit les indications qui doivent figurer sur l'ordre de surveillance de la correspondance postale (pour le contenu des ordres de surveillance de la correspondance par télécommunication, voir le commentaire de l'art. 48).

Concernant les *let. j* et *k*, voir le commentaire de l'art. 5 (protection du secret professionnel et du secret de fonction).

Art. 16 Types de surveillance

L'*art. 16* correspond pour l'essentiel à l'actuel art. 12 OSCPT dans sa teneur du 31 octobre 2001[30]. Il définit les différents types de surveillance qu'il est possible d'ordonner concernant la correspondance postale.

Les données à fournir pour chaque type de surveillance sont sensiblement les mêmes, à la différence près que pour les surveillances en temps réel, il faut désormais aussi indiquer le lieu d'expédition de l'envoi postal (cf. let. b, ch. 4) et livrer la signature du destinataire (cf. let. b, ch. 6), pour autant que ces données soient disponibles. Le destinataire peut être la personne à qui l'envoi est destiné ou un tiers autorisé à réceptionner l'envoi. Il y a lieu de signaler que l'obligation d'enregistrer et de livrer des données secondaires se limite, comme le prévoit l'actuelle ordonnance, aux envois postaux avec justificatifs de distribution, Il faut entendre ici par « justificatif d'envoi » la confirmation remise à l'expéditeur qui envoie un recommandé ou un colis avec fonction de suivi des envois (« Track & Trace »). Les FSP doivent aussi livrer toute autre donnée qu'ils enregistrent (cf. let. c, ch. 2).

On notera encore que les services de communication électronique des FSP, par exemple les services de courriel de la Poste tels que PostMail, relèvent de la surveillance des télécommunications.

Chapitre 3 Correspondance par télécommunication

Compte tenu de la rapidité des progrès technologiques et de la diversité des installations des personnes obligées de collaborer, il n'est pas possible de dresser des listes exhaustives des nombreux services, options et paramètres concernant les types de renseignements et de surveillance. Ont donc plutôt été énumérés des exemples type.

28 FF **2013** 2425-2427
29 RS **780.11**
30 SR **780.11**

Le degré de détail a été considérablement augmenté par rapport à l'ordonnance en vigueur, de manière à répondre aux attentes exprimées pour une plus grande sécurité juridique.

Section 1 Dispositions générales concernant la fourniture de renseignements et les surveillances

Art. 17 Demandes de renseignements

Cet article définit la manière dont les autorités habilitées selon l'art. 15 LSCPT doivent transmettre les demandes de renseignements aux trois catégories de personnes obligées de collaborer (FST, fournisseurs de services de communication dérivés et exploitants de réseaux de télécommunication internes), de même que la manière dont les renseignements doivent être transmis en retour aux autorités concernées. Le Service SCPT exploite un système de traitement qui peut être utilisé entre autres à ces fins (composante système servant à la transmission des demandes et des renseignements).

L'*al. 1* dispose que les autorités habilitées doivent transmettre leurs demandes de renseignements via le système de traitement du Service SCPT et que les données demandées leur sont aussi livrées par ce canal. L'utilisation de tout autre moyen de transmission (par ex. courriel, lettre, téléphone ou fax) n'est admise que si la transmission en ligne via le système de traitement n'est pas disponible pour des raisons techniques ou s'il s'agit d'une urgence au sens de l'al. 3. Les autorités habilitées ne sont pas autorisées à transmettre des demandes de renseignements directement aux personnes obligées de collaborer. Elles doivent toujours passer par le Service SCPT (voir art. 26, al. 2).

L'*al. 2* mentionne des solutions alternatives – en l'occurrence le courrier postal ou une télécopie – pour la transmission des demandes au Service SCPT, mais aussi pour la livraison aux autorités des renseignements communiqués au Service SCPT. Comme indiqué plus haut, les personnes obligées de collaborer utilisent également le système de traitement pour fournir les données demandées (voir commentaire de l'art. 18). Des exceptions sont prévues lorsque le système n'est pas disponible pour des raisons techniques et dans les situations visées à l'art. 18, al. 3 et 5 (voir commentaire de l'art. 18).

En cas d'urgence, les autorités peuvent transmettre au Service SCPT les demandes de renseignements par téléphone, avec transmission ultérieure de la demande électroniquement selon l'al. 1 ou par écrit selon l'al. 2 (*al. 3*). Cette disposition se fonde sur la disposition prévue pour les ordres de surveillance urgents visés à l'art. 3, al. 1, let. c.

Selon l'*al. 4*, la demande de renseignements doit indiquer le nombre maximal d'enregistrements à livrer. Le système de traitement ne permet pas de sélectionner un nombre d'enregistrements à livrer plus élevé que la limite supérieure prédéfinie dans le programme. Ce mécanisme de protection vise un double objectif: d'une part, éviter la transmission d'un trop grand nombre de résultats à l'autorité compétente, ce qui peut avoir des conséquences en termes de coûts; d'autre part, prévenir une surcharge du système et des recherches non ciblées. Le terme « enregistrement » désigne le résultat d'une demande de renseignements.

Art. 18 Obligations concernant la fourniture de renseignements

Cet article précise les obligations des FST et des fournisseurs de services de communication dérivés en matière de fourniture de renseignements. Il semble utile d'expliquer, en préambule, la manière dont se déroule généralement l'exécution d'une demande de renseignements (par ex. aux fins de l'identification d'un usager): le fournisseur commence par chercher, généralement dans les données relatives à ses clients, mais aussi dans les données secondaires de télécommunication conservées ou disponibles si le fournisseur n'a pas d'obligation en matière de surveillance, celles qui correspondent aux critères de recherche indiqués dans la demande pour la période spécifiée. Il livre ensuite, conformément aux instructions figurant sur la demande, les renseignements souhaités sur les usagers, ou les utilisateurs finaux, et les services de télécommunication ou les services de communication dérivés qu'ils ont utilisés.

Vu que certains FST sont libérés de certaines obligations en matière de surveillance et que certains fournisseurs de services de communication dérivés sont soumis à des obligations étendues en matière de fourniture de renseignements, on distingue les sous-catégories ci-après de personnes obligées de collaborer:

- les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51;
- les FST ayant des obligations restreintes en matière de surveillance visés à l'art. 51;
- les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements visés à l'art. 22.

Les deux sous-catégories de FST ont en principe les mêmes obligations en matière de renseignements. Pour les FST ayant des obligations restreintes, la seule différence concerne la procédure de livraison des données (pas d'obligation de fournir les renseignements via une procédure automatisée selon l'al. 2 et autorisation de livrer les données en dehors du système de traitement conformément à l'al. 3) et les types de renseignements spéciaux dans le cas d'adresses IP qui ne sont pas attribuées de manière univoque (art. 37 et 38), que les FST ne sont pas tenus de livrer selon une procédure standard mais qu'ils peuvent fournir sans conditions de forme, en fonction des données dont ils disposent. Les trois sous-catégories ci-dessus de personnes obligées de collaborer doivent garantir leur disponibilité à renseigner. Elles doivent notamment être en mesure de fournir les renseignements visés aux art. 35 à 37 et 40 à 48, ainsi que ceux visés à l'art. 27 en relation avec les art. 35, 40, 42 et 43, concernant les services qu'ils proposent (*al. 1*).

Les autorités habilitées selon l'art. 15 LSCPT adressent leurs demandes de renseignements au Service SCPT via le système de traitement (composante système pour les renseignements), qui les retransmet ensuite aux personnes obligées de collaborer dès lors que celles-ci livrent aussi leurs renseignements via ce canal. Une fois la demande exécutée, les personnes obligées de collaborer enregistrent les données dans le système de traitement, qui les transmet aux autorités à l'origine des demandes. Dans les cas des personnes obligées de collaborer qui ne sont pas tenues de livrer leurs données via le système de traitement, c'est le Service SCPT qui se charge de leur faire parvenir les demandes des autorités et qui réceptionne les renseignements demandés, avant de les retransmettre aux autorités via le système de traitement.

Les types de renseignements selon les art. 34 à 41 se caractérisent par une densité normative élevée. Ils correspondent pour l'essentiel aux actuels renseignements simples A0. Compte tenu de leur très grand nombre (202 052 renseignements en 2016[31]), les demandes de renseignements simples sont traitées via une interface électronique du système de traitement, au moyen d'une procédure automatisée (traitement assuré 24 heures sur 24, 7 jours sur 7) (*al. 2*). L'automatisation du traitement requiert des prescriptions précises, concernant notamment les différents paramètres et types de données. Le DFJP a défini ces prescriptions dans une nouvelle ordonnance, l'OST-SCPT et son annexe technique 1.

L'*al. 3* permet aux FST ayant des obligations restreintes en matière de surveillance selon l'art. 51 de répondre par écrit aux demandes mentionnées, c'est-à-dire sans utiliser l'interface électronique du système de traitement. Tous les FST de cette catégorie ne possèdent pas en effet cette interface.

Il existe des types de renseignements spéciaux concernant les adresses IP qui ne sont pas attribuées de manière univoque (art. 38 et 39) et d'autres types de renseignements (art. 42 à 47) qu'il est aussi possible de fournir selon une procédure manuelle. Dans ce dernier cas, le mode de transmission – manuel ou automatisé – est laissé au choix des personnes obligées de collaborer. Celles d'entre elles qui sont tenues d'utiliser le système de traitement (*al. 4*), doivent livrer les renseignements via cet outil, même si la demande est traitée manuellement (*al. 2*).

L'*al. 4* définit les obligations concernant la fourniture des renseignements selon l'art. 38 (IR_8_IP (NAT)) et l'art 39 (IR_9_NAT), qui prévoient que les données secondaires doivent être conservées pendant six mois. Les FST ayant des obligations restreintes en matière de surveillance (art. 51), sont exemptés de l'obligation de conserver des données secondaires. Ils ne sont dès lors pas non plus tenus de fournir les renseignements ayant fait l'objet d'une standardisation qui sont visés aux art. 38 et 39. Ils restent en revanche soumis à l'obligation de livrer, sans condition de forme, les données secondaires dont ils disposent.

L'*al. 5* précise quelles catégories de personnes obligées de collaborer ne sont pas tenues de fournir les renseignements selon les différents types définis. Ces fournisseurs – à savoir les fournisseurs de services de communication dérivés n'ayant pas d'obligations étendues en matière de fourniture de renseignements (c'est-à-dire ceux qui ne remplissent pas les conditions de l'art. 22) et les exploitants de réseaux de télécommunication internes (art. 1, al. 2, let. k) – livrent les renseignements en leur possession par la poste, par télécopie ou via un moyen de transmission sûr admis par le Service SCPT. Ces deux catégories de personnes obligées de collaborer peuvent décider de livrer leurs renseignements via le système de traitement, selon la procédure standardisée. Sont également exemptées les personnes qui mettent leur accès à un réseau public de communication à la disposition de tiers (art. 1, al. 2, let. l). Toutefois, si une surveillance est ordonnée, elles doivent fournir les renseignements nécessaires à l'exécution de la surveillance (art. 29, al. 1, let. b, LSCPT).

Si le nombre de résultats trouvés dépasse le nombre maximal d'enregistrements à livrer indiqué par l'autorité, le fournisseur communique le nombre de résultats obtenus, mais ne livre aucune donnée (*al. 6*). L'autorité peut alors soumettre une nouvelle demande de renseignements en affinant ses critères de recherche ou en sélectionnant un nombre maximal d'enregistrements plus élevés, sans toutefois

31 Statistiques du Service SCPT : https://www.li.admin.ch/fr/themes/statistiques

dépasser la limite supérieure prescrite par le système. Si l'autorité a besoin de davantage d'enregistrements que ne le permet le système, elle peut soumettre au Service SCPT une demande de renseignements spéciaux au sens de l'art. 25.

Art. 19 Identification des usagers

De manière générale, il suffit que le FST qui fournit le service concerné identifie les usagers par des moyens appropriés (*al. 1*).

Dans le cas de points d'accès publics au réseau WLAN exploités à titre professionnel, les FST doivent veiller à identifier par des moyens appropriés les utilisateurs finaux, c'est-à-dire les utilisateurs effectifs (*al. 2*). L'expression « exploité à titre professionnel » signifie qu'un FST ou un prestataire de services informatiques spécialisé dans les points d'accès publics au réseau WLAN assure aussi l'exploitation technique du point d'accès en question et d'autres points accès qu'il mettrait à disposition. Lorsqu'une personne physique ou morale exploite techniquement, à partir de son propre accès à internet, un point d'accès public au réseau WLAN qu'elle met à la disposition de tiers, le FST qui fournit l'accès à internet ne doit pas veiller lui-même à l'identification des utilisateurs finaux. Dans ce cas, l'identification des usagers conformément à l'al. 1 est suffisante. C'est dans un souci de proportionnalité que l'identification obligatoire des utilisateurs finaux est limitée aux points d'accès publics « exploités à titre professionnel ». Il s'agit d'éviter que les ménages et les petites entreprises qui laissent leur réseau WLAN ouvert ne doivent procéder à des identifications complexes.

On entend par moyens d'identification appropriés – il est ici question d'identification indirecte – des enregistrements implicites ou simplifiés fondés sur des indications dignes de confiance (*trusted*), par exemple:

- identification au moyen du code d'accès envoyé par SMS sur le téléphone mobile et enregistrement du numéro MSISDN;
- identification au moyen de la carte de crédit et enregistrement des données d'autorisation;
- identification au moyen d'une carte d'embarquement valable dans les aéroports et enregistrement des données de la carte;
- identification au moyen d'une carte de voyageur fréquent permettant l'accès aux salles VIP et enregistrement des données d'autorisation;
- identification au moyen de la zone de lecture optique (MRZ) du document d'identité et enregistrement des données qui s'y trouvent;
- identification au moyen d'indications dignes de confiance de partenaires d'itinérance et enregistrement des données d'autorisation;
- indentification au moyen du code d'accès individuel attribué un client lors de son enregistrement dans un hôtel;
- identification au moyen de la carte SIM et enregistrement de l'IMSI.

Art. 20 Saisie d'indications relatives aux personnes dans le cas de services de communication mobile

L'*art. 20* reprend, en les précisant, les dispositions notamment de l'art. 19*a* l'OSCPT dans sa teneur du 31 octobre 2001[32]. Il se fonde en particulier sur les normes de délégation de compétences au Conseil fédéral prévues dans les art. 21, al. 1, let. d, 22, al. 2, et 23, al. 3, LSCPT[33].

Conformément à l'*al. 1,* il faut veiller, lors de la première activation de moyens d'accès à des services de communication mobile (par ex. GSM, GPRS, UMTS, LTE, VoLTE, VoWiFi), à identifier les usagers au moyen d'un passeport, d'une carte d'identité ou d'un titre de séjour pour étrangers au sens des art. 71 et 71*a* de l'ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative (OASA). Il faut entendre ici par « activation » le moment à partir duquel l'usager peut utiliser le service concerné, par exemple le moment de la remise dans le cas d'un moyen d'accès déjà activé ou le moment de l'activation du profil par le fournisseur dans le cas d'une carte SIM intégrée dans l'équipement terminal mobile (*embedded SIM* ou eSim). Exemple: un magasin d'électronique, qui ne procède pas lui-même à l'activation de services de communication mobile, vend à un client une tablette conçue pour la communication mobile et équipée d'une carte SIM intégrée. Dans un premier temps, le client peut uniquement se connecter au WiFi. Pour pouvoir utiliser le « moyen d'accès » (c'est-à-dire la carte SIM intégrée dans l'appareil) au réseau mobile, il doit faire activer la carte SIM intégrée auprès d'un fournisseur de services de communication mobile. Comme il est intégré dans la tablette, le moyen d'accès est « remis » au client au moment de l'achat de l'appareil. Il n'est toutefois pas encore opérationnel. Par conséquent, ce n'est pas le moment de la remise qui intéresse les autorités de poursuite pénale, mais bien le moment de l'activation. Il importe également de savoir qui procède à l'activation. Dans cet exemple, ce n'est pas le magasin d'électronique qui s'en charge. Aussi n'est-il pas tenu d'enregistrer les données du client (il n'est dès lors pas assimilé à un revendeur de cartes ou d'autres moyens d'accès similaires). Il appartient au fournisseur de services de communication mobile qui active la carte d'identifier l'usager.

On part du principe que lors de contacts ultérieurs avec un même client, le fournisseur vérifie à chaque fois les indications et la pièce d'identité, ces vérifications étant aussi dans son intérêt. Le terme « moyens d'accès » est la forme abrégée de l'expression « moyen permettant l'accès au service de télécommunication » (art. 21, al. 1, let. e, LSCPT).

La vérification de l'identité à l'aide d'un document officiel est donc impérative pour la communication mobile. Cette règle, qui vaut déjà pour les usagers de services de téléphonie mobile à prépaiement, est désormais étendue aux usagers de tous les services de communication mobile, indépendamment des modalités de paiement desdits services (sur abonnement, à prépaiement, offre gratuite, etc.). On relèvera néanmoins que la production d'une pièce d'identité est demandée depuis longtemps déjà lors de la conclusion d'un abonnement.

Les fournisseurs de services de télécommunication, les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements visés à l'art. 22 et les revendeurs visés à l'art. 2, let. f, LSCPT doivent

32 RS **780.11**
33 FF **2013** 2429-2430

veiller à une saisie correcte des données de l'usager au moyen de la pièce d'identité produite (art. 23, al. 1, LSCPT). La copie de la pièce d'identité permet de contrôler l'exactitude des données enregistrées. Si la pièce d'identité possède une zone de lecture optique (*machine readable zone*, MRZ), il est recommandé de procéder à une lecture optique, c'est-à-dire automatique, des données de l'usager et de les enregistrer comme suit:

- Saisir comme alias ou identité secondaire les nom et prénom à partir de la zone de lecture optique, où ils sont disponibles dans l'alphabet latin réduit (translittération), de sorte qu'ils peuvent être directement utilisés pour la recherche normale (c'est-à-dire exacte) par nom (voir art. 35).

Pour les indications ci-après relatives à la personne ou à la pièce d'identité, il y a lieu là aussi de privilégie la lecture optique, si disponible, à la saisie manuelle:

- pays ou organisation qui a établi le document (sigle de trois lettres);
- numéro de la pièce d'identité;
- nationalité (sigle de trois lettres);
- date de naissance du titulaire (YYMMDD);
- sexe (« M »=masculin / « F »=féminin / « < »=aucune indication).

Remarque: l'expression « si disponible » (*if available*) signifie, aux termes de l'OSCPT, que les données doivent être livrées dès lors qu'elles sont techniquement disponibles, par exemple un paramètre déterminé dans un message de signalisation. En pratique, la disponibilité des données dépend de toute une série de facteurs, comme la technologie, les normes applicables, le service de communication et le cas de figure concret. Les détails sont réglés dans l'annexe 1 de l'OME-SCPT. En d'autres termes, il y a une obligation pour les fournisseurs lorsque les données existent et qu'elles doivent être livrées ou enregistrées aux fins de la fourniture de renseignements ou de la mise en œuvre de surveillances rétroactives. Exemple: les usagers ne sont pas toujours identifiés par un numéro de client et les fournisseurs ne sont pas non plus tenus d'en générer un. C'est pourquoi le libellé de l'art. 34, al. 1, let. a, précise « s'il est disponible ». Attention cependant à ne pas confondre les expressions « si disponible », qui figure dans l'OSCPT, et « dont ils disposent », qui apparaît dans la LSCPT (par ex. à l'art. 28, al. 2) et désigne une obligation passive de tolérer une surveillance (et non une obligation active d'enregistrer des indications).

Les données selon l'al. 2 ou 3 qui ne figurent pas sur la pièce d'identité (par ex. l'adresse) sont saisies sur la base des indications du client et livrées telles quelles. Les revendeurs transmettent les données saisies et les copies électroniques des pièces d'identité aux fournisseurs des services auxquels le moyen vendu permet d'accéder.

Lorsque le client ou le fournisseur modifie les données (par ex. modification de l'adresse de facturation), les nouvelles données doivent être sauvegardées. Il n'y a toutefois pas d'obligation de contrôler et de mettre à jour régulièrement ces données. De même, on n'exige pas du client qu'il livre de nouvelles données par la suite. Il convient de relever que les fournisseurs sont tenus de bloquer l'accès aux services de télécommunication des clients n'ayant pas souscrit d'abonnement lorsque leurs données n'ont pas été correctement saisies lors de l'ouverture de la relation commerciale (art. 6*a* LTC[34]).

34 FF **2016** 1849

La disposition essentielle est que les fournisseurs doivent conserver les données saisies lors de l'enregistrement du client pendant toute la durée de la relation contractuelle et pendant six mois après la fin de celle-ci (art. 21, al. 2, LSCPT).

Vu le grand nombre d'enregistrements incorrects constatés par le passé, il a semblé nécessaire de prévoir des mesures supplémentaires. La copie de la pièce d'identité apparaît actuellement comme le moyen le plus approprié de prévenir ces erreurs. Aucune autre solution n'a jusqu'ici été évoquée, même si d'autres possibilités sont envisageables, comme la norme Swiss-ID, l'identité électronique (eID) ou un autre moyen similaire (voir la loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique [loi sur la signature électronique, **SCSE**][35] et la future loi eID)[36] (voir l'art. 23, al. 1, LSCPT). Une identification en ligne qui satisferait aux exigences de qualité et de sécurité fixées par la FINMA pour le secteur bancaire dans sa circulaire 2016/7 « Identification par vidéo et en ligne » serait aussi envisageable. Avec l'identité électronique (eID), une procédure d'identification en ligne ou toute autre méthode similaire, l'usager ne doit pas être présent physiquement lors de l'enregistrement de ses données.

Le fournisseur doit enregistrer dans son système une copie électronique – photographie ou copie numérisée – parfaitement lisible de la pièce d'identité du client (al. 1, deuxième phrase). Il n'est pas nécessaire d'en conserver une copie sur papier (voir l'art. 23, al. 1, LSCPT). En cas d'identification au moyen de l'identité électronique ou d'une autre procédure analogue, les données sont saisies électroniquement, si bien que la copie de la pièce d'identité est superflue. Les renseignements selon les al. 2 ou 3 qui ne figurent pas dans l'identité électronique (par ex. l'adresse), sont saisis conformément aux indications de l'usager.

L'*al. 2* précise quelles indications doivent être saisies dans le cas de personnes physiques. L'art. 19*a* OSCPT dans sa teneur du 31 octobre 2001[37] définissait déjà les données qu'il y a lieu d'enregistrer (nom, prénom, date de naissance, type et numéro de la pièce d'identité, adresse). Ces données correspondent à la pratique actuelle. En plus de ces informations, doivent désormais aussi être indiqués le pays ou l'organisation qui a établi le document, la nationalité du titulaire (art. 21, al. 1, let. b, LSCPT et, si elle est connue, sa profession (art. 21, al. 1, let. a, LSCPT). La saisie du pays ou de l'organisation qui a établi le document est nécessaire pour permettre aux autorités de poursuite pénale d'effectuer, le cas échéant, des vérifications.

L'*al. 3* énumère les données à saisir dans le cas de personnes morales: le nom, le siège et les coordonnées (*let.a*), le numéro d'identification de l'entreprise (IDE) en application de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises[38] (*let. b*) et, si ces données sont disponibles, les nom et prénom des personnes qui utilisent les services offerts par le fournisseur, par exemple des collaborateurs (*let. c*).

En application de l'*al. 4*, les FST, les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et les revendeurs doivent saisir des indications supplémentaires pour les relations

35 RS **943.03**
36 https://www.egovernment.ch/fr/umsetzung/schwerpunktplan/elektronische-identitat/
37 RS **780.11**
38 RS **431.01**

commerciales sans abonnement (services à prépaiement, offres gratuites). Les revendeurs de simples cartes téléphoniques permettant de téléphoner sans argent liquide dans les cabines publiques (par ex. les Taxcards contenant un crédit qui sont vendues dans les kiosques) ne sont pas concernés[39]. Conformément à l'art. 1, let. b, de l'ordonnance du 9 mars 2007 sur les services de télécommunication (OST)[40], le terme « client » désigne toute personne physique ou morale qui a conclu un contrat avec un fournisseur de services de télécommunication portant sur l'utilisation de ses services. Cette définition vaut par analogie pour les clients de fournisseurs de services de communication dérivés. Ces données supplémentaires dont l'enregistrement est demandé doivent permettre d'identifier l'auteur d'une saisie manifestement incorrecte (voir aussi la norme pénale correspondante à l'art. 39, al. 1, let. c, LSCPT).

Art. 21 Délais de conservation

L'*art. 21* met en œuvre les dispositions des art. 21, al. 2 (renseignements sur les services de télécommunication), et 22, al. 2 (renseignements visant à identifier les auteurs d'infractions par Internet), LSCPT.

L'*al. 1*, *première phrase*, prévoit que toutes les indications saisies concernant les services de télécommunication et celles saisies aux fins de l'identification – notamment des auteurs d'infractions sur Internet – doivent être conservées et pouvoir être livrées électroniquement pendant toute la durée de la relation commerciale, ainsi que six mois après la fin de celle-ci. Les *indications relatives aux services de télécommunication* comprennent aussi les indications relatives aux personnes selon l'art. 20, al. 1 à 3. Voir également les dispositions transitoires de l'art. 45, al. 3, LSCPT.

Construit de manière analogue à la première phrase, l'*al. 1*, *deuxième phrase*, fixe la durée de conservation des données d'identification selon l'art. 19, al. 2, que les FST qui exploitent, à titre professionnel, des points d'accès publics au réseau WLAN sont tenus d'enregistrer. Par souci de simplification, la durée de l'autorisation d'accès au point d'accès public au réseau WLAN a été prise comme équivalent de la durée de la relation commerciale.

Afin d'éviter toute contradiction avec le délai de conservation prévu à l'art. 26, al. 5, LSCPT, l'*al. 2* définit, en exécution des art. 21, al. 2, deuxième phrase, et 22, al. 2, deuxième phrase, LSCPT, les indications qui ne doivent être conservées et livrées que pendant six mois. Ce délai plus court s'applique aux identifiants des équipements effectivement utilisés, comme le numéro IMEI, l'adresse MAC (voir les art. 36, al. 1, let. d, et 41, al. 1, let. d), ainsi qu'aux indications relatives à la fourniture de renseignements selon les art. 37, 38 et 39.

Dans le cas des FST ayant des obligations restreintes en matière de surveillance selon l'art. 51, le délai de conservation prévu à l'al. 2 serait en contradiction avec l'exonération de certaines obligations en matière de surveillance en application de l'art. 51. Aussi cette exonération est-elle concrétisée dans cette disposition également.

Conformément à l'*al. 3*, les données mentionnées à l'al. 2 doivent être détruites après six mois. Cette disposition met en œuvre une recommandation du 19 septembre 2017 de la Commission des affaires juridiques du Conseil national.

---

39 Voir le message du 27 février 2013 concernant la LSCPT, FF **2013** 2405
40 RS **784.101.1**

Art. 22 Fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements

Toujours plus utilisés, les services de communication dérivés ne cessent de gagner en importance. En matière de surveillance des télécommunications, la loi impose aux fournisseurs traditionnels de ce type de services des obligations plus restreintes qu'aux FST usuels (soumis à des obligations étendues). En effet, les fournisseurs de services de communication dérivés doivent uniquement tolérer la surveillance et livrer les indications dont ils disposent qui sont nécessaires pour mettre en œuvre la surveillance. Concrètement, ils doivent fournir sur demande les données secondaires de télécommunication de la personne surveillée qui sont en leur possession (art. 27, al. 2, LSCPT). Il peut cependant arriver que cette obligation minimale ne soit pas suffisante dans le cas d'infractions commises par Internet. C'est pourquoi le législateur a donné la compétence au Conseil fédéral, à l'art. 22, al. 4, LSCPT, de soumettre également les fournisseurs de services de communication dérivés à des obligations étendues en matière de fourniture de renseignements. Concrètement, il s'agit des mêmes obligations que celles auxquelles sont soumis les FST. Les fournisseurs de services de communication dérivés qui ont des obligations étendues doivent donc remplir toutes les obligations selon l'art. 22, al. 1 et 2, LSCPT.

L'*al. 1* concrétise les critères qui doivent être réunis pour qu'un fournisseur de services de communication dérivés soit considéré comme ayant des obligations étendues en matière de fourniture de renseignements. C'est le cas lorsque, aux termes de la *let. a*, il a dû traiter 100 demandes de renseignements au cours des douze derniers mois (la date de référence étant fixée au 30 juin) ou que, conformément à la *let. b*, il a enregistré, en Suisse, un chiffre d'affaires annuel d'au moins 100 millions de francs pendant deux exercices consécutifs.

La *let. a* se réfère au critère du grand nombre d'utilisateurs mentionné à l'art. 22, al. 4, LSCPT. Il est très difficile, du point de vue des télécommunications, de donner une définition *absolue* de l'expression « grand nombre d'utilisateurs » et d'arrêter par avance un nombre précis, qui plus est si l'on pense aux différents services techniques qui existent. La let. a opte pour un critère qui a fait ses preuves dans la pratique, à savoir le nombre de demandes de renseignements traitées. Comme le montrent les statistiques de la surveillance des télécommunications de ces dernières années, il s'agit d'un critère fiable et adapté au type de services proposés pour appréhender la notion du grand nombre d'utilisateurs. Il permet aussi de tenir compte du principe de proportionnalité, dès lors que seuls sont visés les fournisseurs qui sont réellement importants pour la surveillance des télécommunications.

Le deuxième critère, à la let. b, est en outre subordonné à deux conditions supplémentaires: une grande partie de l'activité commerciale du fournisseur doit consister en la fourniture de services de communication dérivés et 5000 usagers au moins doivent utiliser ses services. Les seuils fixés sont très élevés de manière à protéger les PME suisses.

L'*al. 2* définit les éléments constitutifs d'un groupe de sociétés. Si un fournisseur contrôle une ou plusieurs entreprises tenues d'établir des comptes, le fournisseur et les entreprises contrôlées sont considérées comme formant une seule et même unité pour calculer les valeurs selon l'al. 1, let. a et b. La disposition renvoie à l'art. 963, al. 1 et 2, CO, qui s'applique ici par analogie. Il y a lieu de préciser que la société mère et l'entreprise qu'elle contrôle ne sont considérées comme une unité qu'en ce qui concerne les services de communication qu'elles offrent.

L'*al. 3* impose une obligation d'annonce aux fournisseurs dès lors qu'ils dépassent ou, à l'inverse, qu'ils n'atteignent plus les seuils fixés à l'al. 1, let. a et b. Le Service SCPT met à leur disposition des mécanismes appropriés à cet effet.

L'*al. 4* donne les moyens nécessaires au Service SCPT pour contrôler si, effectivement, un fournisseur n'atteint pas ou à l'inverse dépasse les valeurs selon l'al. 1 avant tout. Le Service SCPT a aussi besoin de données pour déterminer si un fournisseur doit être considéré comme étant un fournisseur de services de communication dérivés. Il peut se procurer à cet effet des documents utiles auprès d'autres autorités, par exemple fiscales.

Aux termes de l'*al. 5* enfin, les fournisseurs qui remplissent les conditions de l'al. 1 disposent de deux mois pour conserver les données nécessaires à la fourniture des renseignements et de douze pour garantir leur disponibilité à renseigner. Les délais commencent à courir à partir de la date de la décision du Service SCPT, qui soutient les fournisseurs dans l'accomplissement de leurs obligations en leur dispensant des conseils.

Art. 23 Recours à l'aide de tiers pour la fourniture de renseignements et l'exécution de surveillances

L'*art. 23* règle les conditions auxquelles les fournisseurs peuvent faire appel à des tiers pour les aider à exécuter un mandat. Afin d'éviter que le recours à une aide extérieure n'entraîne des retards ou une perte de qualité, voire une lacune dans la surveillance, les tiers sont soumis aux mêmes obligations que les fournisseurs. Au besoin, par exemple en cas de problème de transmission, le Service SCPT doit par ailleurs pouvoir prendre directement contact selon le cas avec le fournisseur ou le tiers mandaté par ce dernier.

Art. 24 Standardisation des types de renseignements et des types de surveillance

Cet article traite de la standardisation, sur les plans technique et administratif, des types de renseignements et de surveillance définis dans l'ordonnance.

On entend par standardisation d'un type de renseignement ou de surveillance selon l'*al. 1*, le fait pour le DFJP de définir, dans son ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT), les détails d'ordre technique et administratif relatifs au type de renseignement ou de surveillance question (pour des précisions sur les notions de type de renseignement et de type de surveillance, voir les commentaires respectivement de l'art. 26 et de l'art. 28). Deux conditions prévalent à une standardisation: premièrement, l'existence d'une norme internationale et, deuxièmement, sa faisabilité, c'est-à-dire le caractère proportionnel de sa réalisation.

Conformément à l'*al. 2* si ces deux conditions ne sont pas remplies pour un type de renseignement ou de surveillance au moment de l'entrée en vigueur de l'ordonnance, le DJP renonce dans un premier temps à une standardisation.

L'art. 31, al. 3, LSCPT dispose que le DFJP doit pouvoir déterminer lui-même quels sont les types de renseignements et de surveillance « usuels », c'est-à-dire ceux qui se prêtent le mieux à une standardisation. Il faut éviter que les différents types définis par le Conseil fédéral et standardisés par le DFJP soient strictement liés entre eux, de sorte que le DFJP dispose d'une latitude suffisante pour élargir, réduire ou déplacer,

de sa propre autorité, le périmètre des types de renseignements et de surveillance ayant fait l'objet d'une standardisation et que le Conseil fédéral ne doive pas réviser à chaque fois l'OSCPT.

Art. 25 Surveillances et renseignements spéciaux

Tous les types de renseignements et de surveillance courants sont énumérés aux art. 24 et 25. Les dispositions s'y rapportant figurent respectivement dans les sections 1 (art. 27) et 4 à 6 (art. 35 à 48), et 8 à 11 (art. 54 à 68) du chapitre 3.

Les renseignements et les surveillances qui ne sont pas mentionnés expressément dans l'ordonnance sont ce que l'on appelle des mesures spéciales. Exécutées par le Service SCPT lui-même ou par des personnes qu'il mandate à cette fin, ces mesures correspondent à la pratique actuelle selon les art. 17, al. 5, et 25, al. 5, OSCPT dans sa teneur du 31 octobre 2001[41]. Ces dispositions ont été insérées dans l'OSCPT lors de sa modification du 23 novembre 2011 (en vigueur depuis le 1er janvier 2012) pour réglementer séparément la compétence du Service SCPT d'ordonner l'exécution de mesures de surveillance qui ne figurent pas explicitement dans l'ordonnance mais qui ont été ordonnées par les autorités de poursuite pénale et autorisées par les tribunaux de mesures de contrainte. Conformément à l'arrêt du Tribunal administratif fédéral du 23 juin 2011 (A-8267/2010), les fournisseurs concernés ne peuvent pas s'opposer à ces mesures de surveillance et doivent tolérer leur mise en œuvre, en mettant à la disposition du Service SCPT les interfaces existantes.

L'obligation de tolérer une surveillance qui incombe aux fournisseurs inclut également l'accès à leurs installations (art. 51) et la mise à disposition, gratuitement, des accès existants vers les réseaux de télécommunication publics.

Art. 26 Types de renseignements en général

L'*al. 1* donne un bref aperçu des différents types de renseignements qu'il est possible de recueillir et qui sont réglés en détail aux sections 1 et 4 à 6 du chapitre 3 (art. 27 et 34 à 47). On entend par « type de renseignement » une forme de demande et de fourniture de renseignements définie de manière détaillée dans l'ordonnance et portant sur les données selon les art. 21 et 22 LSCPT concernant des services de télécommunication ou de services de communication dérivés.

Les types de renseignements sont désormais organisés conformément à la norme TS 102 657 de l'Institut européen des normes de télécommunication (ETSI) et répartis par catégorie de services. Cette répartition est prescrite par la norme ETSI. Comme les produits proposés par les fournisseurs peuvent englober plusieurs catégories de services (par ex. un abonnement de communication mobile avec les catégories de services « services d'accès au réseau » et « services de téléphonie et multimédia »), il faudrait en pratique soumettre une demande pour chaque type de renseignement, de manière à couvrir tous les services.

Les catégories de services faisant le plus fréquemment l'objet d'une demande de renseignements sont les *services d'accès au réseau* et les *services de téléphonie et multimédia*. Ces demandes sont subdivisées en deux types, à savoir les demandes concernant les « renseignements sur les usagers » (art. 35 et 40) et celles visant les

41 RS **780.11**

« renseignements sur les services » (art. 36 et 41). Cette subdivision, qui correspond en substance aux actuels renseignements « A0 » et « A1 », a pour fonction de limiter le volume d'informations par type de renseignement, mais aussi de faciliter et d'accélérer le traitement automatisé des demandes.

Cette subdivision n'est pas appliquée en revanche aux catégories de services moins fréquemment indiquées dans les demandes, c'est-à-dire les *services de courrier électronique* et les *autres services de télécommunication et services de communication dérivés*.

La catégorie *services d'accès au réseau* englobe trois autres types spécifiques de renseignements (art. 36 à 38) visant à identifier les auteurs d'infractions par Internet (art. 22 LSCPT).

Pour les types de renseignements visés aux art. 35, 40, 42 et 43, il est possible d'effectuer une recherche flexible de nom. Ce type de recherche est défini à l'art. 27.

L'*al. 2* dispose que les autorités ne peuvent demander des renseignements que les fournisseurs sont tenus de livrer sur la base des dispositions de l'OSCPT que conformément à la procédure prévue dans l'ordonnance. Concrètement cela signifie que les autorités transmettent leurs demandes de renseignements au Service SCPT – via le système de traitement ou, dans les cas visés à l'art. 17, al. 2, par courrier ou par fax, voire par téléphone – mais jamais directement aux personnes obligées de collaborer.

Art. 27 Types de renseignements avec recherche flexible de nom

Cet article recouvre quatre types de renseignements supplémentaires fondés sur les types de renseignements selon les art. 35 (IR_4_NA), 40 (IR_10_TEL), 42 (IR_13_EMAIL) et 43 (IR_15_COM) et se distinguant de ceux-ci uniquement par le type de recherche par nom:

- IR_5_NA_FLEX;
- IR_11_TEL_FLEX;
- IR_14_EMAIL_FLEX;
- IR_16_COM_FLEX.

La recherche par nom est le critère de recherche pour les renseignements selon l'al. 2, let. a, de l'article précédent. Il s'agit d'une recherche phonétique et tolérante à l'erreur, également appelée recherche flexible de nom. Comme l'interface ETSI pour les demandes de renseignements et les réponses à ces requêtes n'offre pas la possibilité de transmettre des instructions sur le type de recherche, ces quatre types de renseignements supplémentaires ont été définis.

Les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements exécuteront dorénavant de manière automatisée les demandes de renseignements fondées sur un nom. Ces recherches sont pour l'heure effectuées par les collaborateurs des FST, qui doivent palier, avec leur intelligence humaine, l'intelligence technique qui fait défaut. Pour garantir un niveau de résultats au moins équivalant à l'avenir et, dans le même temps, tenir compte des besoins des autorités de poursuite pénale, il doit être possible d'effectuer, en plus de la recherche exacte (types de base selon les art. 35, 40, 42 et 43), des recherches phonétiques, tolérantes à l'erreur.

Comme le montre la pratique, les erreurs sont fréquentes lors de la saisie de données personnelles:

1. inversion ou omission de parties de noms
2. fautes de frappe
3. différences dans la translittération de noms à partir d'un alphabet étranger dans l'alphabet latin. L'erreur peut déjà avoir été commise lors de l'établissement du document d'identité, mais bien souvent, c'est au moment de la saisie des données de l'usager ou de leur enregistrement dans la base clients qu'elle se produit. Il est fréquent en effet que les systèmes informatiques ne prennent pas en charge tous les signes diacritiques qui existent.
4. différences dans la transcription (par ex. anglais, français) de noms d'une écriture non latine dans une écriture latine.

Lors d'une recherche flexible de nom, il ne faut donc pas effectuer une comparaison exacte des chaînes de caractères: il faut, d'un côté, rechercher les correspondances phonétiques et, de l'autre, comparer les parties de nom (*name matching*), de manière à identifier, par exemple, les correspondances de parties de noms et leurs inversions. Les systèmes courants de gestion de banques de données contiennent des fonctions de recherche spécifiques pour la recherche flexible de nom. Voir le commentaire de l'art. 9, al. 3, OME-SCPT pour plus de précisions sur ce type de recherche.

Art. 28 Types de surveillance

Cet article donne un bref aperçu des différents types de surveillance, qui sont définis aux sections 8 à 11 du chapitre 3 (art. 54 à 68). On entend par « type de surveillance » une forme de surveillance définie de manière détaillée dans l'ordonnance et portant sur un ou plusieurs services de télécommunication ou services de communication dérivés (art. 31, al. 1, LSCPT). On distingue la surveillance en temps réel (al. 1) et la surveillance rétroactive (al. 2), ainsi que les recherches en cas d'urgence (al. 3) et les recherches de personnes condamnées (al. 4).

Les types de surveillance en temps réel sont à présent structurés de manière à permettre aux autorités de poursuite pénale de demander, pour les principales catégories de services, la livraison en temps réel des seules données secondaires de télécommunication ou, à l'inverse, des données secondaires et du contenu des communications (al. 1). Le but de cette distinction est de permettre une gradation de l'atteinte aux droits fondamentaux des intéressés.

Il n'est possible d'intercepter le contenu des télécommunications (par ex. conversations, courriels et pièces jointes) que dans le cadre d'une surveillance en temps réel. Lors de surveillances rétroactives en revanche (données secondaires de issues de la surveillance rétroactive ou, pour reprendre le terme précis, données secondaires de télécommunication conservées concernant des communications passées), le contenu des télécommunications n'est pas enregistré (pour des précisions sur la notion de *données secondaires*, voir le commentaire introductif de la section 10 du chapitre 3).

La nouvelle ordonnance définit des types de surveillance spécifiques pour les principales catégories de services, de manière à tenir compte du principe de précision et à satisfaire aux prescriptions découlant des normes internationales. Les catégories

de services sont subdivisées en services d'accès au réseau et en applications. Ces dernières englobent les services de téléphonie et multimédia, les services de courrier électronique et d'autres services de télécommunication et services de communication dérivés.

Dans la téléphonie traditionnelle, il n'y avait pas de distinction entre accès au réseau et application (raccordement téléphonique). Il suffisait donc en général de surveiller le raccordement. L'évolution de la technologie fait qu'il existe à présent un nombre toujours plus important de services de communication offrant des possibilités d'accès au réseau presque illimitées. Cibler la surveillance sur l'accès au réseau (raccordement) n'apporterait guère de résultats avec ce type de services, qui plus est dans les cas où le fournisseur ou les équipements terminaux, voire un logiciel, cryptent les communications. Les services nomades de téléphonie par Internet (VoIP) le montrent clairement: les données d'accès de l'usager peuvent être enregistrées dans une application sur le smartphone. L'usager peut naviguer sur Internet avec son smartphone via une multitude de points d'accès (par ex. dans un hôtel, au bureau, dans un aéroport) et utiliser les services de téléphonie par internet au moyen de l'application installée sur son équipement mobile. Comme les autorités de poursuite pénale ne peuvent pas savoir à l'avance quels accès à Internet l'usager surveillé va utiliser et vu la multitude d'accès entrant en ligne de compte (par ex. points d'accès au réseau WLAN), il est plus efficace d'effectuer la surveillance directement auprès du fournisseur de l'application (en l'occurrence, auprès du fournisseur du service de téléphonie par Internet). Cette solution permet de couvrir toutes les communications effectuées via le service de téléphonie par Internet surveillé, indépendamment de l'accès au réseau utilisé par la personne visée par la surveillance. Autre avantage, le fournisseur doit retirer tout cryptage qu'il aurait opéré, afin que les autorités de poursuite pénale puissent effectivement exploiter le contenu des communications interceptées.

Les produits proposés par les fournisseurs peuvent englober plusieurs catégories de services (par ex. abonnement de téléphonie avec la catégorie « accès au réseau » et la catégorie « services de téléphonie et multimédia »). Pour garantir une surveillance complète, plusieurs types de surveillance doivent parfois être ordonnés pour le même identifiant cible. Il ne faut pas non plus perdre de vue que certains produits de télécommunication peuvent comprendre des offres de services différentes, qui relèvent de types de surveillance différents. Lorsqu'il s'agit par exemple d'effectuer la surveillance complète en temps réel (contenu et données secondaires) d'un smartphone, l'autorité doit ordonner deux surveillances distinctes: la première, du type RT_23_NA_CC_IRI, pour l'accès Internet mobile; la seconde, du type RT_25_TEL_CC_IRI, pour le service de téléphonie mobile. Cette séparation obéit à des exigences de nature administrative et technique. Du point de vue administratif, les autorités habilitées doivent pouvoir continuer à ordonner la surveillance des différents services de télécommunication en fonction des besoins de l'enquête et indépendamment les uns des autres. En ce qui concerne l'aspect technique, la surveillance d'un accès Internet mobile est fondamentalement différente de la surveillance d'une application de communication mobile. L'instauration de deux types de surveillance permet ainsi de tenir compte des différences dans les processus d'activation et de mise en œuvre des surveillance auprès des personnes obligées de collaborer.

Section 2 Assurance de la qualité

Art. 29 Qualité des données transmises

Le bon déroulement d'une mesure de surveillance implique aussi, entre autres aspects, de garantir la qualité des données transmises. Cet article définit donc les exigences qui doivent être remplies pour que la qualité des données soit réputée préservée.

L'*al. 1* fixe trois conditions qui doivent être cumulativement remplies pour garantir la qualité des données transmises. Concernant la *let. b*, il y a lieu de signaler que seule la transmission des données issues de surveillances ou de renseignements doit s'effectuer sans perte de données et sans interruption. La qualité des données issues de la surveillance ne peut dès lors pas être supérieure à celle des services surveillés conformément aux prescriptions applicables. De la même manière, la qualité des renseignements livrés ne peut pas être supérieure à la qualité des données relatives aux usagers et des données secondaires de télécommunication saisies et enregistrées conformément aux prescriptions.

L'*al 2* règle les responsabilités quant à la garantie de la qualité et dispose concrètement que ce sont les personnes obligées de collaborer qui répondent, jusqu'au point de livraison, de la qualité des données issues de la surveillance et de renseignements (art. 12, al. 3, LSCPT). Des informations détaillées sur les points de livraison figurent à l'annexe 2 de l'OME-SCPT. Le Service SCPT apporte son soutien aux personnes obligées de collaborer en les conseillant. Même si elle a chargé un tiers d'exécuter la surveillance, la personne obligée de collaborer reste responsable de la qualité des données transmises.

L'*al. 3* prévoit que le Service SCPT et les personnes obligées de collaborer doivent s'informer mutuellement sans délai lorsqu'ils constatent un défaut de qualité des données transmises. Si le problème concerne des prestations fournies pendant le service de piquet (voir art. 11), il doit être immédiatement signalé par téléphone aux services compétents. On peut aussi imaginer que ce soit l'autorité de poursuite pénale qui constate un défaut de qualité. En pareil cas, l'autorité en avertit le Service SCPT, qui informe à son tour la personne obligée de collaborer concernée.

Tant le Service SCPT que les personnes obligées de collaborer effectuent un monitorage à des fins de contrôle de la qualité. Les détails sont réglés dans l'OME-SCPT. Sont des personnes obligées de collaborer tenues d'exécuter des surveillances les FST, hormis ceux qui ont des obligations restreintes en matière de surveillance visés à l'art. 51, et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52.

Lorsqu'un problème est détecté, les personnes obligées de collaborer et le Service SCPT procèdent sur-le-champ à une analyse et s'informent mutuellement et de manière exhaustive des résultats. Si le problème touche les systèmes de la personne obligée de collaborer, cette dernière transmet par écrit au Service SCPT une annonce formelle de dérangement indiquant le moment précis auquel le dérangement s'est produit, donnant une description du problème, récapitulant dans l'ordre chronologique les mesures engagées et précisant le statut du problème. L'annonce de dérangement doit être faite au plus tard le jour ouvré suivant la constatation du problème. La personne obligée de collaborer doit en outre communiquer le plus rapidement possible au Service SCPT la durée estimée du dérangement. Dans un souci d'exhaustivité, elle l'informe également des résultats des différentes clarifications menées à bien et lui transmet les données correspondantes. Ces données nécessaires pour étayer les

résultats des analyses; le Service SCPT peut aussi avoir besoin pour ses propres analyses. Après avoir entendu la personne obligée de collaborer, le Service SCPT détermine avec elle la gravité du problème (par ex. critique, grave, mineur). La personne obligée de collaborer lève le dérangement dans le délai fixé par le DFJP pour chaque degré de gravité. Elle informe le Service SCPT par écrit et régulièrement – c'est-à-dire conformément aux échéances prescrites par le DFJP – des nouvelles mesures qu'elle met en œuvre et de l'évolution du statut du problème. Sitôt le dérangement levé, la personne obligée de collaborer transmet par écrit au Service SCPT une confirmation de clôture du cas, qui complète les données de l'annonce de dérangement.

Les données secondaires issues de la surveillance en temps réel doivent être enregistrées conformément aux possibilités techniques prévues dans la spécification relative à l'interface et livrées sans délai une fois le problème réglé. Si ces données ne sont plus disponibles ou sont incomplètes, la personne obligée de collaborer livre sans délai, sur instruction du Service SCPT, les données secondaires issues de la surveillance rétroactive (voir l'art. 4, al. 3).

Art. 30 Branchements de test

Un *branchement de test* désigne la surveillance technique d'un service de télécommunication (par ex. téléphonie mobile, accès mobile à internet, compte de messagerie électronique) ou d'un service de communication dérivé (par ex. messagerie instantanée, service de chat) aux fins mentionnées à l'*al. 1*. Les appareils et les logiciels utilisés à cette fin sont désignés par le terme *équipement de test*. Il peut s'agir, par exemple, d'équipements terminaux, comme des smartphones, ou de simulateurs, c'est-à-dire des logiciels que l'organisation concernée emploie exclusivement à des fins de test. Dans un branchement de test, la cible de la surveillance est appelée *cible test*. Les données utilisées et générées à cette occasion (par ex. conversations téléphoniques, SMS, trafic Internet) sont des *données de test*. Ces données servent uniquement à remplir les buts visés à l'al. 1 et à garantir le caractère purement fictif de l'ensemble de la correspondance par télécommunication de tous les partenaires de communication intervenant dans le test. En outre, seules les personnes habilitées à utiliser des branchements de test auprès du Service SCPT, des personnes obligées de collaborer, des autorités de poursuite pénale et du SRC ont accès aux cibles, aux services et à l'équipement de test.

Comme elles ne sont utilisées que dans le cadre de branchements de test, les données de test ne relèvent pas du secret des télécommunications. La mise en place d'un branchement de ce type ne requiert dès lors pas l'autorisation de l'instance judiciaire compétente et les conditions de l'art. 269, al. 1, CPP ou de l'art. 70, al. 1, PPM ne doivent pas non plus être remplies. Vu en outre que dans les branchements de test effectués par le Service SCPT aucune autorité n'est associée à la procédure, le Service SCPT peut prendre connaissance des données issues de ses propres branchements de test sans devoir faire approuver au préalable la mesure par un juge (art. 18, al. 2, LSCPT).

Le Service SCPT établit des dossiers de surveillance distincts au sens de l'art. 9 pour les branchements de test. À la différence de la procédure prévue pour les surveillances ordinaires, seuls sont dans ce cas enregistrés les indications relatives à la personne responsable, son unité d'organisation (nom et adresse), le but dans lequel le branchement de test est utilisé et le nom des personnes habilitées à traiter les données recueillies. En revanche, comme pour les surveillances normales, le traitement des

données de tous les branchements de test utilisés est journalisé. Le Service SCPT gère une série de branchements de test qu'il met gratuitement à la disposition des autorités de poursuite pénale et du SRC pour la réalisation de tests et de formations. Aucuns frais ne sont non plus perçus pour les coûts d'utilisation, dans des limites raisonnables, des services de télécommunication ou des services de communication dérivés nécessaires. Le cas échéant, les utilisations extraordinaires générant des coûts élevés requièrent une concertation préalable avec le Service SCPT. En l'absence d'une telle convention, le Service SCPT se réserve de faire valoir des prétentions récursoires.

Le Service SCPT indique, sur le mandat de surveillance qu'il transmet à la personne obligée de collaborer, qu'il s'agit d'un branchement de test. Pour générer des données de test, il peut faire appel au besoin à des personnes obligées de collaborer; le cas échéant, il conçoit un programme de test après les avoir entendues (*al. 2*). Les personnes obligées de collaborer doivent quant à elles mettre gratuitement et aussi longtemps que nécessaire à la disposition du Service SCPT les services de télécommunication ou les services de communication dérivés qu'elles exploitent qui sont nécessaires à la réalisation des branchements de test (*al. 3*). Cela signifie que les frais de base, les frais d'activation, les frais récurrents et tous les frais de communication et d'utilisation liés à ces services sont à la charge des personnes obligées de collaborer. Ainsi, la personne obligée de collaborer fournit gratuitement au Service SCPT le nombre de cartes SIM dont il a besoin, active sans frais les services nécessaires et ne facture pas non plus les coûts liés à leur utilisation.

Il y a lieu de noter que l'utilisation des branchements de test doit se maintenir dans des proportions raisonnables. Comme indiqué précédemment, un accord préalable est indispensable entre le Service SCPT et les personnes obligées de collaborer pour toute utilisation sortant du cadre ordinaire et entraînant des coûts élevés.

Le Service SCPT acquiert les équipements non propriétaires – c'est-à-dire des équipements courants sur le marché – nécessaires. Si les services de télécommunication ou les services de communication dérivés d'une personne obligée de collaborer requièrent l'emploi de terminaux propriétaires, la personne obligée de collaborer doit aussi mettre ces appareils gratuitement à la disposition du Service SCPT.

L'*al. 4* autorise les autorités de poursuite pénale et le SRC à faire effectuer à leurs frais, en plus des branchements de test que le Service SCPT peut mettre gratuitement à leur disposition, des branchements de test pour garantir la qualité des télécommunications transmises ou à des fins de formation. On distingue donc deux types de branchements de test: ceux que le Service SCPT met gratuitement à disposition (al. 3) et ceux que les autorités de poursuite pénale et le SRC peuvent faire activer à leurs frais (al. 4). Pour pouvoir demander l'activation d'un branchement de test propre, les autorités de poursuite pénale ou le SRC doivent désigner un responsable et un suppléant, chargés de gérer les cibles, les services et les équipements de test et habilités à ordonner la mise en place d'un branchement de ce type. Les branchements de test sont activés aux frais de l'autorité qui les ordonne. Celle-ci doit donc prendre à sa charge les indemnités versées aux personnes obligées de collaborer pour l'exécution de la mesure et payer au Service SCPT les émoluments prévus. Le montant des émoluments et des indemnités est fixé dans l'OEI-SCPT. Les coûts correspondant aux services de télécommunication ou aux services de communication dérivés et les équipements terminaux sont aussi à la charge de l'autorité de poursuite pénale concernée ou du SRC. Les données recueillies lors de branchements de test peuvent être transmises aux autorités de poursuite pénale via le système de traitement

du Service SCPT ou au moyen d'un branchement direct. L'art. 18, al. 2, LSCPT s'applique par analogie aux branchements de test des autorités de poursuite pénale.

Les demandes de branchements de test émanant des autorités de poursuite pénale ou du SRC (branchements de test des autorités) suivent la procédure formelle prévue pour les surveillances ordinaires: l'autorité doit tout d'abord transmettre un ordre en ce sens au Service SCPT en précisant le type de surveillance ainsi que le but et la durée du branchement, la durée maximale étant fixée à douze mois. Le Service SCPT vérifie que la demande respecte les critères fixés et qu'elle a bien été soumise par une personne habilitée. Si c'est le cas, il transmet les mandats d'activation des branchements de test aux personnes obligées de collaborer concernées, en indiquant sur le mandat qu'il s'agit en l'occurrence d'un branchement de test d'une autorité. L'interlocuteur désigné par l'autorité peut, sur demande et contre paiement d'un émolument, faire prolonger le branchement de test pour une nouvelle période de douze mois au plus. Trois mois au plus tard avant la date de désactivation prévue, le Service SCPT envoie un rappel aux interlocuteurs habilités de l'autorité qui a sollicité le branchement de test. Si les conditions d'une prolongation sont remplies, le branchement de test reste activé. Dans le cas contraire, le Service SCPT met un terme à la mesure: il transmet pour ce faire le mandat correspondant à la personne obligée de collaborer concernée en la chargeant de désactiver le branchement de test à la date initialement fixée.

Section 3 Garantie de la disponibilité à renseigner et à surveiller

Art. 31 Contrôle de la disponibilité à renseigner et à surveiller

La disponibilité à renseigner désigne le fait, pour les personnes obligées de collaborer ci-après, d'être en mesure de livrer ou de faire livrer par des tiers les types de renseignements suivants concernant les services qu'elles offrent (cf. art. 18):

- FST et fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements visés à l'art. 22: renseignements selon les art. 35 à 37 et 40 à 48 et selon l'art. 27 en relation avec les art. 35, 40, 42 et 43;
- FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51, et fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52: renseignements selon les art. 38 et 39.

La disponibilité à surveiller désigne le fait, pour les personnes obligées de collaborer ci-après, d'être en mesure d'exécuter ou de faire exécuter par des tiers les types de surveillance suivants concernant les services qu'elles offrent (cf. art. 50):

- à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51, et fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52: surveillances selon les art. 54 à 68.

Afin de garantir leur disponibilité à renseigner et à surveiller, les fournisseurs mentionnés doivent désormais apporter la preuve qu'ils peuvent livrer les renseignements demandés et mettre en œuvre les surveillances ordonnées conformément au droit applicable (*al. 1*).

L'*al. 2* dispose que cette preuve est réputée apportée dès lors que les tests effectués selon les prescriptions du Service SCPT ont été concluants (let. a) et que le fournisseur confirme, au moyen d'un formulaire élaboré par le Service SCPT, qu'il remplit les exigences relatives aux renseignements et aux surveillances ayant fait l'objet d'une standardisation. Étant donné que les fournisseurs ont la possibilité de faire exécuter par des tiers leurs obligations en matière de fourniture de renseignements et de surveillance, ils peuvent aussi faire apporter la preuve de leur disponibilité à renseigner et à surveiller par ces mêmes tiers. La responsabilité proprement dite d'apporter la preuve incombe cependant dans tous les cas au fournisseur concerné.

Pour contrôler la disponibilité à renseigner et à surveiller, le Service SCPT accomplit les tâches décrites à l'*al. 3*. On notera à cet égard que les procès-verbaux visés à la *let. e* peuvent être utilisés comme moyen de preuve en cas de différend judiciaire ou fournir des indications de référence pour le prochain contrôle de la disponibilité à surveiller et à renseigner.

Les services offerts différant d'un fournisseur à l'autre, le Service SCPT établit, conformément à l'*al. 4*, une attestation individuelle qui confirme que le fournisseur est en mesure, pour des critères de validité déterminés, de transmettre les données conformément aux prescriptions fixées par le département. Parmi les critères de validité applicables figurent entre autres les indications relatives aux systèmes, aux services et aux types de surveillance testés, les protocoles de test et leurs annexes, ainsi que les interfaces. Les tests portent aussi bien sur les systèmes du Service SCPT (ADMF[42], LEMF[43]) que sur ceux des fournisseurs (ADMF, MF[44]/DF[45], IIF[46]). Lors du test d'un service, comme la téléphonie, on teste également la technologie sur laquelle repose le service en question (par ex. VoLTE). Les tests des types de surveillance concernent essentiellement les surveillances en temps réel (par ex. les types RT_24_TEL_IRI et RT_25_TEL_CC_IRI).

Art. 32 Durée de validité de l'attestation

Il importe de relever ici que les attestations délivrées jusque-là par le Service SCPT – dénommées « Statement of compliance » ou « Confirmation of compliance » – ne sont pas des attestations de la disponibilité à renseigner et à surveiller au sens de l'art. 33, al. 6, LSCPT.

Sitôt la preuve de la disponibilité à renseigner ou à surveiller apportée (voir commentaire de l'art. 31), le Service SCPT délivre une attestation à la personne obligée de collaborer. Aux termes de l'*al. 1*, l'attestation est valable trois ans. Cette durée est calculée à partir de la date de délivrance de l'attestation.

42 ADMinistration Function (cf. ETSI TS 101 671)
43 Law Enforcement Monitoring Facility (cf. ETSI TS 101 671)
44 Mediation Function (cf. ETSI TS 101 671)
45 Distribution Function (cf. ETSI TS 101 671)
46 Internal Interception Function (cf. ETSI TS 101 671)

L'*al. 2* permet au Service SCPT de prolonger, à l'issue de cette période initiale, la validité de l'attestation par nouvelle période de trois ans si la personne obligée de collaborer atteste qu'aucun changement susceptible d'affecter la transmission des données ou sa capacité à renseigner et à surveiller n'est intervenu entre-temps. La personne obligée de collaborer soumet une demande de prolongation au Service SCPT, accompagnée des justificatifs visés à l'al. 2.

L'*al. 3* impose une obligation de déclaration aux personnes obligées de collaborer. Celles-ci sont tenues d'avertir sans délai le Service SCPT si elles constatent qu'elles ne sont plus en mesure de garantir leur disponibilité à renseigner et à surveiller.

Art. 33 Procédure de contrôle

Cette disposition donne la compétence au DFJP de définir la procédure de réception des systèmes techniques et la procédure de contrôle de la disponibilité à renseigner et à surveiller (voir aussi l'art. 31, al. 3, LSCPT).

Art. 34 Annulation de l'attestation de la disponibilité à renseigner et à surveiller

Si un FST ou un fournisseur de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements ou de surveillance n'est plus en mesure de livrer les renseignements ou d'exécuter les surveillances concernant les services qu'il offre, le Service SCPT annule immédiatement l'attestation de la disponibilité à renseigner ou à surveiller qu'il avait délivrée. Si l'impossibilité de garantir la disponibilité à renseigner et à surveiller n'affecte que certains des services proposés par le fournisseur, l'annulation concernera uniquement le service et les types de renseignements ou de surveillance concernés. Le Service SCPT délivre alors une attestation distincte, valable pour les services pour lesquels la disponibilité à renseigner et à surveiller continue d'être garantie. Le cas échéant, un nouveau contrôle peut être ordonné avant la délivrance d'une nouvelle attestation, qui devra indiquer clairement les services auxquels elle se réfère. Si, par exemple, la disponibilité à renseigner est garantie pour certains services, mais pas la disponibilité à surveiller, l'attestation ou la déclaration d'annulation devra le mentionner expressément.

L'attestation peut être annulée dans trois cas de figure: si le fournisseur en fait lui-même la demande (*let. a*), si le fournisseur n'est pas en mesure, dans plusieurs cas, de garantir la transmission des données ou la disponibilité à renseigner ou à surveiller (*let. b*) ou si des déclarations confirmées par le fournisseur ne sont pas conformes à la vérité (*let. c*).

Section 4 Types de renseignements concernant des services d'accès au réseau

Art. 35 Type de renseignements IR_4_NA: renseignements sur des usagers de services d'accès au réseau

Cet article définit le type de renseignements standardisé concernant les usagers de services d'accès au réseau. Ce type de renseignements correspond pour l'essentiel aux

actuels renseignements A0 et, en partie, A1 (*al. 2, let. j et k*). La nouveauté réside dans le fait qu'il sera dorénavant possible de recueillir des renseignements supplémentaires, à savoir le numéro d'identification des entreprises (*al. 2, let. g*), l'identifiant de l'usager (*al. 2, let. h*) et l'identifiant du service (*al. 2, let. i*).

Le terme « services d'accès au réseau » désigne des services de télécommunication qui permettent d'accéder directement (par ex. raccordement Internet DSL) ou indirectement (par ex. réseau privé virtuel ou *virtual private network*, VPN) à des réseaux de télécommunication publics, comme Internet. Le VPN a ceci de particulier qu'un tunnel relie l'accès Internet direct du client VPN au fournisseur de VPN. Cela signifie que les clients VPN accèdent à Internet avec une adresse IP attribuée non pas par leur fournisseur d'accès direct à Internet, mais par le fournisseur de VPN. En d'autres termes, les accès Internet directs des clients VPN ont pour adresse source une adresse IP du fournisseur de VPN. L'adresse IP de l'accès Internet direct du client VPN est visible du seul fournisseur de VPN. C'est pourquoi les fournisseurs de VPN doivent aussi être en mesure de livrer des renseignements sur leurs usagers et leurs services.

Ce type de renseignements se fonde sur la norme ETSI TS 102 657. Il associe les informations générales sur les usagers (*generic subscriber information*) et les principales indications relatives aux services d'accès au réseau utilisés par l'usager. Il est possible de recueillir des indications spécifiques supplémentaires sur les services d'accès au réseau avec le type de renseignements IR_6_NA (*art. 36*).

Un exemple permet d'illustrer concrètement les dispositions de cet article: X utilise différents services proposés par le fournisseur Y, à savoir trois abonnements mobiles (avec téléphonie et Internet), dix cartes prépayées (téléphonie uniquement) et deux services d'accès à Internet via le réseau fixe. Les autorités de poursuite pénale, qui connaissent le nom et l'adresse de X, veulent savoir quels services proposés par le fournisseur Y cette personne utilise. Elles soumettent à cette fin des demandes portant sur les types de renseignements IR_4_NA (art. 35) et IR_10_TEL (art. 40). Le fournisseur Y leur transmet cinq résultats concernant le type de renseignements IR_4_NA (art. 35; ces résultats comptent comme cinq enregistrements au sens de l'art. 17, al. 4) et 13 résultats concernant le type de renseignements IR_10_TEL (art. 40; comptent également comme 13 enregistrements).

L'*al. 1* porte sur les indications relatives aux usagers de services d'accès au réseau qui doivent être livrées en réponse à la demande de renseignements; voir aussi à ce sujet l'art. 21, al. 1, LSCPT (renseignements sur les services de télécommunication) et l'art. 22, al. 2 et 4, LSCPT (renseignements visant à identifier les auteurs d'infractions par Internet).

La *let. a* prévoit la communication de l'identifiant de l'usager utilisé par le fournisseur (par ex. le numéro de client), pour autant que le fournisseur ait attribué un tel identifiant à son client.

Les indications relatives à la personne visées à la *let. b* sont expliquées en détail à l'*art. 20*.

Explication des indications visées sou la *let. c:*

- L'« identifiant du fournisseur » selon le *ch. 1* est un numéro de nature administrative que le Service SCPT attribue à chaque fournisseur pour l'identifier.

- L'« identifiant du service » selon le *ch. 2* renvoie au service de télécommunication ou au service de communication dérivé utilisé par l'usager. La désignation choisie (par ex. un numéro de téléphone, un nom d'utilisateur, un

raccordement à large bande, une adresse électronique) doit permettre une identification sans la moindre ambiguïté, au moins auprès du fournisseur.

- Le *début* de la « période d'utilisation du service » selon le *ch. 3* désigne le moment (date et heure) où débute la relation commerciale, l'activation proprement dite du service pouvant, dans certaines circonstances, intervenir plus tard. Il peut en effet arriver qu'une personne achète une carte SIM un jour donné mais qu'elle ne l'active qu'après plusieurs jours. Les données personnelles du client sont saisies le jour de l'achat. Il faut entendre par activation le moment à partir duquel le service peut être utilisé par l'usager. Le cas échéant, il y a lieu de livrer aussi la date d'activation.

Remarque: l'expression « le cas échéant » (*if applicable*) signifie, aux termes de l'OSCPT, que la réglementation ne s'applique qu'au cas de figure correspondant au critère dont il est question. Par exemple, un numéro SIM (ICCID) ne peut être livré que s'il s'agit d'un service de communication mobile. Cela étant, il peut arriver, dans une configuration spéciale, que le numéro SIM ne soit pas disponible alors que l'on est bien en présence d'un service de communication mobile.

La *date de fin* correspond au moment à partir duquel le service n'est durablement plus utilisable par l'usager. Un blocage temporaire du service n'entre pas dans cette définition. La précision « éventuellement » signifie qu'une *date de fin* ne doit être fournie que si l'usager ne peut plus de façon durable utiliser le service d'accès au réseau.

- Selon le *ch. 4,* il est possible de transmettre également des indications sur des options ou des restrictions du service. Ces indications sont facultatives et doivent être transmises sous une forme lisible par l'homme, par exemple « adresse IP statique » ou « volume de données max. 1 GB » (voir norme ETSI TS 102 657, tableau E.2).

- Les données de localisation de l'accès au réseau selon le *ch. 5* correspondent à l'adresse d'installation de l'accès telle que consignée par le fournisseur pour cet usager.

- Concernant les statuts du service selon le *ch. 6*, les fournisseurs peuvent utiliser leurs désignations usuelles. Une standardisation des appellations nécessiterait trop de travail. La « période de validité » désigne la durée (date de début et, éventuellement, de fin) pendant laquelle le statut est ou était valable.

- Le *ch. 7* prévoit la communication, le cas échéant, de toutes les adresses IP statiques, préfixes IP, plages d'adresses IP et masques de réseau ou longueurs de préfixe attribués en lien avec le servie et leur période de validité respective.

- Selon le *ch. 8*, dans le cas de services de télécommunication gratuits ou à prépaiement il y a lieu de préciser aussi, conformément à l'art. 21, al. 1, let. e, LSCPT et à l'*art. 20*, *al. 1*, le lieu de remise du moyen permettant l'accès au service et le nom de la personne qui s'en est chargée.

- Le *ch. 9* dispose que le fournisseur doit livrer, le cas échéant, tous les numéros de cartes SIM enregistrées dans sa base de données clients en lien avec le service, sans oublier la date d'activation et, éventuellement, de désactivation de chaque carte.

- Conformément au *ch. 10*, il y a lieu de communiquer également l'IMSI (*international mobile subscriber identity*), c'est-à-dire le numéro d'identification international d'un usager dans un réseau de communication mobile.

- Le *ch. 11* prévoit l'indication, pour les services de communication mobile, du type de service, à savoir un service à prépaiement (*prepaid*) ou un abonnement (*postpaid*).

- Enfin, aux termes du *ch. 12*, le fournisseur doit aussi livrer, le cas échéant, l'identifiant alternatif de l'usager. Cette information n'est requise que s'il existe, pour ce service d'accès au réseau, un identifiant d'usager supplémentaire, différent de l'identifiant selon la let. a.

L'*al. 2* énumère les critères de recherche que les autorités de poursuite pénale indiquent dans les demandes qu'elles adressent, via le système de renseignements du Service SCPT, aux fournisseurs. La demande de renseignements doit contenir au moins un critère de recherche. Pour les critères selon les *let. a* à *d*, il importe de préciser un deuxième critère de recherche (*let. a* à *k*) afin de circonscrire la requête. Les critères de recherche selon les *let. e* à *k* sont quant à eux suffisamment précis et peuvent être utilisés **seuls**. Pour les recherches de chaînes de caractères (*let. a, c, d et e*), le fournisseur doit effectuer une recherche exacte au sens de l'art. 13, al. 1, OME-SCPT. Cette recherche correspond sur le principe à la recherche exacte à 100 %, à ceci près que la chaîne de caractères recherchée et la chaîne de caractères qui sert de référence pour la comparaison doivent d'abord être normalisée selon une série de règles: un des principes de base consiste à replacer les lettres qui ne font pas partie des 26 lettres de l'alphabet latin par une ou deux lettres latines. Dans la pratique, une recherche exacte à 100 % ne mènerait souvent pas aux résultats souhaités, parce que différents jeux de caractères utilisés ne permettent pas de représenter tous les signes. Sans compter que des fautes sont également souvent commises concernant les signes typographiques figurant dans les noms

La *let. a* permet de combiner librement les nom et prénom en un seul critère de recherche. Il peut arriver que le prénom et le nom de l'usager aient été intervertis au moment de la saisie des données. Parfois, il n'est pas facile de distinguer le nom du prénom (par ex. Laurent Martin), sans compter que les usagers peuvent avoir plusieurs prénoms ou plusieurs noms (par ex. Mónica Núñez Gómez).

Les bâtiments n'étant pas tous pourvus d'un numéro, la portée de la disposition de la *let. d* est atténuée avec l'insertion d'un *éventuellement*.

La *let. i* exclut l'utilisation d'adresses IP comme critère de recherche. Des types de renseignements spécifiques sont effet prévus à cette fin, à savoir le type IR_7_IP (*art. 37*), le type IR_8_IP (traduction d'adresses de réseau; art. 38) et le type IR_5_NAT (art. 38); voir le commentaire des art. 37, 38 et 39.

Art. 36 Type de renseignements IR_6_NA: renseignements sur des services d'accès au réseau

Cet article définit le type de renseignements standardisé concernant les services d'accès au réseau. Ce type de renseignements se fonde sur la norme ETSI TS 102 657. Le but de cette disposition est de recueillir d'autres données au sens de l'art. 21, al. 1, let. d, LSCPT.

L'*al. 1* précise quelles indications doivent être livrées en réponse à la demande de renseignements, tandis que l'*al. 2* énumère les critères de recherche.

L'*al. 1, let. d*, dispose qu'il convient de fournir la liste des identifiants des équipements **effectivement utilisés** pendant la période couverte par la requête. Le

fournisseur doit récupérer ces informations dans les données secondaires de télécommunication qu'il a enregistrées, sans toutefois communiquer les données secondaires elles-mêmes (pour des précisions sur la notion de *données secondaires*, voir le commentaire introductif de la section 10 du chapitre 3), pour autant bien sûr qu'il soit soumis à des obligations en matière de surveillance. Les fournisseurs qui n'ont pas de telles obligations transmettent uniquement les données dont ils disposent. Dans tous les cas, il ne doit pas être possible de déterminer, à partir de la réponse, la date, les modalités et le lieu d'utilisation de l'équipement en question.

La période de validité indiquée dans la réponse se réfère aux trois paramètres selon la let. b (identifiant du service), la let. c (IMSI et MSISDN) et la let. e (numéro SIM) du premier alinéa, mais ne concerne pas l'identifiant de l'équipement terminal. Si un de ces trois paramètres change pendant la période commune indiquée, la personne obligée de collaborer doit livrer plusieurs enregistrements correspondant au statut des informations. Étant donné que les codes PUK sont liés à la carte SIM, il n'est pas nécessaire de préciser de période de validité pour les paramètres selon l'al. 1, let. f (codes PUK). Leur validité découle directement de la validité des numéros SIM (*al. 1, let. e*).

Art. 37 Type de renseignements IR_7_IP: identification des usagers dans le cas d'adresses IP attribuées de manière univoque

Cet article définit le type de renseignements standardisé visant l'identification d'usagers dans le cas d'adresses IP attribuées de manière univoque. Ce type de renseignements se fonde sur la norme ETSI TS 102 657 et correspond aux actuels types A0.1 (adresse IP statique) et A0.2 (adresse IP dynamique). Cette requête permet de recueillir les indications visées à l'art. 22, al. 2, LSCPT. Comme il n'est pas possible de dire a priori si une adresse IP est ou a été attribuée de statique ou dynamique, toutes les demandes sont ici uniformisées en fonction d'adresses IP statiques et d'adresses IP dynamiques attribuées de manière univoque. À côté de ces deux types d'adresses IP, il existe aussi des adresses IP qui ne sont pas attribuées de manière univoque (voir art. 38 et 39).

L'expression *adresses IP attribuées de manière univoque* signifie qu'à un moment précis, un seul usager accédait à Internet avec l'adresse IP en question. Il peut s'agir soit d'une adresse IP statique, soit d'une adresse IP dynamique attribuée individuellement. Seule la fourniture de ce type de renseignements permet de déterminer si l'adresse IP est ou était attribuée de manière univoque.

Il est capital d'indiquer dans la demande une heure suffisamment précise. La période d'attribution étant très courte dans le cas d'adresses IP dynamiques attribuées de manière univoque, la recherche peut aboutir à des faux-positifs. L'autorité doit veiller en particulier à inscrire le bon fuseau horaire dans le cas d'indications se référant à l'étranger. Il convient également de prévoir un intervalle de tolérance, afin de tenir compte d'éventuelles imprécisions des horloges des systèmes. En lieu et place d'un moment fixe (*al. 2, let. b*), il est donc possible d'indiquer un laps de temps dans la demande de renseignements.

Si une demande de renseignements du type IR_7_IP livre plusieurs résultats, deux explications sont possibles:

1) soit l'intervalle indiqué est trop long et l'adresse IP en question a été attribuée à plusieurs usagers pendant ce laps de temps,

2) soit l'adresse IP sur laquelle se fonde la demande n'était pas attribuée de manière univoque.

L'autorité habilitée doit clarifier la situation avec le fournisseur.

Dans le premier cas, l'autorité soumet une nouvelle demande de renseignements du type IR_7_IP, en indiquant un intervalle plus court.

Dans le second, elle doit aussi soumettre une nouvelle demande, mais cette fois du type IR_8_IP (traduction d'adresses de réseau), en veillant à préciser d'autres critères de recherche (voir commentaire de l'art. 38).

Si, à l'inverse, une demande de renseignements du type IR_4_IP ne livre aucun résultat, il se peut que l'intervalle indiqué soit trop court ou que l'indication temporelle ne soit pas suffisamment précise, par exemple en raison d'une erreur de calcul du changement de fuseaux horaires.

Art. 38 Type de renseignements IR_8_IP (NAT): identification des usagers dans le cas d'adresses IP qui ne sont pas attribuées de manière univoque (traduction d'adresses de réseau)

Ce type de renseignements est nouveau et traite le problème spécifique de l'identification des usagers auxquels une adresse IP n'a pas été attribuée de manière univoque. Il se fonde sur la norme ETSI TS 102 657. La procédure de traduction d'adresses de réseau (*network address translation*, NAT) peut permettre à plusieurs milliers d'utilisateurs de se partager une même adresse IP publique. En pareil cas, l'identification d'un usager n'est possible qu'au prix d'un travail considérable sur le plan technique.

Dans la procédure de traduction d'adresses de réseau au niveau du fourniseur, ou *carrier-grade NAT* (cgNAT), les usagers du réseau exploité par le fournisseur d'accès se voient attribuer une adresse IP privée, valable uniquement dans ce réseau. Lorsque ces usagers accèdent à Internet, leurs adresses IP privées sont converties, c'est-à-dire traduites, à l'extrémité du réseau du fournisseur d'accès, en une adresse IP source publique commune (un grand nombre d'utilisateurs se partagent simultanément une adresse IP publique). Les nombreuses connexions Internet sont distinguées par des numéros de port. Cette procédure de traduction des adresses doit être effectuée pour chaque paquet IP entrant et sortant. On distingue deux types de procédures de traduction, une procédure déterministe et une procédure non déterministe. Dans une procédure non déterministe, l'équipement utilisé pour la traduction, à savoir un routeur, stocke dans une table d'attribution, pour chaque connexion Internet (contexte), le timbre horodateur, la source et la destination de la liaison (adresses IP et numéros de port), l'adresse IP privée correspondante et le numéro de port de l'usager, ainsi que le type de protocole de transport. Dans une procédure déterministe en revanche, les adresses et les numéros de port son traduits au moyen d'un algorithme qui permet de recalculer par la suite l'adresse et le numéro de port initiaux. Le fournisseur d'accès n'a par conséquent pas besoin de sauvegarder les adresses IP et les numéros de port de destination de chaque liaison pour identifier les usagers. Pour des raisons tenant au droit de la protection des données, il y a lieu de mettre en place des procédures dans lesquelles il n'est pas nécessaire d'enregistrer la destination des liaisons.

La traduction d'adresses de réseau est utilisée depuis longtemps déjà pour les accès mobiles à Internet (par ex. GPRS, UMTS, LTE), en raison principalement de la pénurie d'adresses IPv4 publiques, mais aussi pour des considérations de sécurité, car

la procédure masque la structure du réseau vis-à-vis de l'extérieur (*topology hiding*). Comme il ne reste aujourd'hui guère plus d'adresses IPv4 publiques disponibles, les fournisseurs d'accès utilisent toujours plus fréquemment le cgNAT aussi pour les accès fixes à Internet.

À la différence des adresses IPv4, les adresses IPv6 sont disponibles en nombre suffisant. Il faut donc s'attendre à ce que la procédure cgNAT perde de son importance à terme. Mais pour l'heure, on observe plutôt une utilisation accrue, sous l'effet également de la forte croissance du trafic mobile de données (smartphones, tablettes, notamment).

L'*al. 1* définit quelles indications doivent être livrées en cas d'identification concluante. Aucun résultat n'est livré si l'identification n'a pas été concluante. Si l'identification aboutit à plusieurs concordances, il y a lieu de livrer tous les enregistrements trouvés, pour autant que leur nombre ne dépasse pas la valeur maximale fixée dans la demande. Si cette valeur est dépassée, on indiquera seulement le nombre de résultats (art. 18, al. 6).

L'*al. 2* précise quelles indications doivent figurer sur la demande de renseignements:

- l'adresse IP publique source (*let. a*), c'est-à-dire l'adresse IP commune visible dans l'Internet en tant qu'IP d'origine;
- si nécessaire pour l'identification, c'est-à-dire dans le cas d'une procédure de traduction d'adresses de réseau, le numéro de port source public (let. b) visible dans l'Internet en tant que port d'origine;

  Remarque: l'adresse IP privée source et le numéro de port correspondant (IP/port privé) ne sont connus que du fournisseur d'accès.
- si nécessaire pour l'identification, c'est-à-dire dans le cas d'une procédure de traduction d'adresses de réseau non déterministe, l'adresse IP publique et le numéro de port de destination de la liaison (par ex. un serveur Web), ainsi que le type de protocole de transport, par ex. TCP, UDP (*let. c, d et e*);
- le moment de la traduction, indiqué sous la forme d'une date et d'une heure (*let. f*). Il est possible d'indiquer dans la demande un intervalle de temps au lieu d'un moment fixe afin, notamment, de compenser des imprécisions éventuelles des horloges des systèmes. L'indication temporelle doit être suffisamment précise et l'intervalle le plus court possible de manière à éviter les faux-positifs (voir commentaire de l'art. 37)

Les étapes du traitement de la demande de renseignements peuvent être résumées comme suit:

- étape 1 (relève des activités préparatoires et ne fait pas partie à proprement parler de ce type de renseignements): obtenir, auprès de l'exploitant du service Internet (côté serveur), l'historique IP du compte utilisateur recherché, de manière à pouvoir déterminer les détails de la liaison relative aux événements de connexion concernés.

- étape 2: la demande de renseignements est transmise au fournisseur d'accès à Internet (indication des détails de la liaison d'un événement de connexion concret déterminé à l'étape 1) afin d'identifier les usagers.

- étape 3 (ne fait pas partie à proprement parler de ce type de renseignements): la demande de renseignements est transmise au fournisseur d'accès à Internet (indication des identifiants de l'usager ou du service trouvés à l'étape 2) afin de consulter les données personnelles de l'usager.

Précisions concernant l'étape 1: cette étape consiste à consulter l'historique IP d'un compte utilisateur déterminé côté serveur, c'est-à-dire à la destination de la liaison (par ex. exploitant d'un blog, service de courriel Web ou réseau social).

L'autorité de poursuite pénale reçoit en retour un procès-verbal de connexion contenant toutes les indications permettant de déterminer les accès Internet utilisés pour accéder au compte utilisateur recherché: la source de la connexion (adresse IP et port), le serveur de destination de la liaison (adresse IP et port), le timbre horodateur et le type de protocole. Il est ensuite possible, avec ces données, d'identifier les usagers à la deuxième étape.

Précisions concernant l'étape 2: pour illustrer cette deuxième étape, il peut être utile d'expliquer le déroulement d'une recherche portant, par exemple, sur un accès mobile à Internet. Se fondant sur les indications 3 à 6 figurant sur la demande de renseignements, le fournisseur d'accès commence par rechercher l'adresse IP privée et le numéro de port correspondant (qui étaient attribués à l'usager recherché au moment indiqué, c'est-à-dire l'adresse IP source [IP / port privé]) dans les données relatives à la traduction d'adresses de réseau qu'il a enregistrées. L'adresse IP privée, le numéro de port et le timbre horodateur sont utilisés pour rechercher le numéro MSISDN ou le numéro IMSI de l'usager. Le fournisseur d'accès livre ensuite l'identifiant de l'usager ou du service (par ex. MSISDN, IMSI) comme résultat de la demande portant sur ce type de renseignements.

Précisions concernant l'étape 3: l'autorité de poursuite pénale transmet à ce stade une dernière demande de renseignements (type IR_4_NA) afin de consulter, sur la base de l'identifiant de l'usager ou du service trouvé à l'étape 2 (par ex. MSISDN, IMSI), les données personnelles de l'usager.

Des requêtes analogues sont aussi possibles avec d'autres technologies, par exemple Dual-Stack Lite (DS Lite).

Une structure de données standardisée applicable aux données relatives à la traduction d'adresses de réseau a été introduite dans la version V1.14.1 de la norme ETSI TS 102 657, publiée en mars 2014 (voir l'annexe E.3 « ASN.1 definitions for network access services »).

La sauvegarde et la consultation de données relatives à la traduction d'adresses de réseau représentent un défi technique en ce sens que le fournisseur doit enregistrer des volumes de données considérables et garantir l'efficacité des recherches. Les nombreuses connexions IP qui transitent simultanément par le routeur (qui sert à la traduction des adresses de réseau) sont distinguées au moyen des paramètres décrits ci-dessus. En règle générale, un seul usager utilise simultanément des dizaines voire des centaines de liaisons IP. Les numéros de port source et les numéros de port traduits sont libérés et réattribués de manière cyclique. Sur les smartphones par exemple, la liaison Internet est interrompue en cas d'inactivité prolongée, afin d'économiser la batterie. Si la liaison Internet est rétablie, une nouvelle adresse IP (privée) est attribuée à l'appareil. Il s'agit d'un processus extrêmement dynamique, qui produit d'importantes quantités de données. On estime qu'un milliard environ de procédures de traduction d'adresses de réseau sont générées aujourd'hui quotidiennement sur les principaux réseaux mobiles de Suisse.

Les autorités de poursuite pénale doivent avoir conscience de ce que les demandes portant sur ce type de renseignements peuvent parfois n'aboutir à aucun résultat ou aboutir à des résultats ambigus, en particulier si tous les paramètres requis ne sont pas indiqués dans la demande. Il est possible d'accroître la précision des résultats par

exemple en combinant plusieurs demandes. L'enregistrement, par le fournisseur, des données relatives à la traduction d'adresses de réseau ne suffit toutefois pas à lui seul à régler le problème de l'identification des usagers d'Internet. Bien souvent, les serveurs de destination n'enregistrent ni numéros de port source, ni timbre horodateur exact. Or vu que la traduction d'adresses est un processus extrêmement dynamique, il est important de disposer d'indications le plus complètes et le plus précises possibles, de manière à éviter les faux-positifs.

Les ressources d'adressage étant attribuées de façon dynamique, il y a lieu, pour ce type de renseignements, de rechercher dans les données secondaires conservées à qui la ressource d'adressage concernée était attribuée au moment indiqué. Cette recherche doit s'effectuer idéalement en plusieurs étapes, en suivant les indices connus jusqu'à l'origine ou, à l'inverse, jusqu'à la destination de la liaison. Il ne s'agit cependant pas d'une surveillance rétroactive, puisque la liaison faisant l'objet de la recherche est connue et seule doit être identifiée son origine ou sa destination. On relèvera que les fournisseurs d'accès ne doivent conserver que pendant six mois les données relatives à l'attribution dynamique d'adresses IP et, si ces informations sont nécessaires pour l'identification des usagers, les données relatives à la procédure de traduction d'adresses IP et aux numéros de port (art. 21, al. 2, 2e phrase, art. 22, al. 2, 2e phrase, et al. 4, LSCPT et art. 21, al. 2). Les FST ayant des obligations restreintes en matière de surveillance visés à l'art. 51 sont exonérés de l'obligation de conserver les données secondaires de télécommunication (voir aussi le commentaire de l'art. 18, al. 4).

Art. 39 Type de renseignements IR_9_NAT: renseignements sur des procédures de traduction d'adresses de réseau

Ce type de renseignements est nouveau et a pour objet l'identification d'usagers dans le cadre d'enquêtes sur des infractions commises par Internet, conformément à l'art. 22 LSCPT. Il se fonde sur la norme ETSI TS 102 657.

Remarque: dans un souci de simplification, le terme traduction est employé seul dans les passages qui suivent pour désigner le processus de traduction d'adresses de réseau.

Deux types de recherches sont ici possibles: la première vise les renseignements *avant* la traduction, la seconde les renseignements *après* l'opération (les termes « avant » et « après » ont ici un sens temporel et doivent être compris du point de vue de la personne obligée de collaborer sollicitée).

- Première possibilité de recherche:

  Les indications **après** la traduction sont connues (par ex. adresse IP publique source et numéro de port); ce sont donc les indications **avant** la traduction (par ex. adresse IP) que l'on recherche.
  Par analogie avec l'*art. 38, al. 2*, la demande de renseignements sur des processus de traduction d'adresses de réseau doit comporter les indications suivantes (*al. 2*):

  - l'adresse IP source et le numéro de port après la traduction (*let. a et b*), par exemple l'adresse IP publique commune utilisée et le numéro de port, visibles dans l'Internet en tant qu'IP/port source;
  - le type de protocole de transport, par exemple TCP (*let. e*);
  - la date et l'heure de la traduction (*let. f*);

- si nécessaire aux fins de l'identification (cela dépend du processus de traduction utilisé), l'adresse IP publique et le numéro de port (*let. c et d*) de la destination de la liaison.

- Deuxième possibilité de recherche:

  Dans cette configuration, ce sont les données **avant** la traduction qui sont connues (par ex. adresse IP privée); la recherche doit donc permettre d'obtenir les données **après** le processus (par ex. adresse IP publique source).
  Par analogie avec l'*art. 36, al. 2*, la demande de renseignements sur des processus de traduction d'adresses de réseau doit comporter les indications suivantes (*al. 2*):

  - l'adresse IP source et le numéro de port avant la traduction (*let. a et b*), par exemple l'adresse IP privée du fournisseur d'accès à Internet et le numéro de port;
  - le type de protocole de transport, par exemple TCP (*let. e*);
  - la date et l'heure de la traduction (*let. f*);
  - si nécessaire aux fins de l'identification (dépend de la procédure de traduction utilisée), l'adresse IP publique et le numéro de port (*let. c et d*) de la destination de la liaison.

Exemple de recherche selon la première possibilité: lorsqu'une demande portant sur le type de renseignements IR_8_IP (NAT) selon l'*art. 38* est infructueuse, il faut sans doute remonter plus loin pour retracer l'adresse IP source et identifier les usagers. On recourt pour ce faire à la méthode dite de retour en arrière (ou « backtracking »). Celle-ci ne peut être appliquée que si chacune des personnes obligées de collaborer concernées a enregistré de manière précise et exhaustive toutes les informations relatives aux procédures de traduction nécessaires aux fins de l'identification. Les informations qui doivent être enregistrées dépendent de la procédure de traduction employée. En ce qui concerne le retour en arrière, une procédure à plusieurs niveaux (de traduction à traduction) est aussi possible: dans ce modèle, la demande est envoyée à toutes les personnes obligées de collaborer qui ont effectué une traduction pour la liaison Internet recherchée.

Exemple de recherche selon la deuxième possibilité: la surveillance en temps réel d'un accès au réseau révèle que la personne surveillée utilise un certain service de communication dérivé. Les données sont transmises de manière chiffrée, si bien qu'il n'est pas possible de voir l'identifiant d'usager du service de communication dérivée lors de la surveillance. L'autorité de poursuite pénale souhaite donc connaître cet identifiant. En raison de la traduction effectuée par le fournisseur d'accès, l'adresse IP source (publique) visible auprès du fournisseur du service de communication dérivé est différente de l'adresse IP (privée) attribuée à la personne surveillée et que l'autorité de poursuite pénale connaît grâce aux données secondaires issues de la surveillance en temps réel. Pour pouvoir identifier l'accès incriminé auprès du fournisseur de services de communication dérivés, il est possible de rechercher, auprès du fournisseur d'accès, l'adresse IP source et le numéro de port source souhaités, en veillant à préciser dans la demande toutes les données connues concernant la liaison IP.

Section 5 Types de renseignements concernant des applications

Art. 40 Type de renseignements IR_10_TEL: renseignements sur des usagers de services de téléphonie et multimédia

Cet article définit le type de renseignements standardisé concernant les usagers de services de téléphonie et multimédia. Ce type de renseignements correspond sur le principe au type A0 et, en partie, au type A1 (al. 2, let. j et k) actuels. La nouveauté est qu'il sera dorénavant possible d'effectuer des recherches sur la base du numéro d'identification des entreprises (al. 2, let. g), de l'identifiant de l'usager (al. 2, let. h) et des identifiants (al. 2, let. i).

L'appellation « services de téléphonie et multimédia » regroupe, en particulier, les services téléphoniques analogiques et numériques classiques sur le réseau fixe (par ex. raccordement fixe analogique, ISDN), les services téléphoniques mobiles, y compris les SMS et la messagerie vocale (par ex. GSM, UMTS), la téléphonie par Internet (par ex. VoIP), les services téléphoniques multimédia relevant de la norme IP Multimedia Subsystem (IMS; par ex. VoLTE, VoWLAN, Presence, RCS), la visiophonie et les conférences téléphoniques.

Fondé sur la norme ETSI TS 102 657, ce type de renseignements associe les informations générales sur les usagers (*generic subscriber info*) aux principales indications sur les services de téléphonie et multimédia utilisés par la personne. Le type de renseignements IR_12_TEL (art. 41) permet de recueillir des indications spécifiques supplémentaires sur cette catégorie de services.

Ce type de renseignements s'applique aussi bien aux services sur abonnement ou à prépaiement qu'aux offres gratuites. Il est structuré de la même manière que l'art. 35. Le commentaire de l'art. 35 vaut donc aussi pour cet article.

L'*al. 1* définit, sur le modèle de l'art. 35, al. 1, les indications à livrer en réponse à une demande de renseignements portant sur des usagers de services de téléphonie et multimédia. Les indications sur le type de service (*ch. 4*) servent à circonscrire plus précisément le service. Concernant les adresses des installations des accès fixes au réseau et leur période de validité respective (*ch. 5*), les données qui doivent être livrées sont celles qui sont enregistrées chez le fournisseur, pour autant qu'il s'agisse d'un service téléphonique ou multimédia du réseau fixe. Comme l'emplacement peut changer pendant la durée de la relation commerciale, tout l'historique doit être livré, avec, le cas échéant, la date de début et de fin pour chacun des emplacements. Il n'est toutefois pas possible de garantir que ces indications concordent toujours avec l'emplacement effectif de l'accès. Pour bon nombre de services en effet, l'usager peut utiliser les dispositifs d'accès à partir d'un autre emplacement, sans que le fournisseur en ait connaissance.

Le fournisseur doit aussi livrer, le cas échéant, la liste ou la plage des autres ressources d'adressage enregistrées en lien avec le service (*ch. 7*), ainsi que les indications relatives à d'éventuelles présélections pour les liaisons (*ch. 9*), c'est-à-dire un code de sélection du fournisseur (*carrier selection code*), qui peut être activé automatiquement (présélection). L'ordonnance du 17 novembre 1997 de la Commission fédérale de la communication relative à la loi fédérale sur les télécommunications[47] arrête à son art. 9, al. 1, que les fournisseurs de services téléphoniques publics sur réseau fixe

47 RS **784.101.112**

doivent offrir à leurs abonnés la possibilité de choisir, aussi bien de manière prédéterminée qu'appel par appel, un fournisseur pour leurs communications nationales et internationales. Si le code présélectionné du fournisseur de communications nationales et internationales est connu, le fournisseur de services téléphoniques publics sur réseau fixe doit également fournir cette information.

L'*al. 2* énumère, sur le modèle de l'art. 35, al. 2, les critères de recherche pour ce type de renseignements et détaille la manière dont ces critères doivent être utilisés (voir le commentaire de l'art. 35, al. 2). Pour les recherches de chaînes de caractères (*let. a, c, d et f*), le fournisseur doit effectuer une recherche dite exacte au sens de l'art. 13, al. 1, OME-SCPT (voir le commentaire de l'art. 35, al. 2).

Une distinction est faite entre les critères de recherche selon les let. h, j et k et les critères selon la let. i. Les critères selon les let. h, j et k ont pour fonction d'identifier sans ambiguïté des services de téléphonie et multimédia déterminés. À la différence des critères selon la let. i, ils ne remplissent pas de fonction d'adressage lors de l'établissement de la communication. Les identifiants tels que les numéros IMSI ou IMPI servent à identifier les usagers vis-à-vis du réseau. Les fournisseurs traitent ces données de manière strictement confidentielle.

L'ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications[48] autorise, à son art. 23, tout titulaire d'un bloc de numéros à attribuer à son tour à d'autres fournisseurs des numéros de bloc (attribution subséquente de numéros de téléphone). Or le fournisseur qui a procédé à une telle réattribution ne dispose généralement pas de données actuelles sur les usagers. En pareil cas, il signalera dans sa réponse qu'il a attribué le numéro concerné à un autre fournisseur, dont il précisera le nom et les coordonnées (adresse et numéro de téléphone).

Art. 41 Type de renseignements IR_12_TEL: renseignements sur des services de téléphonie et multimédia

Cet article définit le type de renseignements standardisé concernant les services de téléphonie et multimédia. Ce type de renseignements correspond sur le principe à l'actuel type A1 (données techniques). L'appellation *services de téléphonie et multimédia* est expliquée dans le commentaire de l'art. 40.

L'*al. 1* définit, sur le modèle de l'art. 36, al. 1, les indications à livrer en réponse à une demande de renseignements portant sur des services de téléphonie et multimédia. En ce qui concerne la liste des identifiants des équipements (*let. d*), voir le commentaire de l'art. 36, al. 1, let. d.

La période de validité indiquée dans la réponse se réfère aux trois paramètres selon la let. b (identifiant du service), la let. c (IMSI et MSISDN) et la let. e (numéro SIM) du premier alinéa, mais ne concerne pas l'identifiant de l'équipement terminal. Si un de ces trois paramètres change pendant la période commune indiquée, la personne obligée de collaborer doit livrer plusieurs enregistrements correspondant au statut des informations. Étant donné que les codes PUK sont liés à la carte SIM, il n'est pas nécessaire de préciser de période de validité pour les paramètres selon l'al. 1, let. f (codes PUK). Leur validité découle directement de la validité des numéros SIM (*al. 1, let. e*).

48 RS **784.104**

L'*al. 2* énumère, sur le modèle de l'art. 36, al. 2, les critères de recherche pour ce type de renseignements et détaille la manière dont ces critères doivent être utilisés (voir le commentaire de l'art. 36, al. 2).

Une distinction est faite entre les ressources d'adressage (*let. a*) et les identifiants (*let. b*, *c* et *e*).

Art. 42 Type de renseignements IR_13_EMAIL: renseignements sur des usagers de services de courrier électronique

Cet article définit le type de renseignements standardisé concernant les usagers de services de courrier électronique et de services de messagerie. Ce type de renseignements correspond sur le principe au type A0 et, en partie, au type A1 actuels.

Cet article est structuré de la même manière que l'art. 40. Le commentaire de l'art. 39 vaut donc aussi pour cet article.

L'*al. 1* définit les indications à livrer en réponse à une demande de renseignements portant sur des usagers de services de courrier électronique.

Parmi les autres ressources d'adressage concernant le service qui doivent être fournies (*let. c, ch. 4*) figurent, notamment, les alias de messagerie. Il s'agit d'adresses électroniques supplémentaires reliées à un même compte de courrier électronique. L'usager peut créer, modifier ou supprimer à sa guise les adresses de ce type. Leur nombre maximal et leur structure sont fixés par le fournisseur du service de courriel. Les courriels envoyés à un alias de messagerie le sont aussi à l'adresse principale du compte de courrier électronique de l'usager.

Le cas échéant, il y a lieu de livrer, conformément au *ch. 5*, toutes les adresses de courrier électronique vers lesquelles sont automatiquement redirigés les messages envoyés à l'adresse de courrier électronique indiquée dans la demande de renseignements, par exemple dans le cas d'une liste de diffusion, c'est-à-dire une liste d'adresses électroniques à laquelle on a attribué une adresse électronique propre. Les messages envoyés à cette adresse sont automatiquement réexpédiés à l'adresse électronique de chacun des membres de la liste de diffusion. Dans cet exemple, la personne obligée de collaborer doit communiquer les adresses électroniques des membres de la liste de diffusion.

Par « autres ressources d'adressage » selon la *let. d*, il faut comprendre d'autres adresses électroniques ou numéros de téléphone qui ne sont pas en soi liés au service concerné. Ces éléments sont par exemple utilisés pour réinitialiser un mot de passe ou pour envoyer des alertes de sécurité aux usagers.

L'*al. 2* énumère, sur le modèle de l'art. 40, al. 2, les critères de recherche pour ce type de renseignements et détaille la manière dont ces critères doivent être utilisés (voir le commentaire de l'art. 40, al. 2). Pour les recherches de chaînes de caractères (*let. a, c, d et f*), le fournisseur doit effectuer une recherche dite exacte au sens de l'art. 13, al. 1, OME-SCPT (voir le commentaire de l'art. 35, al. 2).

Art. 43 Type de renseignements IR_15_COM: renseignements sur des usagers d'autres services de télécommunication ou de services de communication dérivés

Cet article définit le type de renseignements standardisé concernant les usagers d'autres services de télécommunication ou de services de communication dérivés. Ce type de renseignements correspond lui aussi sur le principe au type A0 et, en partie,

au type A1 actuels, la nouveauté résidant dans le fait qu'il pourra dorénavant aussi être utilisé pour cette catégorie de services. Le but est d'englober tous les services de télécommunication et les services de communication dérivés qui bien que déjà exploités, ne sont pas encore soumis à une norme ETSI, celle-ci étant en cours d'élaboration. Il s'agit aussi, subsidiairement, de couvrir de futurs services dont le progrès technique devrait rendre possible le développement. Les services de communication intégrés dans des réseaux sociaux, les services d'informatique en nuage (*cloud*) et les services de serveur mandataire (*proxy*) sont des exemples d'autres services de télécommunication ou de services de communication dérivés relevant de cet article. Les services d'informatique en nuage sont des services de communication dérivés qui peuvent prendre la forme d'applications ou des systèmes de stockage distribués, accessibles via Internet. Disponibles en ligne, ces services sont hébergés dans des centres de calcul distribués, en fonction des ressources nécessaires. Un serveur mandataire, ou *proxy*, est une interface de communication qui remplit une fonction d'intermédiaire dans un réseau: concrètement, le serveur mandataire réceptionne les requêtes d'un premier poste avant de les relayer vers un second poste en établissant une communication via sa propre adresse, d'où l'importance de ces services pour l'identification d'usagers dans des enquêtes portant sur des infractions commises par Internet.

Les services de messagerie relèvent aussi de cette catégorie. Un service de messagerie est un service autonome (c'est-à-dire indépendant de services de téléphonie ou multimédia), principalement asynchrone, permettant de transférer des messages. On mentionnera, à titre d'exemple, les services de messagerie instantanée, la messagerie IMS, les applications de messagerie et les SMS de fournisseurs tiers (c'est-à-dire des services de SMS qui ne sont pas fournis par le FST de l'usager). Ces services peuvent aussi englober des fonctions supplémentaires étendues, comme une fonction de communication multimédia, le transfert de fichiers ou des informations de présence (l'usager peut voir, par exemple, le statut et éventuellement l'emplacement d'un autre utilisateur).

Cet article est structuré de la même manière que les art. 40 à 42. Les commentaires de ces dispositions valent donc aussi pour cet article.

L'*al. 1* définit les indications à livrer en réponse à une demande de renseignements portant sur des usagers d'autres services de télécommunication ou de services de communication dérivés. Concernant les identifiants selon la let. c, ch. 5, il peut s'agir par exemple de l'identifiant spécifique d'une application et de l'appareil utilisé pour recevoir les notifications envoyées par l'application. En utilisant cet identifiant, on est assuré que les notifications d'une application déterminée sont bien envoyées à un appareil déterminé (par ex. "Device Token" du service de notifications push d'Apple, "Registration Identifier" du système de messagerie Google Cloud Messaging, "Channel URI" du service de notifications push de Windows). Ce paramètre peut être indiqué pour obtenir l'identifiant spécifique d'une application et d'un appareil.

L'*al. 2* énumère, sur le modèle des art. 40 à 42, les critères de recherche pour ce type de renseignements et détaille la manière dont ces critères doivent être utilisés (voir le commentaire relatif à l'art. 40, al. 2). Pour les recherches de chaînes de caractères (*let. a, c, d et f*), le fournisseur doit effectuer une recherche dite exacte au sens de l'art. 13, al. 1, OME-SCPT (voir le commentaire de l'art. 35, al. 2). Il est possible d'utiliser le paramètre selon la let. i par exemple pour une recherche au moyen de l'identifiant spécifique d'une application et d'un appareil.

Section 6 Autres types de renseignements

Art. 44 Type de renseignements IR_17_PAY: renseignements sur la méthode de paiement utilisée par les usagers de services de télécommunication et de services de communication dérivés

Cet article définit le type de renseignements standardisé concernant les méthodes de paiement utilisées par les usagers de services de télécommunication et de services de communication dérivés. Comme les méthodes de paiement ne diffèrent pas fondamentalement entre les différentes catégories de services, cet article les couvre toutes. Ce type de renseignements se fonde sur le paramètre ETSI relatif aux détails de paiement (ETSI-Parameter PaymentDetails).

Il n'existe pas encore de paramètre ETSI approprié pour l'actuel type de renseignements A1 (données techniques) concernant les codes de recharge (*scratch codes*) utilisés. Cet article étend les renseignements qu'il est possible de recueillir à toutes les méthodes de paiement pouvant être utilisées en lien avec des services de télécommunication et des services de communication dérivés, qu'il s'agisse de services sur abonnement ou de services à prépaiement.

L'*al. 1* définit les indications à livrer.

L'*al. 2* précise que le fournisseur doit uniquement livrer les données dont il dispose. Ainsi, pour les services gratuits, comme les services de courrier électronique, aucune information ne doit être saisie concernant la méthode de paiement.

L'al. 3 énumère les critères de recherche pour ce type de renseignements et détaille la manière dont ces critères doivent être utilisés.

Art. 45 Type de renseignements IR_18_ID: copie de la pièce d'identité

L'art. 20 détermine les indications relatives à la personne qu'il y a lieu de saisir aussi bien lors de la vente de cartes à prépaiement que lors de la conclusion d'abonnements ou de l'utilisation d'offres gratuites de communication mobile. Pour garantir l'exactitude des indications saisies et prévenir toute erreur dans l'enregistrement des données personnelles, les personnes obligées de collaborer sont tenues de sauvegarder dans leur système également une copie électronique de la pièce d'identité produite par les usagers. L'article ne prescrit pas la manière dont le fournisseur doit sauvegarder la copie électronique. La seule condition est qu'il s'agisse d'une copie lisible et que le fournisseur soit en mesure de la livrer sur demande.

Grâce à ce type de renseignements, les autorités habilitées peuvent consulter la copie de la pièce d'identité enregistrée avec les données d'un usager ou sauvegardée en lien avec un service en particulier. L'autorité doit préciser le moment sur lequel porte sa requête, ainsi que l'identifiant de l'usager ou l'identifiant du service auquel elle se rapporte (*al. 2*). La copie de la pièce d'identité doit être transmise par voie électronique. Pour les services d'accès au réseau, la recherche peut également se fonder sur l'identifiant d'un équipement. Il convient de préciser qu'un lien direct entre l'identifiant de l'équipement et la pièce d'identité n'existe que si l'appareil a été acheté au moment de la conclusion du contrat et de l'enregistrement de la copie de la pièce d'identité. Il se peut aussi que la personne ait remis ou revendu l'appareil à un tiers, ce que le fournisseur n'a pas la possibilité de savoir.

Art. 46 Type de renseignements IR_19_BILL: copie de factures

Ce type de renseignements correspond à l'actuel type A2 (données de facturation); voir en particulier l'art. 21, al. 1, let. d, LSCPT. Les personnes obligées de collaborer doivent fournir une copie électronique de toutes les pièces comptables disponibles concernant l'usager. Il est important qu'aucune donnée secondaire ne soit livrée dans le même temps. Aucune communication ne doit ainsi apparaître sur la copie d'une facture. Il suffit de transmettre la première page (récapitulation) des factures mensuelles, où sont indiqués le montant dû, le numéro de client et l'adresse de facturation. Comme pour la copie de la pièce d'identité, l'autorité doit préciser dans sa demande la période sur laquelle porte sa requête, ainsi que l'identifiant de l'usager ou l'identifiant du service auquel elle se rapporte (*al. 2*).

Art. 47 Type de renseignements IR_20_CONTRACT: copie du contrat

Ce type de renseignements correspond à l'actuel type A2 (copie du contrat) (voir en particulier l'art. 21, al. 1, let. d, LSCPT). Il a pour objet la transmission d'une copie électronique de tous les documents contractuels disponibles ou tout autre enregistrement comparable. Les contrats pouvant aussi être conclus oralement, il peut arriver que le fournisseur ne dispose pas d'un document écrit. Cet article n'instaure pas d'obligation de conclure des contrats exclusivement par écrit. En l'absence de contrat écrit, il suffit que la personne obligée de collaborer livre, par exemple, une capture d'écran rendant compte de l'existence de la relation contractuelle. L'autorité habilitée doit préciser ici aussi dans sa demande le moment sur lequel porte sa requête, ainsi que l'identifiant de l'usager ou l'identifiant du service auquel elle se rapporte (*al. 2*). Pour les services d'accès au réseau, la recherche peut également se fonder sur l'identifiant d'un équipement. Il convient de préciser ici aussi qu'un lien direct entre l'identifiant de l'équipement et la pièce d'identité n'existe que si l'appareil a été acheté au moment de la conclusion du contrat et de l'enregistrement de la copie de la pièce d'identité. De même, on ne peut pas exclure que la personne ait remis ou revendu l'appareil à un tiers, ce que le fournisseur n'a pas la possibilité de savoir.

Art. 48 Type de renseignements IR_21_TECH: données techniques

Aux termes de cet article, les personnes obligées de collaborer sont tenues de livrer les données techniques relatives aux systèmes de télécommunication ou aux éléments réseau (voir en particulier l'art. 21, al. 1, let. d, LSCPT). Elles doivent conserver ces données pendant six mois. On pourrait néanmoins imaginer que des données complémentaires soient demandées sur la couverture d'une antenne concernant une surveillance rétroactive remontant à plus de six mois. Dans ce cas, les personnes obligées de collaborer devraient livrer les données dans la mesure où celles-ci sont encore disponibles.

Ce type de renseignements correspond à l'actuel type A3. Sont visés en premier lieu les données de localisation d'antennes de téléphonie mobile et de points d'accès publics au réseau WLAN. La norme ETSI pertinente ne prévoit pas, dans sa teneur actuelle, la livraison d'indications supplémentaires, comme le type de technologie de communication mobile ou les fréquences. Ces informations seront néanmoins ajoutées ultérieurement dans l'ordonnance à la faveur d'une révision partielle, sitôt que les conditions requises auront été créées dans la norme ETSI. On relèvera que ces données figurent déjà dans la norme propriétaire relative à la transmission des résultats d'une recherche manuelle en cas d'urgence EP_35_PAGING.

L'*al. 2* définit de manière détaillée le contenu des données de localisation de cellules de téléphonie mobile et de points d'accès au réseau WLAN. Les indications selon les *let. b à d* ne doivent être fournies que dans la mesure où elles sont disponibles. Le champ « azimut » (direction principale d'émission) est prévu dans la norme ETSI. Il ne peut être utilisé de manière judicieuse que si les données correspondantes existent vraiment, d'où la précision « le cas échéant » dans le libellé de la disposition. Le mécanisme spécial mis au point pour les recherches en cas d'urgence afin de permettre la transmission d'attributs tels que « omnidirectionnel » n'est pas disponible pour les recherches visées dans cet article.

L'*al. 3* énumère les différents critères de recherche pour ce type de renseignements et dispose que la demande doit indiquer au moins un critère de recherche. L'autorité doit préciser dans sa demande la période sur laquelle porte sa requête. Lorsque la recherche s'effectue au moyen de coordonnées géographiques (*let. a*), il faut veiller à indiquer des coordonnées suffisamment précises et se rapportant exactement à une localisation. Le fournisseur doit quant à lui livrer les données techniques de tous les éléments réseau situés dans un rayon de 50 mètres autour de la localisation indiquée. Cette distance offre une marge de tolérance qui permet de trouver dans tous les cas l'élément réseau recherché, y compris en cas d'indication de coordonnées géographiques très précises. Le fournisseur ne doit toutefois pas exécuter d'analyse de couverture de réseau pour les coordonnées géographiques signalées dans la demande de renseignements. Pour une analyse de la couverture du réseau, il convient d'utiliser le type de surveillance AS_32_PREP_COV (art. 64).

Section 7 Dispositions générales concernant la surveillance de la correspondance par télécommunication

Art. 49 Ordre de surveillance de la correspondance par télécommunication

Cet article reprend pour l'essentiel les dispositions de l'art. 15 l'OSCPT dans sa teneur du 31 octobre 2001[49]. Il définit les indications que doit contenir l'ordre transmis au Service SCPT pour mettre en œuvre une surveillance de la correspondance par télécommunication (pour la correspondance par poste, voir le commentaire de l'art. 15). Une fois la réception d'un ordre de surveillance confirmée, il n'est plus possible de modifier les indications figurant sur le formulaire, mis à part les droits d'accès. Pour les changements importants, comme le type de surveillance ou l'identifiant à surveiller (target ID), un nouvel ordre est nécessaire. Les émoluments et les indemnités usuels s'appliquent.

L'*al. 1* dresse la liste exhaustive des indications qui doivent figurer sur l'ordre de surveillance.

Let. a: le Service DFJP effectue un contrôle formel pour s'assurer que l'autorité qui a ordonné la surveillance est bien habilitée à le faire ou, dans le cas d'une surveillance ordonnée par le SRC, si la mesure a bien été autorisée et avalisée conformément aux art. 29 à 31 LRens (art. 16, let. a, ch. 2, LSCPT).

49 RS **780.11**

Let. b: le Service SCPT se fonde sur ces indications pour paramétrer dans son système de traitement les droits d'accès aux données issues de la surveillance.

Let. c: ces indications, pour autant qu'elles soient disponibles, permettent de vérifier auprès du FST ou du fournisseurs de services de communications dérivés si l'application ou l'accès Internet à surveiller est effectivement lié à la personne concernée.

Let. d: l'indication du numéro de référence et du nom de l'affaire est nécessaire pour saisir correctement l'ordre dans le système de traitement.

Let. e: le Service DFJP effectue un contrôle formel pour s'assurer qu'il s'agit bien d'une infraction autorisant une surveillance conformément aux art. 269 (surveillances en temps réel) et 273 CPP (surveillances rétroactives) ou à l'art. 70d PPM (surveillances rétroactives).

Let. f: l'autorité qui ordonne la surveillance communique au Service SCPT le nom de la personne obligée de collaborer qui doit exécuter la surveillance.

Let. g: l'autorité doit préciser les types de surveillance qu'il ordonne. Il peut s'agir de surveillances ayant fait l'objet d'une standardisation, comme de mesures non standardisées. En cas de doute ou de contradictions ou si le montant des émoluments sera vraisemblablement élevé, le Service SCPT prend contact avec l'autorité qui a ordonné la surveillance pour clarifier la situation.

Let. h: l'autorité doit indiquer au Service SCPT les identifiants à surveiller. En cas de questions, le Service SCPT prend contact avec l'autorité concernée.

Let. i:

- *ch. 1:* si la personne à surveiller change de raccordement à intervalles rapprochés, le tribunal des mesures de contrainte peut exceptionnellement autoriser, en vertu de l'art. 272, al. 2, CPP, que chaque raccordement identifié utilisé par cette personne soit surveillé sans nouvelle autorisation (autorisation-cadre). La demande d'autorisation-cadre doit être jointe à l'ordre de surveillance.

- *ch. 2:* le Service SCPT veille à la mise en œuvre des mesures de protection indiquées.

Let j: l'autorité doit indiquer la période sur laquelle porte la surveillance, compte tenu des délais pertinents. Les surveillances en temps réel ne peuvent être ordonnées que pour les trois mois au plus à venir, tandis que les surveillances rétroactives ne peuvent remonter que sur six mois au plus.

Let. k et *l*: voir le commentaire de l'art. 5. La let. k concerne les personnes tenues au secret professionnel ou au secret de fonction au sens des art. 271 CPP et 70*b* PPM, comme les avocats ou les médecins. Dans ces cas, le Service SCPT doit préparer le tri des informations issues de la surveillance de la correspondance par télécommunication des personnes concernées et prendre, le cas échéant, les mesures selon la let. l.

L'*al. 2* concerne les surveillances dont l'exécution requiert des indications techniques supplémentaires, par exemple parce qu'il s'agit d'un type de surveillance qui n'a pas fait l'objet d'une surveillance standardisation ou que les données issues de la surveillance ne sont pas transmises via le système de traitement du Service SCPT.

Art. 50 Obligations en matière de surveillance

L'*al. 1*, définit le cercle des personnes obligées de collaborer auxquelles peut être confiée l'exécution de mesures de surveillance de la correspondance par

télécommunication. En plus des fournisseurs de services de télécommunication, un mandat de surveillance active pourra dorénavant aussi être transmis aux fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance au sens de l'art. 52. L'ordonnance précise également qu'un tel mandat ne pourra pas être confié aux FST ayant des obligations restreintes en matière de surveillance. Dans le cas de la correspondance par télécommunication, le terme obligations en matière de surveillance désigne l'exécution des types de surveillance visés aux sections 8 à 12 du chapitre 3. Les personnes obligées de collaborer doivent être en mesure d'exécuter elles-mêmes ces obligations ou de les faire exécuter par des tiers (art. 32 LSCPT).

Conformément à l'*al. 2*, la disponibilité à surveiller doit être garantie dès le début de l'exploitation commerciale d'un service. Cela signifie que la procédure de contrôle de la disponibilité à renseigner et à surveiller doit être menée à bien avant que commence cette exploitation (cf. commentaires des art. 31 à 34). L'exploitation commerciale ne couvre pas les phases de test ou les phases pilotes.

L'*al. 3* dispose que les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance doivent être en mesure, également en dehors des heures normales de travail (voir art. 10), de réceptionner des mandats de surveillance et de les exécuter dans les délais prescrits. La compétence de fixer ces délais de traitement est déléguée au DFJP, qui les définit dans l'OME-SCPT.

L'*al. 4* définit quelle partie de la correspondance par télécommunication doit être surveillée et pendant combien de temps. Le Service SCPT transmet aux personnes obligées de collaborer un mandat d'activation au début de la surveillance et un mandat de désactivation lorsque la mesure doit être levée. Dans le cas de surveillances rétroactives, seul un mandat d'activation indiquant la période sur laquelle porte la mesure est envoyé. Il n'est pas possible de préciser dans le mandat d'activation d'une surveillance en temps réel quand exactement prendra fin la mesure. Cette date n'est communiquée aux personnes obligées de collaborer qu'avec le mandat de désactivation de la surveillance.

Les fournisseurs doivent garantir qu'ils peuvent exécuter la surveillance de toute correspondance par télécommunication qu'ils contrôlent. Seule doit toutefois être transmise la correspondance ayant pour origine ou pour destination l'accès au réseau surveillé ou qui concerne l'application ou l'identifiant cible surveillé (target ID; par ex. appels ayant pour origine ou pour destination le numéro de téléphone d'un service de téléphonie). L'expression « la correspondance par télécommunication qu'il contrôle » désigne toute l'infrastructure dont la personne obligée de collaborer est la propriétaire, qu'elle loue, qu'elle gère, qu'elle a externalisée ou qu'elle utilise contractuellement en vertu d'un droit d'utilisation particulier (par ex. opérateur de réseau virtuel mobile, ORVM). En ce qui concerne l'utilisation d'une infrastructure *étrangère* (par ex. itinérance à l'étranger), les télécommunications ne doivent être surveillées que dans la mesure où elles peuvent être contrôlées par le fournisseur dans le cadre de ses procédures techniques usuelles d'exploitation (par ex. routage, signalisation). Les procédures techniques d'exploitation doivent en principe être identiques pour les usagers (cibles) ou les services (cibles) surveillés et les usagers ou les services qui ne font pas l'objet d'une surveillance. En cas d'utilisation de l'infrastructure *nationale* d'un fournisseur étranger (par ex. itinérance nationale, opérateur de réseau mobile virtuel), la personne obligée de collaborer doit garantir la livraison, par ses propres soins ou par des tiers, de toute la correspondance par télécommunication faisant l'objet de la surveillance.

Les personnes obligées de collaborer doivent donc aussi être en mesure de surveiller les télécommunications contenant des ressources d'adressage qu'elles n'ont pas attribuées elles-mêmes ou qui ne se trouvent pas dans leur réseau ou n'y sont pas enregistrées (par ex. surveillance d'un numéro de téléphone étranger, voir l'art. 69).

L'itinérance recouvre deux cas de figure:

1. Itinérance sortante: il s'agit ici de surveiller la correspondance par télécommunication d'un usager géré par la personne obligée de collaborer lorsque l'équipement terminal de la personne est enregistré en tant que visiteur dans un réseau étranger. On distingue deux situations:

A) l'utilisation d'un réseau étranger sur le territoire national et

B) l'utilisation d'un réseau étranger à l'étranger

Dans la situation A, la personne obligée de collaborer – ou les tiers mandatés par elle – doit veiller à ce que les communications soient aussi surveillées dans leur intégralité lorsque l'usager utilise un réseau étranger en Suisse.

Dans la situation B en revanche, la personne obligée de collaborer doit uniquement être en mesure de surveiller le contenu et les données secondaires des communications qu'elle contrôle dans le cadre de ses procédures techniques usuelles d'exploitation et auxquels elle peut par conséquent accéder.

2. Itinérance entrante: il s'agit de surveiller la correspondance par télécommunication d'un usager étranger lorsque son équipement terminal est enregistré en tant que visiteur dans le réseau de la personne obligée de collaborer chargée d'exécuter la surveillance. Dans ce cas de figure, c'est précisément parce que l'équipement de l'usager étranger est enregistré en tant que visiteur dans un réseau en Suisse que la surveillance est possible. Il peut toutefois arriver, en raison de certaines particularités techniques, que le contenu des communications interceptées soit crypté. C'est le cas par exemple lorsque les données transitent de manière chiffrée dans un tunnel entre l'équipement de l'usager étranger et son réseau d'origine et que le cryptage n'a pas été opéré par la personne obligée de collaborer, qui ne peut logiquement pas non plus le supprimer. Il convient de noter qu'un fournisseur de services de communication mobile étranger n'a pas d'obligations au sens de la LSCPT dès lors qu'il n'est pas considéré comme une personne obligée de collaborer au sens de l'art. 2 LSCPT et que ses clients sont uniquement enregistrés en tant qu'invités (itinérance entrante) dans un réseau suisse.

Les données livrées doivent correspondre à la correspondance indiquée dans le mandat de surveillance. Au besoin, le fournisseur apporte son soutien au Service SCPT pour s'en assurer (*al. 5*).

Les personnes obligées de collaborer doivent en outre veiller, conformément à l'*al. 6,* à ce que les éventuels identifiants supplémentaires associés à l'identifiant surveillé (target ID) soient aussi surveillés. Le Service DFJP définira tous les cas possibles d'association d'identifiants après avoir entendu les fournisseurs (par ex. alias de messagerie auprès d'un fournisseur de services de courrier électronique).

Art. 51 FST ayant des obligations restreintes en matière de surveillance

Les FST doivent être en mesure d'exécuter ou de faire exécuter par des tiers les obligations en matière de surveillance qui concernent les services qu'ils proposent (art. 32 LSCPT). Cela signifie, entre autres obligations, qu'ils doivent disposer des

équipements nécessaires à cette fin. L'acquisition des équipements requis entraîne des coûts d'investissement que les FST ne peuvent pas tous assumer avec la même facilité, notamment les FST de petite taille et ceux de taille moyenne. C'est pourquoi le législateur a donné la compétence au Conseil fédéral, à l'art. 26, al. 6, LSCPT, de dispenser de certaines obligations légales les FST offrant des services de télécommunication de faible importance économique ou dans le domaine de l'éducation. Ceux-ci ne peuvent toutefois pas être dispensés des obligations légales minimales consistant à tolérer une surveillance, à supprimer les cryptages qu'ils ont opérés, à garantir l'accès à leurs installations et à livrer, sur demande, les données secondaires de télécommunication de la personne surveillée dont ils disposent (art. 26, al. 2 et 6, LSCPT). Comme demandé pendant la consultation, l'expression « domaine de l'éducation » a été remplacée dans les ordonnances par « domaine de la recherche et de l'éducation ».

L'*al. 1* définit les conditions qui doivent être remplies pour que le Service SCPT puisse déclarer, par une décision, un FST qui en fait la demande comme ayant des obligations restreintes en matière de surveillance. En cas de décision positive, le FST ne doit pas exécuter des obligations autres que les obligations minimales mentionnées plus haut. Concrètement, un FST peut être considéré comme ayant des obligations restreintes en matière de surveillance s'il offre ses services exclusivement dans le domaine de la recherche et de l'éducation (let. a) ou s'il ne remplit pas les deux conditions selon la let. b. Si après examen des documents produits, le Service SCPT arrive à la conclusion que le FST satisfait aux exigences de l'al. 1, il rend une décision en ce sens, qu'il communique au FST concerné, lequel n'est plus tenu à partir de ce moment de garantir la disponibilité à surveiller. Le Service SCPT doit pour sa part prendre les mesures nécessaires pour que les surveillances continuent d'être exécutées (art. 17, let. e, et art. 26, al. 2, let. b, LSCPT; voir aussi le commentaire de l'art. 53, accès aux installations).

Aux termes de la *let. a*, les FST qui n'offrent leurs services que dans le domaine de la recherche et de la formation sont considérés, de ce seul fait, comme ayant des obligations restreintes en matière de surveillance. Ils doivent uniquement exécuter les obligations minimales prévues par la loi.

La première condition fixée à la *let. b*, *ch. 1*, pour qu'un FST puisse être considéré comme ayant des obligations restreintes en matière de surveillance est qu'il ait exécuté des mandats de surveillance portant sur moins de dix cibles différentes au cours des douze mois écoulés, la date de référence étant arrêtée au 30 juin. C'est le nombre cumulé de surveillances en temps réel et rétroactives qui est ici déterminant. On utilise ici un critère qui a fait ses preuves, celui du nombre de mandats de surveillance. Même si l'art. 26, al. 6, LSCPT ne prévoit pas explicitement ce critère, sa formulation ouverte (termes « peut » et « en particulier ») donne toute latitude au Conseil fédéral de fixer d'autres critères objectifs. Comme le montre la statistique de la surveillance des télécommunications de ces dernières années, les fournisseurs importants au regard de la surveillance des télécommunications ont toujours exécuté un certain nombre de mandats. Par conséquent, en fixant un nombre minimal de mandats de surveillance à atteindre, il est possible de déterminer de manière relativement fiable quels sont les FST qui revêtent une importance moindre en matière de surveillance – lesquels peuvent dès lors être considérés comme ayant des obligations restreintes – et tenir mieux compte du principe de proportionnalité.

Conformément à la seconde condition selon la *let. b*, *ch. 2*, pour être considéré comme ayant des obligations restreintes en matière de surveillance, un FST ne doit pas avoir

réalisé un chiffre d'affaires annuel supérieur à 100 millions de francs pendant deux années consécutives. La portée de ce critère est néanmoins circonscrite en ce sens que seul est déterminant le chiffre d'affaires généré par les services de télécommunication et les services de communication dérivés.

Au vu du seuil selon la *let. b*, le nombre de FST ayant des obligations actives en matière de surveillance pourrait ainsi être ramené de 600 selon le droit en vigueur à un nombre compris entre 20 et 30. La surveillance des télécommunications doit rester garantie nonobstant la dispense de certains fournisseurs d'obligations étendues en matière de surveillance: des surveillances pourront aussi être exécutées auprès de fournisseurs dont les obligations sont réduites, puisque ceux-ci restent soumis à l'obligation de tolérer une surveillance et d'y coopérer. La dispense qui leur est accordée ne les libère pas, en effet, de l'obligation de livrer sur demande les données secondaires de télécommunication dont ils disposent pour la personne surveillée (art. 26, al. 6, LSCPT). Comme indiqué précédemment, le Service SCPT doit quant à lui prendre les mesures nécessaires pour que les surveillances continuent d'être mises en œuvre.

L'*al. 2* dispose que l'art. 22, al. 2, s'applique par analogie au cas des fournisseurs qui contrôlent une ou plusieurs entreprises tenues d'établir des comptes. Afin d'empêcher les abus, le fournisseur et les entreprises contrôlées sont considérés, ici aussi, comme formant une unité (voir le commentaire de l'art. 22 pour plus de précisions).

L'*al. 3* instaure une obligation pour les FST ayant des obligations restreintes en matière de surveillance d'informer le Service SCPT, pièces justificatives à l'appui, s'ils n'offrent plus leurs services exclusivement dans le domaine de la recherche et de l'éducation (*let. a*) ou s'ils atteignent, pendant deux exercices consécutifs, les valeurs selon l'al. 1, let. b, ch. 2 (*let. b*). La communication doit intervenir dans les trois mois suivant la fin d'un exercice. Les participants à la consultation se sont plaints de ce que les obligations des FST ayant des obligations restreintes en matière de surveillance ne ressortaient pas clairement du texte de l'ordonnance. La démarche retenue pour la révision de l'OSCPT a été de ne pas énumérer, dans une disposition générale, les obligations des différentes catégories et sous-catégories de personnes obligées de collaborer, mais d'inscrire les obligations dans les diverses normes matérielles. Le tableau à la fin du présent rapport récapitule les obligations des personnes obligées de collaborer.

L'*al. 4* autorise le Service SCPT à se procurer d'autres données pour vérifier si un fournisseur dépasse ou, à l'inverse, n'atteint pas les valeurs selon l'al. 4 et rendre sa décision.

Comme prévu également à l'art. 22, al. 5, les FST doivent garantir l'enregistrement des données nécessaires pour exécuter la surveillance et assurer la disponibilité à surveiller respectivement dans les deux et les douze mois à compter du moment où le Service SCPT décide qu'ils ne sont plus considérés comme des FST ayant des obligations restreintes en matière de surveillance (*al. 5*).

Art. 52 Fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance

Comme pour les obligations en matière de fourniture de renseignements visées à l'art. 22 LSCPT, le législateur donne la compétence au Conseil fédéral, à l'art. 27, al. 3, LSCPT, de soumettre les fournisseurs de services de communication dérivés à

des obligations étendues en matière de surveillance. Cet article concrétise cette compétence.

Structuré de la même manière que l'art. 22, qui définit les conditions qui doivent être remplies pour que les fournisseurs de services de communication dérivés soient soumis à des obligations étendues en matière de fourniture de renseignements, l'art. 50 traite spécifiquement des surveillances. La seule différence par rapport à l'art. 21 concerne la condition alternative du nombre de mandats: au cours des douze mois écoulés, le fournisseur doit avoir exécuté des mandats de surveillance concernant au moins dix cibles différentes. La *let. a* se réfère au critère du grand nombre d'utilisateurs mentionné à l'art. 27, al. 3, LSCPT. Il est très difficile, du point de vue des télécommunications, de donner une définition *absolue* de l'expression « grand nombre d'utilisateurs » et d'arrêter par avance un nombre précis, qui plus est si l'on pense aux différents services techniques qui existent. La let. a opte pour un critère qui a fait ses preuves dans la pratique, à savoir le nombre de mandats de surveillance. Comme le montrent les statistiques des mandats de surveillance des télécommunications de ces dernières années, il s'agit d'un critère fiable et adapté au type de services proposés pour appréhender la notion du grand nombre d'utilisateurs. Il permet aussi de tenir compte du principe de proportionnalité, dès lors que seuls sont visés les fournisseurs qui sont réellement importants au regard de la surveillance des télécommunications. Pour le reste, les dispositions de l'art. 50 et de l'art. 21 sont identiques. Le commentaire de l'art. 22 vaut donc aussi pour cet article (remarque: une distinction entre surveillances en temps réel et surveillances rétroactives n'est pas prévue pour examiner les obligations des fournisseurs en matière de surveillance. C'est donc le nombre cumulé de surveillances en temps réel et rétroactives qui est ici déterminant).

Les fournisseurs de services de communication dérivés ont les mêmes obligations que les FST. Cela signifie qu'ils sont soumis, notamment, aux obligations selon l'art. 26, al. 1 et 3 à 5, LSCPT. Ils doivent en particulier prendre activement toutes les dispositions nécessaires pour être en mesure d'exécuter ou de faire exécuter par des tiers les types de surveillance ayant fait l'objet d'une standardisation définis aux sections 7 à 12 du chapitre 3 et pour conserver pendant six mois les données secondaires de télécommunication. Les dispositions de la LSCPT régissant les obligations des fournisseurs de services de télécommunication s'appliquent par analogie aux fournisseurs de services de communication dérivés (art. 27, al. 3, LSCPT).

Art. 53 Accès aux installations

Certaines personnes obligées de collaborer ne sont pas tenues, conformément à la loi, d'exécuter activement des mandats de surveillance (par ex. les FST ayant des obligations restreintes au sens de l'art. 51), tandis que d'autres ne sont pas encore en mesure de garantir la disponibilité à surveiller et ne peuvent pas, dès lors, mettre en œuvre une surveillance. Le Service SCPT exécute alors lui-même l'ordre de surveillance ou le fait exécuter par des tiers (art. 26, al. 2, let. b, LSCPT). De même, il exécute ou fait exécuter par des tiers les surveillances qui n'ont pas fait l'objet d'une standardisation (art. 32, al. 2, LSCPT). Dans tous les cas, l'accès aux installations de la personne obligée de collaborer concernée doit être garanti.

L'*art. 53* précise ce qu'il faut entendre par « accès aux installations »: concrètement, cela signifie qu'il faut pouvoir accéder aux bâtiments, mais aussi aux infrastructures, aux équipements, aux lignes, aux systèmes, aux réseaux et aux services; cet accès doit

être garanti physiquement ou à distance (al. 1). Si l'exécution de la surveillance le requiert, la personne obligée de collaborer doit aussi mettre gratuitement à la disposition du Service SCPT ou des tiers qu'il aura mandatés les accès dont elle dispose aux réseaux de télécommunication publics (par ex. raccordement Internet; al. 2). Si elle ne dispose pas de tels accès, elle doit les créer, pour autant que cela ne représente pas une charge disproportionnée. Au besoin, elle doit aussi mettre en place, en collaboration avec le Service SCPT ou avec les tiers mandatés, de nouveaux accès au réseau. Les frais se rapportant à ces accès sont à la charge du Service SCPT.

Section 8 Types de surveillance en temps réel de services d'accès au réseau

Art. 54 Type de surveillance RT_22_NA_IRI: surveillance en temps réel des données secondaires de services d'accès au réseau

Cet article a pour objet la surveillance en temps réel d'un service d'accès au réseau (correspond à l'actuel type de surveillance PS 2). À la différence du type de surveillance défini à l'art. 55, le type de surveillance visé dans cet article porte uniquement sur les données secondaires de télécommunication. Il est utilisé uniquement pour des accès mobiles à Internet (*al. 1*), afin d'obtenir les données de localisation en temps réel.

De manière générale, aucune donnée secondaire concernant des applications n'est livrée dans ce type de surveillance. Si une personne utilise une application de téléphonie par Internet (VoIP) via le service d'accès au réseau surveillé, les données secondaires de l'application en question ne sont pas transmises à l'autorité. Des types de surveillance spécifiques sont prévus pour les applications. Il en va de même des messages MMS: dans le cadre d'une surveillance de ce type, seules sont livrées les données secondaires de l'accès au réseau et non les données secondaires concernant spécifiquement les MMS (les MMS sont considérés comme étant une application).

L'*al. 2* définit les données secondaires de la correspondance par télécommunication reçue ou émise via le service d'accès au réseau surveillé qu'il y a lieu de transmettre en temps réel dans ce type de surveillance. Les « changements techniques » selon l'*al. 2*, *let. g*, désignent des événements qui modifient les propriétés techniques de l'accès au réseau surveillé ou qui concernent son système de gestion de la mobilité (*mobility management*, MM), comme la modification du service support (*bearer modification*) et l'actualisation de la position (*location update*).

L'*al. 3* précise le contenu des données de localisation selon l'al. 1, let. h. Trois options s'offrent aux personnes obligées de collaborer. Le cas échéant, elles doivent préciser qu'il s'agit de données déterminées – et donc vérifiées – par le réseau. Celles-ci sont en effet plus fiables que les données qui pourraient provenir d'un équipement terminal ou d'une application, lesquelles ne sont pas vérifiées.

Conformément à la *let. a*, la personne obligée de collaborer doit fournir, notamment, la direction principale d'émission de la cellule utilisée, pour autant que cette information soit disponible et univoque. Pour les antennes ayant plusieurs secteurs par exemple, il n'est pas possible d'établir une moyenne. Il est impératif de livrer la direction principale d'émission de chaque secteur individuel, dès lors que chaque secteur possède son propre identifiant (par ex. Cell ID). Dans le cas d'une cellule

simple, la direction principale d'émission décrit l'angle en degrés [°] entre le nord géographique et la direction principale d'émission de l'antenne, alors que dans le cas d'une cellule complexe avec plusieurs directions principales d'émission ou d'une cellule omnidirectionnelle, c'est-à-dire qui émet à 360 degrés, ce champ est vide. Si cette information est disponible, il y a lieu d'indiquer également le type de technologie de communication mobile utilisée. S'il s'agit de 2G ou de 3G, cette indication n'est pas possible, car elle ne figure pas dans la norme correspondante. L'indication est en revanche possible pour la 4G, car la norme s'y rapportant prévoit le paramètre « Radio Access Technology » (RAT), qui peut contenir la donnée « 4G » ou « WiFi ».

La *let. c* offre une troisième possibilité pour livrer les données de localisation. Cette disposition renvoie uniquement aux normes internationales en vigueur et à venir concernant la communication des données de localisation. Elle rend superflue une adaptation de l'ordonne chaque fois que les normes internationales sont mise à jour ou que de nouvelles normes sont adoptées.

Art. 55 Type de surveillance RT_23_NA_CC_IRI: surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau

Le type de surveillance défini dans cet article correspond à l'actuel type PS 1. Lors d'une surveillance de ce type, la personne obligée de collaborer doit livrer l'intégralité de la correspondance par télécommunication émise (téléversement) ou reçue (téléchargement) via le service d'accès au réseau surveillé, par exemple un accès mobile à Internet. Concrètement, cela signifie que tant le contenu (*communication content*, CC) que les données secondaires (IRI) selon l'art. 54 doivent être transmis en temps réel.

Comme relevé dans les explications relatives à l'art. 50, al. 4, si la personne obligée de collaborer doit garantir la surveillance de l'ensemble de la correspondance par télécommunication transitant par l'infrastructure qu'elle contrôle, elle ne doit livrer que la correspondance ayant pour origine ou pour destination l'accès au réseau surveillé. En cas d'utilisation de l'infrastructure nationale d'un fournisseur étranger (par ex. itinérance nationale, opérateur de réseau mobile virtuel [MVNO]), la personne obligée de collaborer doit veiller à la livraison, par ses propres soins ou par des tiers, de l'ensemble de la correspondance par télécommunication faisant l'objet de la surveillance.

En ce qui concerne les infrastructures à l'étranger (par ex. itinérance à l'étranger), les télécommunications ne doivent être surveillées que dans la mesure où elles peuvent être contrôlées par le fournisseur. Si, en revanche, celui-ci contrôle l'infrastructure étrangère, il doit transmettre le contenu des communications surveillées et les données secondaires dans leur intégralité.

Il y a lieu de s'arrêter ici sur le cas particulier des services MMS associés à un service de téléphonie mobile: dans ce type de surveillance, le contenu des MMS n'est pas surveillé en tant qu'application (voir section 9), mais est englobé dans l'accès au réseau. Conformément aux normes ETSI, le contenu des MMS entrants et sortants est considéré comme faisant partie du flux de données transmises dans le cadre de la surveillance de l'accès. En d'autres termes, la surveillance d'un accès mobile à Internet inclut automatiquement la surveillance des MMS. On notera néanmoins qu'aucune donnée secondaire se rapportant spécifiquement aux MMS n'est transférée lors de la surveillance en temps réel d'un accès au réseau. Ces renseignements sont en

revanche livrés avec les types de surveillance RT_24_TEL_IRI (art. 56) et RT_25_TEL_CC_IRI (art. 57).

Ce type de surveillance se fonde sur les normes ETSI ci-après (selon la nature de l'accès au réseau – fixe ou mobile – ou la technologie utilisée):

- accès mobile au réseau (GPRS, UMTS, EPS [LTE], WLAN-Interworking): ETSI TS 101 671, TS 133 108, TS 102 232-1, TS 102 232-7,
- accès fixe au réseau: ETSI TS 102 232-1, TS 102 232-3,
- TS 102 232-7.

Section 9 Types de surveillance en temps réel d'applications

Art. 56 Type de surveillance RT_24_TEL_IRI: surveillance en temps réel des données secondaires de services de téléphonie et multimédia

Cet article définit le type de surveillance standardisé de la surveillance en temps réel de services de téléphonie et multimédia (correspond aux actuels types de surveillance CS 2 et CS 3). On se référera également au commentaire de l'art. 57, qui traite de la surveillance en temps réel des données secondaires et du contenu de services de téléphonie et multimédia. À la différence toutefois du type de surveillance défini à l'art. 57, le type de surveillance visé dans cet article a pour objet uniquement la transmission en temps réel des données secondaires de télécommunication, dont font aussi partie les données de localisation. Les SMS constituent ici la seule une exception: les données secondaires peuvent, pour des raisons techniques, inclure aussi le contenu du message, qui est alors livré avec les données secondaires.

L'*al. 1* énumère les données secondaires qui doivent être livrées en temps réel. Les informations sauvegardées relatives aux événements d'enregistrement et aux réponses correspondantes, visées à la *let. b*, se rapportent par exemple à la requête SIP « REGISTER » (voir RFC 3261). De la même manière, il faut entendre par évènement de souscription par exemple la requête SIP « SUBSCRIBE » (voir RFC 6665). Les « changements techniques » visés à la *let. e* désignent des événements qui modifient les propriétés techniques du service surveillé ou qui concernent son système de gestion de la mobilité (*mobility management*, MM), comme la modification du service support (*bearer modification*) et l'actualisation de la position (*location update*). Dans le cas de services mobiles, doivent également être fournies les données de localisation disponibles (let. e, ch. 9). Les données de localisation à livrer sont décrites en détail à l'al. 2. Des précisions sur leur contenu figurent dans le commentaire de l'art. 54, al. 3.

Pour les liaisons sortantes établies au moyen du libre choix du fournisseur (*carrier selection*) ainsi que pour les tentatives d'établissement de liaisons sortantes, le fournisseur du service téléphonique doit livrer également les données secondaires.

Art. 57 Type de surveillance RT_25_TEL_CC_IRI: surveillance en temps réel du contenu et des données secondaires de services de téléphonie et multimédia

Le type de surveillance défini dans cet article se fonde sur les actuels types CS1, CS2 et CS3. La surveillance des services téléphoniques classiques à commutation de circuits est néanmoins étendue aux services téléphoniques à commutation de paquets

et aux services multimédia. Les services de téléphonie et multimédia regroupent également les services convergents, en particulier les SMS, la messagerie vocale et les services de communication riches (voir l'annexe 1 pour une définition des termes et des abréviations). Le terme *service convergent* désigne toute application que la personne obligée de collaborer fournit à l'usager en relation étroite avec un service téléphonique ou multimédia ou comme faisant partie intégrante de ce service, par exemple de la téléphonie mobile et des SMS, de la messagerie vocale et des services de communication riches ou de la téléphonie fixe convergeant avec de la téléphonie mobile. Les offres multiples combinant plusieurs services comme la téléphonie, un accès à Internet et la télévision qui sont commercialisées en un seul paquet ne sont pas des services convergents.

Il existe toute une série de services téléphoniques à commutation de paquets: la téléphonie par Internet – ou *Voice over IP* (VoIP) – en est un exemple connu. Pour la téléphonie mobile, il s'agit principalement des services VoLTE (*Voice over LTE*, c'est-à-dire le transport de la voix sur les réseaux mobiles 4G) et VoWLAN (*Voice over WLAN* ou accès non-3GPP, c'est-à-dire la téléphonie mobile via le réseau WLAN). S'agissant des services multimédia, on mentionnera notamment ViLTE (*Video over LTE*, c'est-à-dire la vidéotéléphonie sur les réseaux cellulaires 4G).

Les services de téléphonie et multimédia ne font pas l'objet d'une surveillance au point d'accès au réseau. De manière générale, ils sont surveillés en tant qu'applications. Même si le fournisseur de l'accès (par ex. raccordement téléphonique ou accès au réseau cellulaire) est aussi souvent le fournisseur de l'application (service téléphonique), qu'il s'agisse de téléphonie mobile ou de téléphonie filaire classique, ce n'est plus forcément toujours le cas dans les services téléphoniques de nouvelle génération, comme la téléphonie par Internet. Le dégroupage des raccordements progresse dans les réseaux téléphoniques classiques et les clients peuvent désormais choisir librement leur fournisseur pour leurs communications (art. 9 de l'ordonnance du 17 novembre 1997 de la Commission fédérale de la communication relative à la loi sur les télécommunications[50]). Dans le domaine de la communication mobile, le fournisseur du service n'est pas l'opérateur de réseau mobile virtuel ou le fournisseur de l'accès au réseau cellulaire dans le cas de l'itinérance. De la même manière, dans l'architecture IMS (*IP Multimedia Subsystem*) l'accès au réseau peut aussi se faire via les réseaux d'autres fournisseurs qui ne sont pas des réseaux de communication mobile (accès dit non-3GPP). Il ne s'agit là que de quelques exemples de situations dans lesquelles le fournisseur de l'accès au réseau et le fournisseur du service utilisé par l'usager ne sont pas identiques.

Dans ce type de surveillance, les personnes obligées de collaborer doivent transmettre en temps réel l'intégralité des communications passées via le service téléphonique et média surveillé, services convergents compris. En d'autres termes, elles doivent livrer le contenu des communications (*communication content*) et les données secondaires (IRI) énumérées à l'art. 56.

Pour les liaisons sortantes établies au moyen du libre choix du fournisseur (*carrier selection*), ainsi que pour les tentatives d'établissement de liaisons sortantes, le fournisseur du service téléphonique doit livrer également le contenu des communications et les données secondaires.

50 RS **784.101.112**

Art. 58 Type de surveillance RT_26_EMAIL_IRI: surveillance en temps réel des données secondaires de services de courrier électronique

Cet article définit, de manière analogue à l'art. 59, le type de surveillance standardisé de la surveillance en temps réel de services de courrier électronique (correspond à l'actuel type PS 4). Selon le droit en vigueur, un fournisseur de services de courrier électronique n'est tenu d'exécuter une surveillance ayant pour objet des courriels que s'il est aussi fournisseur d'accès à Internet (art. 15, al. 4, LSCPT dans sa teneur du 6 octobre 2000[51]). Cette restriction est supprimée. La surveillance et la transmission des données récoltées obéissent, sur le plan technique, aux prescriptions de la norme ETSI TS 102 232-2. L'actuelle solution propriétaire suisse ne sera plus prise en charge que pendant une période transitoire (voir art. 74).

À la différence du type de surveillance défini à l'art. 59, le type de surveillance visé dans cet article a pour objet uniquement la transmission en temps réel des données secondaires relatives au compte de courrier électronique surveillé, dont font partie les informations de l'enveloppe STMP. Le contenu des messages, pas même la ligne d'en-tête où figure l'objet, ne doit en aucun cas être livré.

La surveillance porte aussi bien sur les opérations concernant le serveur de courrier électronique – comme l'envoi et la réception de courriels et leur enregistrement dans la mémoire des messages (boîte aux lettres électronique) – que sur les accès de clients de courrier électronique au serveur de courrier électronique, c'est-à-dire des opérations telles que les connexions et tentatives de connexion de l'utilisateur à sa boîte de messagerie et les déconnexions (*let. a*), le téléchargement d'un message à partir de la boîte aux lettres électroniques ou la suppression d'un message. Les principaux paramètres des données secondaires, comme les informations AAA hors mot de passe (*let. b*), sont énumérés aux let. *a* à *d*. La *let. d* définit sommairement les événements pour lesquels il y a lieu de générer des informations relatives à l'interception (*Interception Related Information*, IRI). Les détails sont réglés dans la norme ETSI TS 102 232-2 et dans l'annexe 1 de l'OME-SCPT. La surveillance vise aussi les courriels internes, c'est-à-dire les boîtes aux lettres électroniques desservies par le même serveur de messagerie, ainsi que les alias de messagerie et les listes de distribution rattachés au compte de messagerie surveillé (pour des précisions sur les alias de messagerie et les listes de distribution, voir le commentaire de l'art. 42).

Art. 59 Type RT_27_EMAIL_CC_IRI: surveillance en temps réel du contenu et des données secondaires de services de courrier électronique

Le type de surveillance défini dans cet article correspond à l'actuel type PS 3. Les fournisseurs doivent livrer en temps réel tant le contenu que les données secondaires du compte de messagerie électronique qui est l'objet de la surveillance (voir le commentaire de l'art. 58), en veillant à supprimer les cryptages qu'ils ont opérés (art. 26, al. 2, let. c, LSCPT).

51 Voir aussi FF **1998** 3727 ad art. 13, al. 3

Section 10 Types de surveillance rétroactive

Les données collectées dans le cadre d'une surveillance rétroactive (art. 26, al. 4, LSCPT) ou aux fins de l'identification d'auteurs d'infractions par Internet (art. 22 LSCPT) sont appelées dans le langage technique « données retenues » (*retained data*). Il s'agit de données qui sont conservées « en réserve ». De fait, les données secondaires de tous les usagers font l'objet d'une telle conservation. La loi parle de *données secondaires de télécommunication conservées concernant des communications passées* (art. 26, al. 4, LSCPT). Dans le chapitre 3, qui traite exclusivement de la correspondance par télécommunication, c'est plutôt la forme courte *données secondaires conservées* qui est utilisée. Comme la *surveillance rétroactive* se rapporte aux communications passées, on pourrait aussi parler de *données secondaires des communications passées*. On signalera aussi que la surveillance rétroactive existe aussi pour la surveillance de la correspondance par poste (voir art. 16, let. c).

En vertu de la compétence conférée au Conseil fédéral par l'art. 31 LSCPT, la *section 10* du chapitre 3 définit les données secondaires que les personnes obligées de collaborer doivent conserver et livrer dans le cadre d'une surveillance rétroactive.

Les données secondaires qu'il y a lieu de conserver pour permettre l'identification d'auteurs d'infractions commises par Internet (art. 22 LSCPT) sont quant à elles énumérées à l'art. 21, al. 2.

Les données secondaires de télécommunication conservées concernant des communications passées, c'est-à-dire les données secondaires obtenues lors d'une surveillance rétroactive, ne sont pas les mêmes que celles collectées et transmises lors d'une surveillance en temps réel (désignées par l'abréviation IRI). On relèvera, à titre d'exemple, qu'une surveillance en temps réel permet de recueillir aussi des données qui ne sont pas en lien direct avec la communication ou la tentative d'établissement de la communication (par ex. actualisation de la localisation). De même, pour certaines applications (par ex. MMS), les *données secondaires à conserver* ont fait l'objet d'une standardisation, mais pas les données secondaires qui doivent être transmises en temps réel (IRI).

Comme exposé dans le message du 27 février 2013 relatif à la LSCPT (cf. commentaire de l'art. 26, al. 1, let. b)[52], les fournisseurs ne doivent plus seulement livrer les données secondaires conservées des communications, connexions et accès aux réseaux qui ont été établis, mais aussi celles des tentatives d'établissement de la communication.

Dans le cas de services de téléphonie et multimédia, on parle de tentative d'établissement de la communication lorsque la liaison est bel et bien établie mais que l'appel reste sans réponse ou que le service de gestion du réseau intervient. Les deux exemples qui suivent permettent d'illustrer ces deux cas de figure: dans le premier cas, l'usager compose un numéro valable, laisse sonner brièvement et raccroche aussitôt; dans le deuxième cas, l'usager compose un numéro valable et entend un message lui indiquant que l'interlocuteur ne peut pas être joint pour le moment. Si dans ce second exemple, l'appelant est directement redirigé vers une messagerie vocale, on considère alors qu'il s'agit d'une communication, et plus d'une simple tentative. Il convient de noter que la composition d'un numéro incomplet ou d'un

52 FF **2013** 2739

numéro non valable ne constitue pas une tentative d'établissement d'une communication ni, a fortiori, une communication.

En ce qui concerne les services de courrier électronique et les services de messagerie, il n'existe pas de tentatives d'établissement de la communication, car la transmission réussie d'un courriel ou d'un message au serveur de courrier électronique ou de messagerie est déjà en soi une communication, même si la remise du courriel ou du message au destinataire devait ensuite échouer. Par conséquent, on ne parle pas non plus de tentatives d'établissement de la communication pour les autres services de télécommunication et les services de communication dérivés.

Les personnes obligées de collaborer ne doivent néanmoins conserver les données secondaires de ces tentatives d'établissement de communications que dans les limites définies par l'art. 50, al. 4. Lorsqu'une tentative d'appel est interrompue par un autre réseau avant même que le signal n'atteigne le réseau de la personne obligée de collaborer (dans ce cas, le téléphone appelé ne sonne pas), celle-ci ne peut pas conserver les données secondaires de cette tentative d'établissement d'une communication pour la simple et bonne raison que ces informations ne sont techniquement pas disponibles.

Il peut par ailleurs arriver que des communications ou des tentatives d'établissement de communications ne contiennent que des ressources d'adressage incomplètes ou que certaines ressources d'adressage fassent défaut. Lors d'appels émanant de l'étranger, le numéro de l'appelant peut parfois être incomplet ou manquer tout simplement. En cas de surveillance rétroactive, il ne serait pas possible de trouver les données secondaires conservées concernant ce numéro étranger (target ID), puisque le numéro surveillé (target ID) ne figurerait pas dans les données secondaires conservées ou seulement de manière incomplète.

Les *données secondaires conservées* décrites dans tous les types de surveillance rétroactive (art. 60 à 66) se fondent sur la norme ETSI TS 102 657.

Art. 60 Type de surveillance HD_28_NA: surveillance rétroactive des données secondaires de services d'accès au réseau

Le type de surveillance défini dans cet article correspond à l'actuel type PS 5 et a pour objet la surveillance rétroactive d'un accès à Internet. Concrètement, elle consiste en la transmission des données secondaires conservées concernant les communications émises ou reçues via le service d'accès au réseau faisant l'objet de la surveillance.

Les *let. a* à *i* énumèrent les données que les personnes obligées de collaborer doivent conserver et livrer: la date et l'heure de l'établissement de l'accès au réseau, ainsi que le moment de la déconnexion (*let. a*), à défaut du moment de la déconnexion, il est aussi possible d'indiquer la durée de l'accès; le type (par ex. xDSL, modem câble, WLAN, communication mobile) et le statut (connexion établie avec succès) de l'accès au réseau (*let. b*); l'identifiant utilisé pour l'authetification de l'usager au point d'accès surveillé, par ex. le nom d'utilisateur (*let. c*); les adresses ou plages d'adresses IP attribuées à la cible par le fournisseur d'accès au réseau, ainsi que leur type (*let. d*); pour autant que ces données soient disponibles, les identifiants des équipements terminaux de la cible (let. *e*); les volumes de données téléchargées et téléversées pendant la session (*let. f*).

Les données de localisation (*let. g et h*) correspondent soit à l'emplacement de l'antenne que la cible mobile utilise pour accéder au réseau via un service à commutation de paquets, soit à l'emplacement du point d'accès au réseau WLAN dont

se sert la cible. Doivent être livrées les données de localisation au début et à la fin de chaque session intervenue pendant la période de surveillance indiquée, c'est-à-dire le moment du début et de fin de la session (dès lors que ces moments sont compris dans la période précisée sur l'ordre de surveillance). Pour autant que ces informations soient disponibles, il y a lieu de fournir également les données de localisation pendant la session.

Dans le cas d'accès au réseau via le réseau mobile, en plus des données selon les let. a à f, les données de localisation à la fin de la session (*let. g*). Pour la transmission des données de localisation selon la let. g, la personne obligée de collaborer a le choix entre trois options.

Pour les accès au réseau via un WLAN public (*let. h*), il y a lieu de transmettre, en plus des indications selon les let. *a* à *f*, les informations suivantes:

- le BSSID (adresse MAC du point d'accès);
- si disponible, le SSID (sous une forme lisible par l'homme);
- si disponible, les données de localisation sous la forme des coordonnées géographiques ou de l'adresse postale du point d'accès au réseau WLAN utilisé par la cible;
- le nom d'utilisateur, tel que les personnes obligées de collaborer en ont pris connaissance (vérification non nécessaire);
- le type d'authentification de l'usager (par ex. SMS, EAPSIM, bon);
- les informations supplémentaires disponibles concernant l'authentification de l'usager (numéro de téléphone, adresse MAC, le cas échéant l'IMSI, l'identifiant utilisateur et le mot de passe utilisés pour l'authentification); et
- l'adresse IP du point d'accès au réseau WLAN.

Si disponibles, il convient de transmettre des données de localisation supplémentaires de la navigation maritime (nom et numéro du navire) ou aérienne (code de la compagnie aérienne, numéro d'immatriculation de l'aéronef selon le registre matricule, numéro du vol de la compagnie aérienne).

En cas d'accès au réseau via le réseau fixe, doivent être livrées, en plus des données selon les let. *a* à *f*, les ressources d'adressage de l'accès au réseau et, si ces données sont disponibles, leur adresse postale.

Art. 61 Type de surveillance HD_29_TEL: surveillance rétroactive des données secondaires de services de téléphonie et multimédia

Le type de surveillance défini dans cet article se fonde sur l'actuel type CS 4 (surveillance d'un service téléphonique), étendu aux services multimédia. Il a pour objet la surveillance rétroactive de services de téléphonie et multimédia. En d'autres termes, il consiste en la transmission des données secondaires conservées concernant ces services. Les termes « services de téléphonie et multimédia » et « services convergents » sont expliqués dans le commentaire de l'art. 57. Une explication du terme « tentative d'établissement de la communications » figure dans les remarques introductives à la section 10 (voir ci-dessus).

Dans ce type de surveillance, le fournisseur du service téléphonique doit aussi livrer les données secondaires des liaisons sortantes – y compris les tentatives d'établissement de liaisons – établies via un raccordement sur lequel est activée l'option du libre choix du fournisseur (*carrier selection*), telle que définie dans le

commentaire de l'art. 57. La personne obligée de collaborer doit être en mesure de reconnaître la correspondance avec les numéros E.164, même lorsque les numéros se présentent sous différents formats (national, international).

Alors que dans une surveillance en temps réel, les services MMS sont surveillés en même temps que l'accès au réseau, dans une surveillance rétroactive ils sont surveillés en tant qu'application, dans le cadre du type de surveillance réglé dans cet article, et non en tant que mesure de surveillance propre.

Il existe deux types de structure standard pour la livraison des données historiques de communications téléphoniques et multimédia. Les détails de chacune d'elles ne sont toutefois pas présentés ici.

Les données de localisation correspondent à l'emplacement de l'antenne que la cible mobile utilise pour accéder au réseau via un service à commutation de paquets, à l'emplacement du point d'accès au réseau WLAN dont se sert la cible ou au point d'accès au réseau dans le cas de services multimédia. Doivent être livrées les données de localisation au début et à la fin de chaque communication et tentative d'établissement de communication intervenues pendant la période de surveillance indiquée, c'est-à-dire le moment de début et de fin de la liaison ou de la tentative correspondante (dès lors que ces deux moments sont compris dans la période précisée sur l'ordre de surveillance). Pour autant que ces informations soient disponibles, il y a lieu de fournir également les données de localisation pendant la communication ou la tentative d'établissement. S'agissant de services multimédia, la session compte commune communication. Bei Multimediadiensten gilt die Sitzung als Kommunikation. Si disponibles, il convient de transmettre des données de localisation supplémentaires de la navigation maritime (nom et numéro du navire) ou aérienne (code de la compagnie aérienne, numéro d'immatriculation de l'aéronef selon le registre matricule, numéro du vol de la compagnie aérienne).

Les *let. a* à *i* énumèrent les données que les personnes obligées de collaborer doivent conserver et livrer, à savoir:

a. la nature de la communication (par ex. téléphonie fixe à commutation de circuit, téléphonie mobile à commutation de circuit, SMS, MMS, réseau fixe multimédia, réseau mobile multimédia), la date et l'heure de début et éventuellement de fin (non requises par ex. pour les SMS et les MMS) de la communication ou, à défaut, sa drée. Dans le cas de tentatives d'établissement de communications, il y a lieu d'indiquer leur nature, ainsi que la date et l'heure de début;

b. les ressources d'adressage (par ex. MSISDN, numéro E.164, SIP URI, IMPU) de tous les participants à la communication et leurs rôles respectifs (par ex. appelant, appelé, auteur du transfert, destinataire du transfert);

c. le motif pour la fin de la communication ou de la tentative d'établissement de la communication (par ex. normal, occupé, pas de réponse et pour le protocole SIP, le code s'y rapportant);

d. dans le cas de services de communication mobile (s'agissant de services multimédia, si ces données sont disponibles): l'IMEI de l'équipement terminal de la cible et l'IMSI de la cible;

e. le cas échéant, le type de service support (par ex. voix, données, fax);

f. dans le cas de SMS et de MMS, des informations sur l'événement (message texte ou message multimédia), le type (uniquement pour les SMS) et le statut;

g. dans le cas de services de communication mobile, les données de localisation de la cellule utilisée au début et à la fin de la communication ou de la tentative d'établissement de la communication:
   1. les identifiants de cellule et de zone géographique, les coordonnées géographiques et, le cas échéant, les directions principales d'émission et les adresses postales, ou
   2. les positions de la cible calculées par le réseau (exprimées sous la forme, par ex., de coordonnées géographiques accompagnées de la valeur d'incertitude correspondante ou de polygones, avec indication des coordonnées géographiques de chaque point de polygonation), ainsi que les adresses postales correspondantes ou
   3. d'autres indications, selon les normes internationales, concernant les positions de la cible ou des cellules utilisées par la cible, ainsi que les adresses postales correspondantes;

h. dans le cas de services multimédia:
   1. l'adresse IP du client, avec précision du type, et le numéro de port,
   2. l'identifiant de corrélation généré pour la communication,
   3. les types de contenus multimédia,
   4. les informations sur les composantes multimédia (heure, nom, description, initiateur, identifiant de corrélation généré pour l'accès), et
   5. le cas échéant, les informations sur les services IMS (type de service utilisé, rôle de l'élément réseau dont sont issues les données secondaires, etc.);

i. dans le cas de services multimédia, les informations sur l'accès au réseau utilisé par la cible:
   1. le type d'accès (par ex. 3GPP E-UTRAN TDD),
   2. la classe d'accès (par ex. 3GPP HSPA),
   3. si les informations sur l'accès sont issues du réseau (les données de localisation qui ne proviennent pas du réseau, mais qui pourraient être issues de l'équipement terminal ou d'une application présentent une fiabilité moindre car elles sont susceptibles d'être falsifiées), et
   4. les données de localisation ci-après relatives à l'accès au réseau au début et la fin de la session multimédia et, si ces données sont disponibles, aussi pendant la session:
      - en cas d'accès au réseau via le réseau de communication mobile, les données de localisation de la cellule utilisée par la cible selon la let. g, ou
      - en cas d'accès au réseau via le réseau WLAN, les données de localisation disponibles pour le point d'accès au réseau WLAN utilisé par la cible (coordonnées géographiques, adresse postale), ou
      - en cas d'accès au réseau via le réseau fixe, l'adresse postale disponible pour l'accès utilisé par la cible.

Art. 62 Type de surveillance HD_30_EMAIL: surveillance rétroactive des données secondaires de services de courrier électronique

Le type de surveillance défini dans cet article correspond à l'actuel type PS 6 (surveillance rétroactive d'un service postal électronique asynchrone). Les *let. a* et *b* énumèrent les données que les personnes obligées de collaborer doivent conserver et livrer. Dans ce type de surveillance, l'accent est mis sur deux catégories d'événements: d'un côté, la réception et l'envoi de messages; de l'autre, les procédures de connexion et de déconnexion en lien avec la boîte de courrier électronique. Les informations concernant les autres événements ne doivent être conservées et livrées que dans la mesure où elles sont disponibles. Cette règle flexible tient compte du fait que l'infrastructure de nombreux fournisseurs de services de courrier électronique, qui remonte à plusieurs années déjà, devrait être adaptée pour permettre la surveillance, en plus des événements principaux, des autres événements visés dans cet article, ce qui entraînerait des charges disproportionnées. Les nouveaux systèmes doivent en revanche permettre la conservation et la transmission de toutes les données mentionnées aux let. a et b.

Art. 63 Type de surveillance HD_31_PAGING: détermination de la dernière activité constatée de l'équipement terminal mobile de la personne surveillée

Le type de surveillance HD_31_PAGING a pour objet la détermination de la dernière activité (services d'accès au réseau, ainsi que services de téléphonie et multimédia) de l'équipement terminal mobile de la personne surveillée qui a été constatée par le fournisseur de services de communication mobile. Il correspond sur le plan technique au nouveau type de recherche en cas d'urgence EP_35_PAGING, lequel se fonde sur l'actuel type de recherche urgente N1. Ce type de surveillance, qui était jusque-là réservé aux recherches de personnes disparues, pourra dorénavant aussi être ordonné dans le cadre d'une procédure pénale, conformément à l'art. 273 CPP ou à l'art. 70*d* PPM.

Art. 64 Type de surveillance AS_32_PREP_COV: analyse de la couverture de réseau préalablement à une recherche par champ d'antennes

Le type de surveillance défini dans cet article correspond à l'actuel type CS 5 (analyse du réseau pendant une recherche par champ d'antennes).

Les autorités habilitées à ordonner une surveillance peuvent, en prévision d'une recherche par champ d'antenne, demander au Service SCPT une liste des cellules de téléphonie mobile ou de points d'accès au réseau WLAN (*WLAN access points*) le plus susceptibles de couvrir un emplacement géographique donné à un moment déterminé (*al. 1*). L'emplacement géographique doit être indiqué sous la forme soit de coordonnées géographiques, soit d'une adresse postale (voir commentaire de l'art. 67, let. a, ch. 1). La fourniture d'indications supplémentaires, comme le moment de la journée, peut certes contribuer à mieux cerner la zone géographique couverte, mais n'est pas obligatoire.

L'*al. 2* précise quels renseignements les FST doivent livrer au Service SCPT.

Art. 65 Type de surveillance AS_33_PREP_REF: communications de référence ou accès au réseau de référence préalablement à une recherche par champ d'antennes

Le type de surveillance défini dans cet article correspond à l'actuel type CS 7 (analyse du réseau au moyen d'appels de référence des autorités de poursuite pénale préalablement à une recherche par champ d'antennes).

Comme le type de surveillance visé à l'art. 64, la mesure décrite dans cet article sert à préparer une recherche par champ d'antennes. Concrètement, l'autorité qui entend ordonner une recherche par champ d'antennes fournit au Service SCPT une liste de communications ou d'accès au réseau de référence afin d'identifier les cellules de téléphonie mobile et les points d'accès au réseau WLAN utilisés (*WLAN access points*).

L'*al. 2* énumère les indications que l'autorité doit transmettre au Service SCPT pour l'exécution de l'ordre. Les FST ont besoin de ces informations pour pouvoir identifier les cellules de téléphonie mobile ou les points d'accès au réseau WLAN.

L'*al. 3* décrit les recherche que les FST doivent effectuer dans leurs systèmes sur la base des critères mentionnés à l'al. 2 et précise les renseignements qu'ils doivent ensuite livrer au Service SCPT.

Art. 66 Type de surveillance AS_34: recherche par champ d'antennes

Le type de surveillance défini dans cet article correspond à l'actuel type CS 6 (recherche par champ d'antennes) et couvre désormais aussi la communication à commutation de paquets (*packet switched*, PS).

Cet article détaille les indications que les FST doivent livrer.

Il convient de signaler avant toute chose que l'exécution d'une surveillance du type AS_32_PREP_COV ou AS_33_PREP_REF n'est pas une condition préalable à une recherche par champ d'antennes du type AS_34.

L'*al. 1* circonscrit la portée de la surveillance en la limitant à deux heures au plus par ordre. Cette durée maximale, qui reprend la pratique actuelle, a été fixée pour réduire les charges liées à la surveillance, en limitant dans le temps les grands volumes de données à traiter, et pour tenir compte du principe de proportionnalité. Si les autorités de poursuite pénale veulent ordonner une surveillance plus longue, elles doivent fractionner la durée souhaitée en périodes de deux heures. Les émoluments sont perçus par ordre, pour une durée de deux heures. Si une autorité de poursuite pénale veut faire effectuer, auprès du fournisseur Y, une recherche par champ d'antennes pendant cinq heures concernant les cellules A, B et C, elle doit transmettre neuf ordres au total au Service SCPT: deux ordres de deux heures et un ordre d'une heure pour la cellule A, deux ordres de deux heures et un ordre d'une heure pour la cellule B et deux ordres de deux heures et un ordre d'une heure pour la cellule C, soit neuf ordres en tout. L'émolument prévu dans l'OEI-SCPT pour une recherche par champ d'antennes est, lui aussi, multiplié par neuf. Le tribunal des mesures de contrainte doit valider chacun des ordres. Vu que ce type de mesure touche un grand nombre de personnes, l'examen de sa proportionnalité requiert une attention particulière. A ce propos, la manière de procéder lors de l'enquête (compte tenu des prérequis techniques et des buts de l'enquête) peut également privilégier la voie où le nombre de suspects est réduit au strict minimum.

L'*al. 2* dispose que les FST doivent livrer conformément aux modalités définies aux art. 60 et 61 les données recueillies selon l'al. 1. On se réfèrera pour plus de précisions au commentaire de ces deux articles.

Section 11 Recherche en cas d'urgence et recherche de personnes condamnées

La LSCPT révisée permet désormais de surveiller la correspondance postale également en dehors d'une procédure pénale, dans le cadre d'une recherche en cas d'urgence (art. 35, al. 1, LSCPT) ou d'une recherche de personnes condamnées (art. 36, al. 1, LSCPT). Par rapport à la surveillance postale ordonnée dans le cadre d'une procédure pénale, seule diffère la procédure de transmission de l'ordre et d'autorisation de la surveillance. Il n'est cependant pas nécessaire pour autant de prévoir dans l'ordonnance des types de surveillance spécifiques ou des réglementations spéciales.

Des réglementations spéciales ont en revanche été insérées dans l'ordonnance pour les mesures de surveillance de la correspondance par télécommunication ordonnées en dehors d'une procédure pénale pour retrouver des personnes disparues (recherche en cas d'urgence, art. 35 LSCPT) ou des personnes condamnées (art. 36 LSCPT). En ce qui concerne les types de surveillance qui peuvent être ordonnés dans le cadre d'une recherche en cas d'urgence (art. 67), les surveillances portant sur des accès au réseau et celles ayant pour objet des applications ont été regroupées, contrairement à ce qui est le cas dans les surveillances usuelles. Le facteur temps est décisif dans les recherches en cas d'urgence, car la vie ou la santé d'une personne peut être sérieusement menacée. Les procédures de transmission de l'ordre au Service SCPT puis du mandat correspondant aux personnes obligées de collaborer doivent donc être le plus simples possible. Ensuite, ce type de surveillance vise à recueillir toutes les informations disponibles concernant une personne recherchée. Les personnes obligées de collaborer doivent dès lors surveiller tous les services de télécommunication qu'elles proposent en lien avec les identifiants à surveiller (target ID).

Il importe de signaler ici que conformément à l'art. 35, al. 3, LSCPT, il est possible d'avoir recours à des dispositifs techniques spéciaux de surveillance de la correspondance par télécommunication selon l'art. 269bis CPP (par ex. un IMSI-catcher) dans le cadre également d'une recherche en cas d'urgence. De la même manière, l'art. 36, al. 2, LSCPT, autorise le recours à des dispositifs techniques spéciaux selon l'art. 269bis CPP (par ex. un IMSI-catcher) ou à des programmes informatiques spéciaux de surveillance de la correspondance par télécommunication selon l'art. 269ter CPP (par ex. un GovWare) aux fins de la recherche de personnes condamnées.

Art. 67 Types de surveillance EP: recherche en cas d'urgence

Cet article remplace l'art. 16*a* de l'OSCPT dans sa teneur du 31 octobre 2001, qui règle la recherche et le sauvetage de personnes disparues. La LSCPT révisée permettra de surveiller également, dans le cadre d'une recherche en cas d'urgence, le contenu (let. b) de la correspondance par télécommunication. Les mesures autorisées par la loi

en vigueur sont les surveillances de type « paging » (let. a), c'est-à-dire la recherche de personnes proprement dite, la surveillance en temps réel des données secondaires (let. c) et la surveillance rétroactive (let. d). Ces types de surveillance sont conservés dans la nouvelle loi.

La *let. a* règle le type de surveillance « paging », utilisé pour déterminer la dernière activité constatée de l'équipement terminal mobile, et définit la composition des données que les personnes obligées de collaborer doivent livrer. Est ici visée la dernière localisation disponible, indépendamment de la technologie et du type d'accès au réseau utilisés sur l'appareil. L'*identifiant du réseau de communication mobile* est composé du code pays du réseau de communication mobile (*mobile country code*, MCC) et du code désignant le réseau lui-même (*mobile network code*, MNC). Les ch. 1 à 3 décrivent différentes méthodes de localisation. Les personnes obligées de collaborer doivent utiliser une de ces trois méthodes et communiquer les données visées. L'*adresse postale* mentionnée au *ch. 1* peut aussi consister en une description géographique analogue (par ex. un numéro de rue avec une indication kilométrique, le code postal d'une commune) de l'emplacement de la cellule. Toutes les antennes n'ont pas en effet d'adresse postale au sens propre. Le champ *direction principale d'émission* peut être vide ou, à l'inverse, contenir plusieurs valeurs et des attributs. Ainsi, s'il s'agit d'une cellule omnidirectionnelle, c'est-à-dire une cellule émettant dans toutes les directions à une puissance égale, ce champ ne contient aucune indication, alors que dans le cas de cellules complexes ou spéciales, il peut contenir, en plus des valeurs correspondant aux directions principales d'émission, une série d'attributs, par exemple le code « inh » (pour « inhouse », lorsque la cellule est située à l'intérieur d'un bâtiment) ou « tun » (pour « tunnel », lorsque la cellule possède des répéteurs pour assurer la couverture radio à l'intérieur d'un ou plusieurs tunnels).

La *let. b* définit la surveillance en temps réel du contenu et des données secondaires des télécommunications. L'autorité qui ordonne ce type de surveillance transmet, pour chaque personne obligée de collaborer et pour chaque équipement terminal recherché, un ordre au Service SCPT, qui charge ensuite les fournisseurs concernés d'exécuter la mesure. Ces derniers mettent en œuvre la surveillance conformément aux dispositions des art. 55 et 57, en fonction du type spécifique de surveillance ordonnée, de manière à couvrir tous les services qu'ils fournissent en lien avec l'équipement terminal recherché. On tient ainsi compte de l'urgence de la mesure, puisqu'il s'agit de localiser et de retrouver le plus rapidement possible des personnes dont la vie ou l'intégrité corporelle est menacée. Soumettre un mandat pour chaque service de télécommunication et service de communication dérivé à surveiller, comme c'est normalement le cas, prendrait ici trop de temps: si une personne obligée de collaborer est chargée d'exécuter un recherche urgente du type EP_36_RT_CC_IRI (let. b) portant sur le numéro MSISDN X et que le détenteur de ce numéro a souscrit, auprès de ladite personne obligée de collaborer, un abonnement mobile comprenant la téléphonie et l'accès à Internet, la personne obligée de collaborer met en œuvre une surveillance en temps réel du contenu et des données secondaires de services de téléphonie et multimédia (art. 57) pour le service de téléphonie et une surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau (art. 55) pour l'accès à Internet. Dans les recherches en cas d'urgence également, les surveillances en temps réel restent actives aussi longtemps que le Service SCPT n'a pas transmis aux personnes obligées de collaborer concernées le mandat demandant la levée de la mesure.

La *let. c* traite de la surveillance des données secondaires uniquement, c'est-à-dire sans le contenu. La procédure est la même que pour la surveillance en temps réel selon la let. b (cf. explications ci-dessus), à la différence près que chaque personne obligée de collaborer est tenue de mettre en œuvre les types de surveillance pertinents selon les art. 54 et 56, de manière à couvrir tous les services qu'elle fournit en lien avec l'équipement terminal mobile recherché.

La *let. d* règle les recherches en cas d'urgence dites rétroactives, par exemple lorsque l'équipement terminal n'est plus actif. Trois éléments distinguent cette surveillance de la surveillance selon la let. b: premièrement, il s'agit ici d'une surveillance rétroactive; deuxièmement, les personnes obligées de collaborer sont tenues de mettre en œuvre les types de surveillance pertinents selon les art. 60 et 61, de manière à couvrir tous les services qu'elles fournissent en lien avec l'équipement terminal mobile recherché; troisièmement, la transmission d'un mandat pour mettre un terme à la mesure n'est pas nécessaire, puisqu'il s'agit d'une surveillance rétroactive.

L'indemnité versée aux personnes obligées de collaborer est fonction du nombre de recherches en cas d'urgence ordonnées par les autorités pour chaque personne obligée de collaborer et pour chaque équipement terminal recherché et non du nombre de surveillances concrètement mises en œuvre.

Art. 68 Recherche de personnes condamnées

Cet article est nouveau. Il règle la recherche de personnes condamnées définie à l'art. 36 LSCPT. Trois types de surveillance peuvent être ordonnées à cette fin: une surveillance en temps réel portant sur le contenu et les données secondaires (*let. a*), une surveillance en temps réel portant sur les données secondaires uniquement (*let. b*) ou une surveillance rétroactive (*let. c*). Les types de recherches de personnes condamnées correspondent exactement aux types de surveillance. Contrairement aux recherches en cas d'urgence, il n'est dès lors pas possible de combiner ici plusieurs types de surveillance. L'ordre de surveillance doit contenir l'indication « recherche de personnes condamnées », de manière à pouvoir distinguer clairement ces mesures dans les statistiques. Si plusieurs types de surveillance doivent être mis en œuvre pour rechercher une personne condamnée, l'autorité concernée doit transmettre un ordre pour chaque type de surveillance. Il y a lieu de signaler que lors de la recherche de personnes condamnées, un émolument est perçu pour chaque type de surveillance ordonné, ainsi que pour chaque fournisseur et chaque identifiant à surveiller (target ID; voir l'OEI-SCPT).

Section 12 Identifiants externes au réseau

Art. 69

Cet article règle, de manière similaire aux art. 16*b* et 24*c* de l'OSCPT dans sa teneur du 31 octobre 2001, la surveillance des identifiants externes au réseau et les cas d'itinérance. Les identifiants externes au réseau sont des identifiants qui ne sont pas

gérés par la personne obligée de collaborer chargée d'exécuter la surveillance ou qui ne sont pas enregistrés dans son réseau.

Cette disposition s'applique aux surveillances en rapport avec une ressource d'adressage étrangère (surveillance d'un raccordement téléphonique avec un numéro d'appel étranger). Par souci de simplification, les termes « propre » et « externe » sont utilisés dans ce commentaire pour qualifier les ressources d'adressage du point de vue du fournisseur chargé de mettre en œuvre la surveillance. La surveillance en rapport avec une ressource d'adressage étrangère consiste, pour le fournisseur concerné, à surveiller des identifiants « externes » qui apparaissent dans son « propre » réseau en tant qu'intervenants dans une communication. Seules sont analysées les ressources d'adressage. Le contenu des communications en particulier ne doit pas être inspecté. Aussitôt qu'un client « propre » du fournisseur mandaté établit une communication, via une application « propre » (service de téléphonie et multimédia, service de courrier électronique), avec la ressource d'adressage « externe » surveillée, il y a lieu de surveiller ladite communication. En d'autres termes, le fournisseur doit livrer, selon le type surveillance ordonnée, les données secondaires et, le cas échéant, le contenu de la communication. Ce type de mesure est déjà utilisé couramment aujourd'hui pour surveiller un numéro de téléphone étranger, c'est-à-dire « externe » au réseau du fournisseur chargé de la surveillance.

La surveillance en rapport avec une ressource d'adressage étrangère a fait l'objet d'une standardisation pour les applications (services de téléphonie et multimédia, services de courrier électronique), mais non pour les services d'accès au réseau. Des restrictions s'appliquent en outre en ce qui concerne les identifiants à surveiller (target ID; par ex. pas d'IMSI, ni d'IMEI dans le cas de la téléphonie mobile). Compte tenu des spécificités techniques propres de chaque fournisseur et de chaque service de télécommunication à surveiller, il est souhaitable que l'autorité prenne contact avec le Service SCPT pour s'informer de la faisabilité de la mesure.

Contrairement à la pratique actuelle, il n'est pas nécessaire de faire figurer une remarque spéciale sur le mandat de surveillance.

Une autre nouveauté par rapport à la pratique actuelle concerne la standardisation des surveillances en rapport avec une ressource d'adressage étrangère dans le cas de services de courrier électronique, c'est-à-dire la surveillance de courriels adressés à un client « propre » à partir d'une adresse électronique « externe » surveillée et, inversement, l'envoi de courriels par un client « propre » à l'adresse électronique « externe » surveillée. Comme indiqué en introduction, seules doivent ici être analysées les ressources d'adressage de l'enveloppe SMTP. Pour des raisons techniques, dans ce type de mesure, la surveillance peut porter uniquement sur des opérations de serveur de messagerie, comme les procédures d'envoi et de réception de message, mais pas les accès à la boîte de messagerie « externe ».

Il y a lieu de signaler que la surveillance d'une ressource d'adressage en rapport avec l'étranger n'est pas une forme d'exploration du réseau câblé. Pour des précisions sur la notion de ressource d'adressage étrangère, on se référera au commentaire de l'art. 31 LSCPT figurant dans le message du Conseil fédéral du 27 février 2013[53].

53 FF **2013** 2444, 2445 [s.]

Chapitre 4 Dispositions finales

Art. 70 Prescriptions organisationnelles, administratives et techniques

L'*art. 70* reprend, moyennant les adaptations requises, les dispositions de l'art. 33 OSCPT dans sa teneur du 31 octobre 2001[54].

Cet article crée, avec l'art. 31, al. 3, LSCPT[55], la base légale de l'ordonnance du DFJP du 15 novembre 2017 sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT). L'ordonnance du DFJP du 15 novembre 2017 sur l'organe consultatif en matière de surveillance de la correspondance par poste et télécommunication (organe consultatif) se fonde quant à elle directement sur la LSCPT (art. 5, al. 3, LSCPT).

L'art. 70 dispose que le département édicte les dispositions techniques et administratives, mais aussi celles de nature organisationnelle, régissant la mise en œuvre de la surveillance de la correspondance par poste et télécommunication. Les prescriptions du DFJP s'appliquent tant aux fournisseurs de services de télécommunication et de services de communication dérivés, qu'aux fournisseurs de services postaux.

Selon le droit en vigueur, les modalités techniques et administratives sont fixées dans des directives du Service SCPT (art. 33, al. 1bis, OSCPT dans sa teneur du 31 octobre 2001[56]; voir www.li.admin.ch).

D'autres normes de délégation au DFJP figurent aux art. 33 (procédure de réception), 49, al. 2 (indications techniques dans l'ordre de surveillance) et 29, al. 1 (qualité des données transmises).

La *deuxième phrase* précise que le DFJP fixe les délais impartis pour la livraison des données demandées.

Art. 71 Exécution

L'*al. 1* reprend pour l'essentiel l'art. 33, al. 2, OSCPT dans sa teneur du 31 octobre 2001[57]. Grâce à cette disposition, le Service SCPT pourra continuer à mettre à la disposition des autorités habilitées à ordonner une mesure et des personnes obligées de collaborer les interfaces et les formulaires électroniques que celles-ci doivent employer. Dans un souci d'efficacité mais aussi pour éviter toute erreur, seuls peuvent être utilisés les interfaces et les formulaires électroniques du Service SCPT.

Conformément à l'*al. 2*, les formulaires électroniques pourront être remplacés ultérieurement par un accès en ligne au système de traitement du Service SCPT. Cette date n'étant pas encore connue, le Service SCPT pourra décider lui-même du moment du changement de pratique. Les formulaires continueront néanmoins d'être utilisés dans deux cas de figure: premièrement, si un accès en ligne au système de traitement n'est pas possible; deuxièmement, si le système est hors service.

54 RS **780.11**
55 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. e, FF **2013** 2445/2446
56 RS **780.11**
57 RS **780.11**

Art. 72 Abrogation d'un autre acte

L'OSCPT du 31 octobre 2001 sera abrogée avec l'entrée en vigueur de l'ordonnance entièrement révisée.

Art. 73 Modification d'autres actes

Deux autres ordonnances sont aussi partiellement modifiées:

- l'ordonnance du 17 novembre 1999 sur l'organisation du Département fédéral de justice et police (Org DFJP)[58]; est ici adapté l'art. 25.

- l'ordonnance du 9 mars 2007 sur les services de télécommunication[59]; il s'agit d'une adaptation formelle de l'art. 80.

Art. 74 Dispositions transitoires

La LSCPT contient à son art. 45 des dispositions transitoires, qu'il y a lieu d'expliciter, pour certaines d'entre elles, et de préciser par des dispositions transitoires supplémentaires. Une entrée en vigueur échelonnée des ordonnances de mise en œuvre de la LSCPT entièrement révisée n'est ainsi pas nécessaire.

Les dispositions transitoires de l'art. 74 sont structurées par ordre chronologique. Pour les al. 1 à 6, le moment déterminant est l'entrée en vigueur de l'ordonnance révisée, tandis que pour les al. 7 et 8, il s'agit de la mise en service du nouveau système de traitement, c'est-à-dire les nouvelles composantes système dont l'acquisition est prévue dans le cadre du programme « Surveillance des télécommunications ».

Conformément à l'art. 45, al. 1, LSCPT, le nouveau droit de consulter le dossier et d'accéder aux données (art. 10 LSCPT), les nouvelles règles en matière de surveillance (art. 41 LSCPT), les nouvelles dispositions relatives aux voies de droit (art. 42 LSCPT) et les nouvelles normes concernant la qualité des données transmises (art. 18 LSCPT et art. 29 OSCPT) s'appliquent aux surveillances en cours au moment de l'entrée en vigueur de la loi.

L'un des aspects de la phase de transition est que les autorités habilitées ne pourront ordonner les types de renseignements et de surveillance actuels qu'aussi longtemps que le Service SCPT pourra transmettre aux personnes obligées de collaborer le mandat correspondant avant que la nouvelle OSCPT entre en vigueur. À partir de l'entrée en vigueur de l'ordonnance révisée, les autorités ne pourront plus utiliser que les nouveaux types de renseignements et de surveillance pour leurs nouveaux ordres.

Comme un grand nombre de surveillances en temps réel ordonnées selon le droit actuel seront encore actives lors de l'entrée en vigueur de la nouvelle ordonnance, une disposition transitoire a été inscrite à l'*al. 1* pour ce type de cas. L'art. 45, al. 1, LSCPT dispose que les surveillances en cours au moment de l'entrée en vigueur de la loi se poursuivent selon le nouveau droit. Il importe néanmoins de ne pas compliquer

58 RS **780.11**
59 RS **784.101.1**

excessivement l'exécution des ces mesures[60]. C'est pourquoi il faut partir du principe que la volonté du législateur n'était pas d'appliquer les nouveaux types de surveillance aux surveillances en cours, ce qui serait en totale contradiction avec cet objectif. Aussi l'al. 1 prévoit-il que les modalités d'exécution des surveillances déjà ordonnées demeurent inchangées. Si l'on appliquait les nouveaux types de surveillance, il faudrait lever les mesures concernées et les réactiver, ce qui compliquerait nettement la progression des enquêtes en cours et ce, pour plusieurs raisons: tout d'abord, il en résulterait un surcroît de travail administratif et technique disproportionné et des coûts élevés pour les autorités, le Service SCPT et les personnes obligées de collaborer. Ensuite, avec le passage aux nouveaux types de surveillance, les autorités devraient ordonner une nouvelle fois les mesures en cours et celles-ci devraient de nouveau être autorisées par le tribunal des mesures de contrainte. De leur côté, le Service SCPT et les personnes obligées de collaborer devraient désactiver les mesures ordonnées précédemment pour activer les nouvelles. À cela s'ajoute que les surveillances en cours devraient être classées en deux catégories (anciennes et nouvelles), ce qui accroît le risque d'une perte de données.

Cette règle vaut également pour les surveillances rétroactives et les demandes de renseignements en cours lors de l'entrée en vigueur de l'OSCPT révisée.

La prolongation et la levée des mesures en cours continuent d'obéir aux types de surveillance précédemment en vigueur. Le terme prolongation désigne ici les prolongations périodiques de surveillances en temps réel conformément à l'art. 274 CPP ou 70*e* PMM. Cette procédure administrative continuera de se dérouler entre l'autorité qui a ordonné la mesure, l'instance chargée de l'autoriser et le Service SCPT. Dans un souci de simplification, ce sont là aussi les types de surveillance précédemment en vigueur qui s'appliqueront pendant la phase transitoire. Une surveillance ordonnée avant l'entrée en vigueur de l'ordonnance révisée pourra donc être prolongée selon les modalités prévues dans l'ancien droit. Comme c'est le cas à présent, les personnes obligées de collaborer auprès desquelles une surveillance en temps réel est activée ne seront pas informées d'une prolongation éventuelle.

Pour des raisons techniques, les types de surveillances en vigueur actuellement ne pourront être utilisés pour lever une mesure que tant que l'actuelle composante système utilisée par le Service SCPT pour la gestion des mandats (AMIS) sera encore en service. La nouvelle composante système ne prendra en effet en charge que les nouveaux types de surveillance. Vu néanmoins la durée moyenne d'une surveillance en temps réel, la majorité des mesures de ce type ordonnées selon l'ancien droit auront de toute façon pris fin avant le remplacement du système AMIS.

Conformément à l'*al. 2*, une fois l'ordonnance révisée en vigueur, le Service SCPT surpprimera les branchements de test mis en place selon l'ancienne pratique (voir commentaire de l'art. 30), car ils se fondent sur les anciens types de surveillance, qui ne seront guère plus testés.

La disposition transitoire de l'*al. 3* permet aux FST de soumettre une demande pour être considérés comme des FST ayant des obligations restreintes en matière de surveillance selon l'art. 51. S'il est vraisemblable que la demande sera approuvée, les FST sont considérés comme tels à partir du moment du dépôt de leur demande et

60 Cf. FF **2013** 2463, ad art. 45, al. 1, LSCPT

jusqu'à ce que le Service SCPT rende sa décision. Le but de cette disposition est de préserver les FST d'investissements inutiles pour adapter leurs systèmes en vue de garantir leur disponibilité à surveiller entre l'entrée en vigueur de la nouvelle ordonnance et la décision relative à leurs obligations. Concrètement, les FST ont trois mois à partir de l'entrée en vigueur de l'OSCPT pour soumettre leur demande. Dans sa décision ou décision incidente au sens des art. 5, 45 et 46 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA[61]), soit le Service SCPT reconnaît formellement que le FST doit être considéré comme ayant des obligations restreintes, soit, à l'inverse, il déclare que le FST est soumis à toutes les obligations. La dernière phrase de l'*al. 3* exclut d'appliquer le délai transitoire de l'art. 51, al. 5, à un groupe déterminé de FST qui ne sont plus considérés comme ayant des obligations restreintes en matière de surveillance. Les FST qui sont soumis, selon le droit en vigueur, à l'obligation d'annoncer – c'est-à-dire des FST qui doivent exécuter des obligations en matière de surveillance conformément à l'actuelle LSCPT– pourraient en effet être tentés de présenter une demande dans le seul but d'être considérés comme ayant des obligations restreintes en matière de surveillance pendant trois mois. Le Service SCPT considère ces FST comme ayant des obligations étendues en matière de surveillance et fixe individuellement les délais déterminants pour garantir l'enregistrement des données nécessaires à la surveillance et la disponibilité à surveiller.
L'*al. 4* répond au souhait des fournisseurs de disposer d'une période de transition afin, notamment, de doter leurs points de vente de services de télécommunication mobile de l'équipement technique nécessaire pour enregistrer les copies des pièces d'identité, d'adapter leurs systèmes servant à la saisie des données des clients et d'être en mesure d'assurer, par des moyens appropriés, l'identification des usagers ou, dans le cas de points d'accès au réseau WLAN exploités à titre professionnel, des utilisateurs finaux.

Conformément à l'*al. 5*, les fournisseurs tenus de conserver les données secondaires de télécommunication (voir art. 21, al. 2, let. b) doivent adapter leurs systèmes dans les six mois au plus à compter de l'entrée en vigueur de l'ordonnance révisée pour pouvoir livrer les renseignements selon les art. 38 (identification des utilisateurs dans le cas d'adresses IP qui ne sont pas attribuées de manière univoque (traduction d'adresses de réseau) et 39 (renseignements sur des procédures de traduction d'adresses de réseau); voir aussi le commentaire de l'art. 18, al. 4).

L'*al. 6* donne 24 mois aux FST – toujours à compter de l'entrée en vigueur de la nouvelle OSCPT – pour être en mesure de livrer, dans le cadre de surveillances rétroactives, les données secondaires de tentatives d'établissement de communications (*let. a*). Ce délai transitoire doit leur permettre de procéder aux adaptations requises de leurs systèmes. Les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance qui sont visés à l'art. 52 ne sont pas mentionnés ici, car ils ne possédent pas encore de systèmes de ce type. Dans leur cas, c'est le délai de 12 mois à compter de la décision du Service SCPT selon l'art. 52, al. 2, en relation avec l'art. 22, al. 5, qui s'applique. Les FST disposent aussi de 24 mois pour configurer leurs système de manière à pouvoir exécuter la surveillance de services de courrier électronique conformément aux dispositions de l'OSCPT et de l'OME-SCPT (*let. b*). L'OME-SCPT ne reconnaît pas les prescriptions propriétaires, aujourd'hui dépassées, en vigueur en Suisse pour

61 RS **172.021**

la surveillance des services de courrier électronique. Le système de traitement du Service SCPT ne les prendra en charge que durant cette période transitoire, et uniquement si les systèmes concernés étaient déjà en fonctionnement lors de l'entrée en vigueur de l'OSCPT révisée.

L'al. 7, let. a, donne la possibilité au Service SCPT d'établir les statistiques selon l'ancien droit jusqu'à la mise en exploitation des composantes système prévues dans l'étape 1 du programme relatif au développement et à l'exploitation du système de traitement pour la surveillance des télécommunications et des systèmes d'information de police de la Confédération (programme Surveillance des télécommunications[62]). Les systèmes actuels, principalement le CCIS, dont le contrat de maintenance ne peut plus être adapté, ne permettent pas d'établir les statistiques selon les règles fixées dans le nouveau droit.

La *let. b* prévoit en outre que les données relatives aux nouveaux types de renseignements (art. 27 et 35 à 48) et de surveillancs (art. 54 à 68) continueront d'être transmises avec le système, les formats et les formulaires actuels jusqu'à la mise en service du nouveau système de traitement. Les demandes de renseignements, ainsi que les mandats pour les personnes obligées de collaborer et les réponses de ces dernières, sont livrés via un moyen de transmission sûr autorisé par le Service SCPT (voir commentaire de l'art. 3, al. 1, let. a), par la poste ou par télécopie. Pour rappel, les autorités habilitées doivent utiliser les nouveaux types de renseignements et de surveillance pour les ordres et les demandes de renseignements qu'ils transmettront une fois l'ordonnance révisée en vigueur. Les surveillances ordonnées avant cette date restent demeurent inchangées (types de surveillance et formats précédemment en vigueur) dans le système utilisé actuellement. Il convient de noter que le nouveau droit s'applique aussi à ces mesures (art. 45, al. 1, LSCPT), notamment en ce qui concerne la surveillance exercée par le Service SCPT (art. 41 ss LSCPT) et la qualité des données transmises (art. 28 OSCPT).

La *let. c* est à considérer en relation avec l'al. 8. Comme le nouveau système de traitement ne sera pas encore en service au moment de l'entrée en vigueur de l'ordonnance révisée, il ne sera pas possible dans un premier temps de soumettre des demandes de renseignements avec recherche flexible de nom selon l'art. 27. Les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements disposent d'un délai de douze mois suivant l'entrée en vigueur de la nouvelle OSCPT pour adapter leurs systèmes pour ce type de recherche (al. 8). Si une autoritée habilitée selon l'art. 15 LSCPT transmet une demande de renseignements avec recherche flexible de nom à partir du moment où le nouveau système de traitement est en service, celle-ci ne pourra logiquement être exécutée que par les fournisseurs qui auront déjà procédé aux modifications requises sur leurs dispositifs.

L'al. 8 dispose qu'au plus tard 12 mois après la mise en service du nouveau système de traitement, les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de renseignements (visés à l'art. 22) adaptent leurs systèmes ou leurs logiciels pour être en mesure de livrer les renseignements selon les art. 34 à 36 et 39 à 41 de manière automatisée, via l'interface de consultation du système de traitement. Aux termes de l'art. 18, al. 3, les FST ayant des obligations restreintes en matière de surveillance (art. 51) ne sont pas tenus de livrer les

62 FF **2015** 2809

renseignements de manière automatisée via cette interface. Il peuvent néanmoins le faire de leur propre initiative.

Art. 75 Entrée en vigueur

La date d'entrée en vigueur de l'OSCPT entièrement révisée est coordonnée avec celle de la LSCPT et de ses autres ordonnances d'exécution.

Une entrée en vigueur en plusieurs étapes n'est pas nécessaire.;

Annexe

Tableau récapitulatif des obligations des FST et des FSP

Annexe au rapport explicatif relatif à la révision totale de l'OSCPT

08.09.2016		RENSEIGNEMENTS			SURVEILLANCE		
		LSCPT	OSCPT	Obligations	LSCPT	OSCPT	Obligations
Fournisseurs de services postaux (**FSP**)		____	____	____	19	14	
Fournisseurs de services de télécommunication (**FST**) art. 2, let. b, LSCPT	MODESTE[63] (ou domaine éducation[64]), art. 26, al. 6,	21/22	11, al. 2 18, al. 1 et 3 21 31 (conformité)	A	26, al. 2 et 6	11, al. 2 51	B
	NORMAL	21/22	11, al. 2 18, al. 1 et 2 19, 20 21 31 (conformité) 74 (disp. trans.)	C	26, al. 1 à 5	11, al. 2 50 31 (conformité)	D
Fournisseurs de services de communication dérivés art. 2, let. c, LSCPT	NORMAL	22, al. 3	11, al. 2 18, al. 4	E	27, al. 1 et 2	11, al. 2	F
	IMPORTANT[65] (obligations étendues)	22, al. 4	11, al. 2 18, al. 1 et 2 22 31 (conformité) 74 (disp. trans.)	G	27, al. 3 26, al. 1 à 5	11, al. 2 31 (conformité) 50 52	H

63 Réduction (Downgrade)
64 Comme demandé pendant la consultation, l'expression « domaine de l'éducation » a été remplacée dans les ordonnances par « domaine de la recherche et de l'éducation ».
65 Renforcement (Upgrade)

A. Obligations des FST ayant des obligations retreintes en matière de surveillance (FST de taille modeste) s'agissant de l'exécution de demandes de renseignements

Condition = Les FST offrent des services de télécommunication de faible importance économique ou dans le domaine de la recherche et de l'éducation (critères selon l'art. 51, al. 1 et 2, OSCPT)

- Ils ont les mêmes obligations que les FST de taille dite normale (pas de réduction des obligations), ce qui signifie qu'ils doivent garantir la disponibilité à renseigner (art. 31 et 32 OSCPT).
- Exceptions:
  - ils peuvent livrer les renseignements par écrit, en dehors du système de traitement (art. 18, al. 3, OSCPT), en d'autres termes :
    - ils ne doivent pas se raccorder à l'interface de consultation du système de traitement du Service SCPT et,
    - ils ne doivent pas livrer de manière automatisée les renseignements selon les art. 35 à 37 et 40 à 42 OSCPT et selon l'art. 27 en relation avec les art. 35, 40 et 42 OSCPT;
  - ils ne doivent pas livrer selon la procédure standardisée les renseignements selon les art. 38 et 39 OSCPT, mais uniquement sur la base des données secondaires dont ils disposent;
  - conformément à l'art. 11, al. 2, OSCPT, ils sont dispensés de l'obligation d'assurer un service de piquet.

B. Obligations des FST ayant des obligations restreintes en matière de surveillance (FST de taille modeste) s'agissant de l'exécution de surveillances, de recherches d'urgence et de recherche de personnes condamnées

Condition = Les FST offrent des services de télécommunication de faible importance économique ou dans le domaine de la recherche et de l'éducation (critères selon l'art. 51, al. 1 et 2, OSCPT)

- Ils sont libérés des obligations selon l'art. 26, al. 1 et 3 à 5, LSCPT, ils ne doivent notamment pas garantir la disponibilité à surveiller.
- Conformément à l'art. 11, al. 2, OSCPT, ils sont libérés de l'obligation d'assurer un service de piquet.
- Ils ont uniquement les obligations suivantes, conformément à l'art. 26, al. 2 et 6, LSCPT:
  - livrer les informations nécessaires à l'exécution de la surveillance;
  - tolérer la surveillance;
  - supprimer les cryptages qu'ils ont opérés;
  - livrer, sur demande, les données secondaires de télécommunication de la personne surveillée dont ils disposent.

C. Obligations des FST (de taille normale) s'agissant de l'exécution de demandes de renseignements

- Livrer des renseignements sur les services de télécommunication (art. 21 LSCPT).
- Livrer des renseignements visant à identifier les auteurs d'infractions par Internet (art. 22 LSCPT).
- Garantir la disponibilité à renseigner (art. 31 et 32 OSCPT).
- Livrer tous les types de renseignements via l'interface de consultation du système de traitement du Service SCPT.

- Livrer les renseignements selon les art. 38 et 39 OSCPT.
- Livrer de manière automatisée les renseignements selon les art. 35 à 37 et 40 à 42 OSCPT et selon l'art. 27 en relation avec les art. 35, 40 et 42 OSCPT.
- Respecter les délais de conservation des données selon les art. 21, al. 2, et 22, al. 2, LSCPT et selon l'art. 21 OSCPT.
- Assurer un service de piquet conformément à l'art. 11, al. 2, OSCPT.

Autorisation:

- Livrer manuellement les renseignements selon les art. 38, 39 et 43 à 48 OSCPT et selon l'art. 27 en relation avec l'art. 43 OSCPT.

D. Obligations des FST (de taille normale) s'agissant de l'exécution de surveillances, de recherches d'urgence et de recherche de personnes condamnées

- Exécuter les obligations selon l'art. 26 LSCPT:
    - livrer le contenu des télécommunications de la personne surveillée;
    - livrer les données secondaires de télécommunication de la personne surveillée;
    - livrer les informations nécessaires à l'exécution de la surveillance;
    - tolérer la surveillance;
    - supprimer les cryptages qu'ils ont opérés;
    - conserver pendant six mois les données secondaires de télécommunication.
- Garantir la disponibilité à surveiller (art. 31 et 32 OSCPT).
- Assurer un service de piquet conformément à l'art. 11, al. 2, OSCPT.
- Exécuter les obligations en matière de surveillance selon l'art. 50 OSCPT.

E. Obligations des fournisseurs de services de communication dérivés (de taille normale) s'agissant de l'exécution de demandes de renseignements

- Livrer au Service les indications dont ils disposent en vue de l'identification d'auteurs d'infractions par Internet (art. 22, al. 3, LSCPT).
- Conformément à l'art. 11, al. 2, OSCPT, ils sont dispensés de l'obligation d'assurer un service de piquet.
- Ils ne sont pas liés par les types de surveillance standardisés, mais livrent sans exigences de formes les données dont ils disposent (art. 18, al. 4, OSCPT).

F. Obligations des fournisseurs de services de communication dérivés (de taille normale) s'agissant de l'exécution de surveillances, de recherches d'urgence et de recherche de personnes condamnées

- Exécuter les obligations selon l'art. 27, al. 1, LSCPT:
    - tolérer les surveillances (garantir l'accès à leurs installations et livrer les informations nécessaires à l'exécution de la surveillance);
    - livrer, sur demande, les données secondaires de télécommunication de la personne surveillée dont ils disposent.

- Conformément à l'art. 11, al. 2, OSCPT, ils sont dispensés de l'obligation d'assurer un service de piquet.

G. Obligations des fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements (fournisseurs de grande taille) s'agissant de l'exécution de demandes de renseignements

Condition = Les fournisseurs offrent des services d'une grande importance économique ou à un grand nombre d'utilisateurs (critères selon l'art. 22, al. 1 et 2, OSCPT).

- Ils ont les mêmes obligations que les FST de taille dite normale s'agissant de l'exécution de demandes de renseignements.
- Livrer des renseignements sur des services de communication dérivés (art. 21 LSCPT par analogie).
- Livrer des renseignements visant à identifier les auteurs d'infractions par Internet (art. 22 LSCPT).
- Garantir la disponibilité à renseigner (art. 31 et 32 OSCPT).
- Livrer tous les types de renseignements via l'interface de consultation du système de traitement du Service SCPT.
- Dans la mesure où ils ont aussi des obligations étendues en matière de surveillance (conservation des données secondaires), livrer les renseignements selon les art. 38 et 39 OSCPT (livraison possible aussi manuellement).
- Livrer de manière automatisée les renseignements selon les art. 35 à 37 et 40 à 42 OSCPT et selon l'art. 27 en relation avec les art. 35, 40 et 42 OSCPT.
- Respecter les délais de conservation des données selon les art. 21, al. 2, et 22, al. 2, LSCPT et selon l'art. 21 OSCPT.
- Conformément à l'art. 11, al. 2, OSCPT, ils sont dispensés de l'obligation d'assurer un service de piquet.
- Livrer manuellement les renseignements selon les art. 43 à 48 OSCPT et selon l'art. 27 en relation avec l'art. 43 OSCPT.

H. Obligations des fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance (fournisseurs de grande taille) s'agissant de l'exécution de surveillances, de recherches d'urgence et de recherche de personnes condamnées

Condition = Les fournisseur offrent des services d'une grande importance économique ou à un grand nombre d'utilisateurs (critères selon l'art. 52, al. 1 et 2, OSCPT).

- Ils ont les mêmes obligations que les FST de taille dite normale s'agissant de l'exécution de surveillances, de recherches d'urgence et de recherche de personnes condamnées (art. 27, al. 3, LSCPT).
- Exécuter les obligations selon l'art. 26, al. 1 à 5, LSCPT:
  - livrer le contenu des télécommunications de la personne surveillée;
  - livrer les données secondaires de télécommunication de la personne surveillée;
  - livrer les informations nécessaires à l'exécution de la surveillance;
  - tolérer la surveillance;
  - supprimer les cryptages qu'ils ont opérés;
  - conserver pendant six mois les données secondaires de télécommunication.
- Garantir la disponibilité à surveiller (art. 31 et 32 OSCPT).

- Assurer un service de piquet conformément à l'art. 11, al. 2, OSCPT.
- Exécuter les obligations en matière de surveillance selon l'art. 50 OSCPT.