Rapport explicatif **Projet de mars 2017**

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, correspondance postale, télécommunications et dispositions finales. 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 décrites 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 dans le domaine des télécommunications, afin de favoriser l'automatisation des procédures.

Une autre différence est que la nouvelle ordonnance 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 63).

À l'occasion de la révision totale de la loi, 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

1 RS **780.1**

une communication unilatérale (par ex. mise en ligne d'un document) ou multilatérale (par ex. courrier électronique, 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].

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. D'abord parce que la nouvelle loi donne au Conseil fédéral la possibilité 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 (voir commentaire de l'art. 49). 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 renseignement et de surveillance, notamment s'ils offrent des services d'une grande importance économique ou à un grand nombre d'utilisateurs. 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. 50) 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 communication dérivés et de services de télécommunications 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). 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 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 pourra lui aussi demander tous types de renseignements au Service SCPT.

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. 27). 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,

---

2 RS **784.10**

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 24 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 commentaire des art. 29 à 32).

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[3] (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[4] pour tenir compte de l'art. 15, al. 2, let. a et b, LSCPT : le Service de renseignement de la Confédération (SRC; *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)[5] du 17 décembre 2010[6];

- *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)[7];

---

3 RS **780.11**
4 RS **780.11**
5 RS **783.0**
6 Voir le message du 27 février 2013 concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), ad. art. 2, let. a, FF **2013** 2402 in fine

- *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)[8];

- *let. k* : les exploitants de réseaux de télécommunication internes[9];

- *let. l* : les personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers[10];

- *let. m :* les revendeurs professionnels de cartes ou de moyens semblables qui permettent l'accès à un réseau public de télécommunication[11].

Art. 2 Termes et abréviations

L'art. 2 se fonde sur l'art. 2 de l'OSCPT du 31 octobre 2001[12] 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'*art. 3, 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. 47). Le détenteur du rôle OrgAdmin gère ensuite de manière autonome dans le système de traitement les droits d'accès des membres de son organisation pour les différentes mesures de surveillance, conformément aux

7 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
8 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. c, FF **2013** 2403 in fine
9 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. d, FF **2013** 2404 in fine
10 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. e, FF **2013** 2405
11 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. f, FF **2013** 2405
12 RS **780.11**

indications de l'autorité qui les a ordonnées (cf. à cet égard les art. 8 et 9 de l'ordonnance du xx xxxx sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication[13] [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. 47).

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. Aucun nouvel émolument n'est en revanche 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 DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT ; voir aussi le commentaire de l'art. 70).

La *let. b* autorise une transmission des documents par poste ou télécopie, 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.

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[14], l'*art. 4* règle la mise en œuvre de la surveillance.

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

---

13 RS **XX.XXX**
14 RS **780.11**

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.

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[15]. Il a pour objet la protection du secret professionnel et du secret de fonction. Il y a lieu de 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

15 RS **780.11**

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 et art. 70*b*, al. 1 PPM) »[16].

Aux termes des art. 15, let. j et k (correspondance par poste), et 46, 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[17]. 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'aucun tri n'a été ordonné.

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 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 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

16 FF **2013** 2421 ; voir aussi le commentaire des art. 271 CPP et 70*b* PPM dans le message concernant la LSCPT

17 FF **2013** 2392, ch. 1.4.5

supprime toutes les autres données[18]. 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 (SRC) 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[19]. 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 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.

---

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

19 RS **780.11**

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[20]. 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 doit être 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 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 d'exécution du ou des mandats par les personnes obligées de collaborer (avec indication de la date et de l'heure), les décisions de

20 FF **2013** 2424

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[21].

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. 22 et 25. 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.

21 RS **172.220.111.3**

L'*al. 2* définit quant à lui les prestations des personnes obligées de collaborer. Dans un souci de proportionnalité, les FST ayant des obligations restreintes en matière de surveillance (art. 49), 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. 50) 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.

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 en vigueur pour la surveillance de la correspondance postale et à l'art 13, al. 1, let. j, de la LSCPT en vigueur pour la surveillance de la correspondance par télécommunication.

Introduit par le Conseil des États le 10 mars 2014, l'art. 16, let. k, de la LSCPT entièrement révisée 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 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. 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[22]). L'*al. 2* ne contient pas finalement de disposition concernant le nombre de surveillances qui n'ont pas été autorisées (comme demandé par les

22 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**

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 actuelle 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, du code de procédure pénale (CPP)[23], s'agissant des ministères publics, et les nouveaux art. 70*bis*, al. 2, et 70*ter*, al. 4, de la procédure pénale militaire du 23 mars 1979[24] (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[25]). 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 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

23 RS **312.0**
24 RS **322.1**
25 RS **322.2**

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. L'*al. 3* prévoit une fréquence annuelle pour la publication de ces statistiques. 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.

La question des coûts de l'utilisation de dispositifs techniques et de programmes informatiques spéciaux est, elle, légèrement plus problématique. Les programmes informatiques de ce type sont généralement achetés une fois afin d'être utilisés dans différentes procédures, moyennant des adaptations. Certains modèles de coûts prévoient en outre des frais de licence pour chaque utilisation, sans oublier les coûts, très difficiles à chiffrer, concernant notamment le personnel nécessaire pour préparer l'installation de GovWare (policiers, informaticiens, traducteurs, etc.). Au vu de toutes ces difficultés, 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[26]. 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 commentaire dans le message relatif à la LSCPT[27], ainsi que le commentaire de l'art. 16 ci-après.

26 RS **780.11**
27 FF **2013** 2425-2427

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[28]. 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. 47).

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[29]. 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 qu'il faut désormais aussi indiquer, s'il est connu, le lieu d'expédition de l'envoi postal (cf. let. b, ch. 4). 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.

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.

28 RS **780.11**
29 SR **780.11**

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

Art. 17 Demandes de renseignements

La fourniture de renseignements (par ex. pour identifier un usager) se déroule normalement de la manière suivante : le fournisseur commence par chercher, généralement dans les données relatives à ses clients, mais aussi dans les données secondaires de télécommunication conservées, 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 et les services de télécommunication ou les services de communication dérivés qu'ils ont utilisés.

L'*al. 1* dispose que les autorités habilitées doivent transmettre leurs demandes de renseignements via le système de traitement et que les personnes obligées de collaborer doivent elles aussi utiliser ce système pour livrer les données demandées. L'utilisation de tout autre moyen de transmission (par ex. courriel, lettre, téléphone ou fax) n'est admise que si le système de traitement n'est pas disponible pour des raisons techniques ou s'il s'agit d'une exception au sens de l'art. 18, al. 3 ou 4.

Selon l'*al. 2*, 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

Aux termes de l'*al. 1*, les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements (art. 21) doivent être en mesure de répondre aux demandes de renseignements (art. 33 à 46). L'art. 48, al. 1, fixe les obligations correspondantes en matière de surveillance.

Les demandes de renseignements selon les sections 4 et 5 du chapitre 3 (art. 33 à 41) sont traitées via une interface électronique du système de traitement, au moyen d'une procédure automatisée. Pour certains types de renseignements (art. 42 à 46), un traitement manuel est néanmoins possible (*al. 2 in fine*). Même si la demande n'est pas traitée selon une procédure automatisée, les renseignements doivent tout de même être livrés via le système de traitement.

L'*al. 3* permet aux FST ayant des obligations restreintes en matière de surveillance selon l'art. 49 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.

L'*al. 4* 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. 21), les exploitants de réseaux de télécommunication internes (art. 1, al. 2, let. k) – doivent uniquement livrer par écrit les renseignements en leur possession.

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. 5*). 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 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. 22, al. 1.

Art. 19 Saisie d'indications relatives aux personnes

L'*art. 19* reprend les dispositions notamment de l'art. 19*a* l'OSCPT dans sa teneur du 31 octobre 2001[30]. 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[31].

Conformément à l'al. 1, il faut veiller, lors de l'activation de moyens d'accès à des services de télécommunication ou à des services de communication dérivés, à identifier les utilisateurs par des moyens appropriés. 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 dans le cas d'une carte SIM intégrée dans l'équipement terminal mobile (embedded SIM). 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). Sont considérés des moyens d'identification appropriés, par exemple, une carte de crédit ou un numéro de téléphone mobile, sur lequel est ensuite envoyé à l'usager un code d'accès par SMS.

L'al. 2 prévoit que l'identité des usagers de services de téléphonie mobile doit être vérifiée au moyen d'un passeport, d'une carte d'identité ou d'un titre pour étrangers au sens des art. 71 et 71a de l'ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative (OASA)[32].

La vérification de l'identité à l'aide d'un document officiel est donc impérative pour la téléphonie mobile. Cette règle, qui vaut déjà pour les usagers de services de téléphonie mobile à prépaiement, est désormais étendue aux usagers qui souscrivent un abonnement. On relèvera néanmoins que la production d'une pièce d'identité est demandée depuis longtemps déjà lors de la conclusion d'un abonnement. Les prescriptions relatives à l'identification des usagers sont légèrement plus strictes en ce qui concerne les services de téléphonie mobile, notamment parce que les services de ce type sont très largement diffusés et parce que d'autres services doivent pouvoir procéder à des identifications indirectes sur la base des indications enregistrées.

---

30 RS **780.11**
31 FF **2013** 2429-2430
32 RS **142.201**

Les données personnelles doivent être saisies telles qu'elles figurent sur la pièce d'identité produite (art. 23, al. 1, LSCPT). 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. 21 et les revendeurs visés à l'art. 2, let. f, LSCPT doivent veiller à une saisie correcte des données de l'usager au moyen de la pièce d'identité produite. La copie de la pièce d'identité permet de contrôler l'exactitude des données enregistrées. Quant aux données qui ne figurent pas sur la pièce d'identité (par ex. l'adresse), elles seront 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. 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**][33] et la future loi eID)[34] (voir l'art. 23, al. 1, LSCPT).

Le fournisseur doit enregistrer dans son système une copie électronique – photographie ou copie numérisée – parfaitement lisible de la pièce d'identité du client (al. 2, deuxième phrase). Il n'est pas nécessaire d'en conserver une copie sur papier (voir l'art. 23, al. 1, LSCPT).

L'*al. 3* précise quelles indications doivent être saisies dans le cas de personnes morales. L'art. 19*a* OSCPT dans sa teneur du 31 octobre 2001[35] 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 correspondant à la pratique actuelle. La seule nouveauté concerne la profession, qui doit désormais être indiquée si elle est connue (art. 21, al. 1, let. a, LSCPT).

L'*al. 4* énumère les données à saisir dans le cas de personnes morales. L'expression « personne physique responsable » figurant à la *let. c* se réfère à la personne physique habilitée à représenter la personne morale selon l'inscription au registre du commerce. Il peut s'agir d'une personne différente de la personne responsable au sens du code des obligations et de l'utilisateur du service de téléphonie mobile (par ex. un collaborateur). Pour ces derniers, il suffit de saisir les nom et prénom, dès lors qu'ils sont connus (*let. d*).

---

33 RS **943.03**
34 https://www.egovernment.ch/fr/umsetzung/schwerpunktplan/elektronische-identitat/
35 RS **780.11**

En application de l'*al. 5*, 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 commerciales sans abonnement (services à prépaiement). 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[36]. Conformément à l'art. 1, let. b, de l'ordonnance du 9 mars 2007 sur les services de télécommunication (OST)[37], 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. 20 Délais de conservation

L'*art. 20* 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* 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. 19, al. 1 à 3.

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, comme le numéro IMEI, l'adresse MAC (voir les art. 34, al. 1, let. d, et 39, al. 1, let. d), ainsi qu'aux indications selon les art. 35, al. 1, 36, al. 1, et 37, al. 1.

Voir également les dispositions transitoires de l'art. 45, al. 3, LSCPT.

Art. 21 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. La loi impose des obligations restreintes en matière de surveillance des télécommunications aux fournisseurs traditionnels de ce type de services. Ceux-ci doivent uniquement tolérer la surveillance et livrer les indications dont ils disposent qui sont nécessaires pour mettre en œuvre la surveillance. Il peut

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

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 lorsqu'il a dû traiter 50 demandes de renseignements au cours des douze derniers mois (la date de référence étant fixée au 30 juin) ou qu'il a enregistré un chiffre d'affaires annuel d'au moins 100 millions de francs pendant deux exercices consécutifs. Ce deuxième critère 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 clients 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 réalisent 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.

Aux termes de l'*al. 4*, 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 du moment où sont vérifiées les conditions selon l'al. 1, c'est-à-dire dès que le fournisseur constate qu'il remplit les conditions fixées à la let. a ou b. Le Service SCPT apporte son soutien aux fournisseurs dans l'accomplissement de leurs obligations en leur dispensant des conseils.

Art. 22 Surveillances et renseignements spéciaux

Tous les types de renseignements et de surveillance courants sont énumérés aux art. 23 et 24. Les dispositions s'y rapportant figurent respectivement dans les sections 4 à 6 (art. 33 à 46) et 8 à 11 (art. 52 à 68) du chapitre 3.

Les renseignements et les surveillances qui ne sont pas mentionnés expressément dans l'ordonnance, ainsi que, provisoirement, les surveillances selon les art. 58 ou 59, 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[38]. 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. La même règle vaut pour les fournisseurs qui recourent à des tiers ou des auxiliaires pour donner suite aux demandes de renseignements ou exécuter des surveillances (*al. 2*).

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. 23 Types de renseignements

L'*art. 23* donne un bref aperçu des différents types de renseignements qu'il est possible de recueillir et qui sont réglés en détail aux sections 4 à 6 du chapitre 3 (art. 33 à 46). 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 selon les art. 33 à 40 présentent une densité normative élevée, nécessaire pour permettre un traitement automatisé de ces demandes. Ils correspondent en substance aux actuels renseignements simples « A0 ». Vu le très grand nombre de demandes qui sont transmises au Service SCPT concernant cette catégorie de renseignements (à titre indicatif, 181 835 demandes en 2015[39]) un traitement automatisé est indispensable.

Cette automatisation requiert des règles précises, notamment en ce qui concerne les différents paramètres et types de données. Ces règles sont fixées dans l'ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT) (art. 31, al. 3, LSCPT).

À côté de ces types de renseignements régis par un cadre très formel (art. 40 à 46), on trouve d'autres renseignements qui peuvent aussi être livrés via une procédure manuelle.

La procédure de transmission des demandes est identique pour tous les types de renseignements : les autorités habilitées selon l'art. 15 LSCPT soumettent leur demande au Service SCPT, qui la transmet aux personnes obligées de collaborer. Ces dernières livrent les renseignements demandés au Service SCPT, qui les fait parvenir à son tour à l'autorité à l'origine de la demande. Dans la mesure où la

38 RS **780.11**
39 Statistiques du Service SCPT, disponibles sur le site www.li.admin.ch/fr/themes/statistiques

technique le permet, tant la demande que les résultats sont transmis de manière automatisée, via le système de renseignements du Service SCPT.

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 téléphonie 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. 33 et 38) et celles visant les « renseignements sur les services » (art. 34 et 39). 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. 35 à 37) visant à identifier les auteurs d'infractions par Internet (art. 22 LSCPT).

Art. 24 Types de surveillance

L'*art. 24* donne quant à lui un bref aperçu des différents types de surveillance, qui sont réglés en détail aux sections 8 à 11 du chapitre 3 (art. 52 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 prévis, données secondaires de télécommunication conservées concernant des communications passées), le contenu des télécommunications n'est pas enregistré et ne peut dès lors

pas être transmis (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_16_NA_CC_IRI, pour l'accès Internet mobile ; la seconde, du type RT_18_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 téléphonie 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.

Art. 25 Non-standardisation

Lorsqu'il standardise un type de renseignements ou de surveillance, le DFJP inscrit dans l'OME-SCPT, c'est-à-dire une ordonnance du département, les modalités concrètes d'ordre technique et administratif régissant le type de renseignements ou de surveillance en question (pour des précisions sur les termes « type de renseignements » et « type de surveillance » voir le commentaire respectivement de l'art. 23 et de l'art. 24). La standardisation est subordonnée à deux conditions : premièrement, il doit exister une norme internationale portant sur les renseignements ou la surveillance concernés ; deuxièmement, la standardisation doit être faisable et ne pas demander une charge de travail disproportionnée.

Si ces conditions ne sont pas remplies pour un type de renseignements ou de surveillance déterminé lors de l'entrée en vigueur de l'ordonnance, le DFJP renonce à une standardisation dans un premier temps.
Conformément à l'art. 31, al. 3, LSCPT, le DFJP doit pouvoir déterminer quels sont les types de renseignements et de surveillance « usuels » qui se prêtent à une standardisation. Il faut éviter que les types définis par le Conseil fédéral et standardisés par le DFJP soient trop étroitement liés, afin que le département conserve une marge de manœuvre suffisante pour procéder, sous sa propre responsabilité, c'est-à-dire sans qu'une révision de l'OSCPT – qui relève de la compétence du Conseil fédéral – soit nécessaire à chaque fois, à un élargissement ou à une réduction, notamment, de la liste des types de renseignements et de surveillance ayant fait l'objet d'une standardisation.

Section 2 Assurance de la qualité

Art. 26 Branchements directs pour raisons techniques

L'*art. 26* règle les cas dans lesquels le Service SCPT n'est pas en mesure, pour des raisons techniques, de réceptionner et d'enregistrer dans son système de traitement les données issues de la surveillance. Dans une situation de ce type, il faut que les personnes obligées de collaborer puissent transmettre les données recueillies directement à l'autorité concernée, sans passer par le Service SCPT (branchement direct au sens des art. 17, let. c, et 26, al. 1, phrase introductive, LSCPT). Les données ne sont pas enregistrées dans le système de traitement et l'autorité destinataire doit procéder elle-même à leur sauvegarde.

S'il constate qu'un branchement direct est nécessaire pour des raisons techniques, le Service SCPT en informe les personnes obligées de collaborer concernées, l'autorité qui a ordonné la surveillance et l'autorité désignée par celle-ci. Pour que le branchement direct puisse être mis en place, il faut non seulement que les personnes obligées de collaborer soient en mesure de transmettre directement aux autorités de poursuite pénale les données issues de la surveillance, mais aussi que ces autorités soient en mesure de réceptionner les données.

La disposition ne précise pas cependant de combien temps disposent les fournisseurs et les autorités pour être en mesure, en cas de problème, de réaliser un branchement direct. Selon une estimation réaliste, il faut s'attendre à ce que plusieurs mois soient nécessaires. Le Service SCPT apporte son soutien aux

personnes obligées de collaborer et aux autorités de poursuite pénale concernées en les conseillant.

Comme dans les cas des mesures de surveillances qui sont exécutées au moyen du système de traitement, l'ordre de surveillance doit être transmis au Service SCPT, qui le transmet ensuite à la personne obligée de collaborer, en lui signalant que le mandat ne peut pas, pour des raisons techniques, être exécuté via le système de traitement et que les résultats doivent être livrés directement à l'autorité concernée. La procédure est portée dans le même temps à la connaissance de l'autorité concernée. La personne obligée de collaborer confirme la réception du mandat au Servie SCPT et lui indique si elle est en mesure d'effectuer elle-même le branchement direct. L'autorité doit elle aussi indiquer au Service SCPT si elle est en mesure de recevoir directement les données issues de la surveillance. Sitôt que la personne obligée de collaborer et l'autorité de poursuite pénale ont confirmé la faisabilité du branchement direct, la personne obligée de collaborer exécute la surveillance ou la fait exécuter par un tiers et en informe le Service SCPT (pour des détails sur l'exécution d'un mandat de surveillance, voir l'art. 11 OME-SCPT et son commentaire dans le rapport explicatif).

Les spécifications relatives aux interfaces utilisées pour la transmission des données via le système de traitement valent aussi pour la transmission des données recueillies avec un branchement direct. De même, tout comme les mesures de surveillance mises en œuvre au moyen du système de traitement, un branchement direct peut rester actif aussi longtemps que déterminé par l'autorité qui a ordonné la mesure. Des prolongations sont là aussi possibles. Il n'est pas possible en revanche de transférer un branchement direct vers le système de traitement. Le cas échéant, l'autorité concernée doit ordonner une nouvelle fois la mesure et le Service SCPT doit de nouveau mandater la personne obligée de collaborer. Les émoluments et les indemnités usuels s'appliquent au nouvel ordre.

Des restrictions sont mises aux branchements directs dans les cas visés aux art. 271 CPP et 70*b* PPM (voir les art. 271, al. 2, CPP et 70*b*, al. 2, PPM ; voir le message du 27 février 2013 concernant la LSCPT, FF **2013** 2474 s.).

Art. 27 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.

Aux termes de l'*al. 1*, la qualité des données transmises est réputée préservée lorsque la transmission satisfait aux exigences fixées par le département (*let. a*), qu'elle s'effectue sans perte de données et sans interruption (*let. b*) et que les données transmises lors de la surveillance ou les renseignements livrés correspondent respectivement à la correspondance par télécommunication désignée dans l'ordre de surveillance ou aux données indiquées dans la demande de renseignements (*let. c*). La disposition concerne exclusivement le processus de transmission. Si les données dont dispose la personne obligée de collaborer sont déjà incomplètes, leur qualité est réputée préservée dès lors que leur transmission s'effectue sans perte et sans interruption. En d'autres termes, seules peuvent être transmises les informations disponibles dans le réseau des personnes obligées de collaborer. 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.

Les *al 2* et *3* règlent les responsabilités quant à la garantie de la qualité et disposent concrètement que ce sont les personnes obligées de collaborer qui répondent de la qualité des données issues de la surveillance et de renseignements. Le Service SCPT leur apporte son soutien 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. 4* 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.

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 département pour chaque degré de gravité. Elle informe le Service SCPT par écrit et régulièrement – c'est-à-dire conformément aux échéances prescrites par le département – 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. 28 Branchements de test

Conformément à l'*al. 1*, des branchements de test sont utilisés pour garantir la qualité de la transmission de données des personnes obligées de collaborer au Service SCPT et aux autorités de poursuite pénale (*let. a*), pour contrôler la disponibilité à surveiller et à renseigner des personnes obligées de collaborer (*let. b*), pour tester le système de traitement du Service SCPT (*let. c*), pour effectuer des formations (*let. d*) et pour produire des données de référence (*let. e*).

Un *branchement de test* désigne la surveillance technique d'un service de télécommunication (par ex. abonnement mobile, carte SIM à prépaiement, raccordement fixe) ou d'un service de communication dérivé (par ex. un service de messagerie, un service de courriel Web) 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 et des autorités de poursuite pénale 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 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 n'a pas besoin, non plus, de faire approuver la mesure par un juge.

Le Service SCPT établit des dossiers de surveillance distincts au sens de l'art. 9 pour les branchements de test. A 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 la cible test est utilisée et le nom des personnes habilitées à traiter les données recueillies. En revanche, comme pour les surveillances normales, le Service SCPT journalise le traitement des données de toutes les cibles test utilisées.

L'*al. 4* autorise les autorités de poursuite pénale à faire effectuer à leurs frais des branchements de test pour garantir la qualité des télécommunications transmises ou à des fins de formation. Pour ce faire, ils doivent transmettre un ordre au Service DFJP. La mesure est soumise à émolument. Autre condition, les autorités de poursuite pénale 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 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 (voir le commentaire de l'art. 26). L'art. 18, al. 2, LSCPT s'applique par analogie aux branchements de test des autorités de poursuite pénale.

Le Service SCPT indique, sur le mandat de surveillance, qu'il s'agit d'un branchement de test. Il peut, au besoin, faire appel à des personnes obligées de collaborer pour générer des données de test (*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'ils exploitent qui sont nécessaires à la réalisation des branchements de test (*al. 4*). 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.

Le Service SCPT acquiert en revanche 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.

Les demandes de branchements de test émanant des autorités de poursuite pénale 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 combien de temps le branchement direct doit rester activé, la durée maximale étant fixée à douze moins. 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. Les autorités de poursuite pénale peuvent, 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 de poursuite pénale. Si les conditions d'une prolongation sont remplies, le branchement de test reste activé. Dans le cas contraire, le Service SCPT met à 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. 29 Contrôle de la disponibilité à renseigner et à surveiller

Chaque FST et chaque fournisseur de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements selon l'art. 21 doit être en mesure de livrer ou de faire livrer par des tiers les types de renseignements

visés aux art. 33 à 46 concernant des services qu'il offre (disponibilité à renseigner ; cf. art. 18).

Chaque FST et chaque fournisseur de services de communication dérivés ayant des obligations étendues en matière de surveillance visé à l'art. 50 doit être en mesure d'exécuter ou de faire exécuter par des tiers les types de surveillance selon les art. 52 à 68 concernant des services qu'il offre (disponibilité à surveiller ; cf. art. 48). Les FST ayant des obligations restreintes en matière de surveillance visés à l'art. 49 sont dispensés de cette obligation.

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. Dans ce cas, le tiers concerné est aussi appelé à fournir la preuve requise lors du contrôle de la disponibilité à renseigner et à surveiller. La responsabilité proprement dite d'apporter la preuve incombe dans tous les cas au fournisseur concerné.

Pour contrôler la disponibilité à renseigner et à surveiller, le Service SCPT accomplit diverses tâches, décrites à l'*al. 3* : il fixe, en accord avec le fournisseur, un calendrier ferme pour la réalisation des tests et définit les scénarios de tests que le fournisseur doit exécuter ; il contrôle les résultats des tests effectués (*let. a*), analyse les formulaires transmis par les fournisseurs (*let. b*), consigne les procédures de contrôle dans un procès-verbal (*let. c*) et, si la disponibilité à renseigner et à surveiller est confirmée, il délivre une attestation aux fournisseurs (*let. d*). Le Service SCPT conserve les procès-verbaux pendant toute la durée de validité de l'attestation et pendant dix ans après la fin de la validité de celle-ci (*let. e*). Ces procès-verbaux 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.

L'attestation confirme que le fournisseur est en mesure, pour des critères de validité déterminés, de transmettre les données conformément aux prescriptions fixées par le département et que sa disponibilité à renseigner et à surveiller est ainsi garantie (*al. 4*).

Art. 30 Durée de validité de l'attestation

Si le contrôle de la disponibilité à renseigner et à surveiller confirme que la personne obligée de collaborer est en mesure d'exécuter les mandats conformément aux prescriptions applicables, le Service SCPT lui délivre une attestation (voir à ce sujet le commentaire de l'art. 29).

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.

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. 31 Procédure de contrôle

Cette disposition donne la compétence au département 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. 32 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 et 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*), s'il existe des éléments indiquant que le fournisseur n'est pas en mesure, dans un ou plusieurs cas, de garantir la transmission des données ou la disponibilité à renseigner et à surveiller (*let. b*) oui 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. 33 Type de renseignements IR_1_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. l*).

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_2_NA (*art. 34*).

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_1_NA (art. 33) et IR_6_TEL (art. 38). Le fournisseur Y leur transmet cinq résultats concernant le type de renseignements IR_1_NA (art. 33 ; ces résultats comptent comme cinq enregistrements au sens de l'art. 17, al. 2) et 13 résultats concernant le type de renseignements IR_6_TEL (art. 38 ; 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. 19*.

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. 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 à prépaiement il y a lieu de préciser aussi, conformément à l'art. 21, al. 1, let. e, LSCPT et à l'*art. 19, al. 1*, le lieu de remise du moyen permettant l'accès au service et le nom de la personne qui s'est en 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 téléphonie mobile.

- Le *ch. 11* prévoit l'indication, pour les services de téléphonie 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 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.

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_3_IP (*art. 35*), le type IR_4_IP (traduction d'adresses de réseau; art. 36) et le type IR_5_NAT (art. 37); voir le commentaire des art. 35, 36 et 37.

Art. 34 Type de renseignements IR_A2_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). Concrètement, cela signifie qu'il ne doit pas être possible de déterminer, à partir de la réponse, la date, les modalités et le lieu d'utilisation du service en question.

Art. 35 Type de renseignements IR_3_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 manière unique, toutes les demandes sont ici uniformisées en fonction de l'adresse IP. Dans le cas où l'adresse IP n'est ou n'avait pas été attribuée individuellement à un usager, le fournisseur l'indique dans sa réponse. L'autorité concernée peut alors soumettre une nouvelle demande de renseignements, portant cette fois sur le type IR_4_IP (NAT) (art. 36), en mentionnant des critères de recherche supplémentaires (voir commentaire de l'art. 36).

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 à la seconde près. 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.

Le fournisseur effectue la recherche pour l'heure indiquée en prévoyant un intervalle de tolérance de plus ou moins quelques secondes, afin de tenir compte d'éventuelles imprécisions des horloges des systèmes. Cet intervalle est défini dans l'ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT), où sont aussi détaillées les différentes étapes pour répondre à une demande de renseignements de ce type.

Art. 36 Type de renseignements IR_4_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) permet 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 (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 pour identifier les usagers.

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, let. a* définit quelles indications doivent être livrées en cas d'identification concluante. La *let. b* dispose qu'il y a lieu d'indiquer, le cas échéant, dans la réponse la raison pour laquelle l'identification n'a pas été concluante (par ex. aucune concordance ou, à l'inverse, plusieurs concordances).

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 de destination (par ex. un serveur Web), le numéro de port de destination et 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*). Remarque: il faut veiller à indiquer une heure précise et à réduire le plus possible le domaine de recherche afin d'éviter les faux-positifs (voir commentaire de l'art. 35)

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.

- 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 selon l'historique IP).

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 (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 (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 [privée] et le port source) 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 trouvés dans un premier temps sont utilisés pour rechercher le numéro MSISDN ou le numéro IMSI de l'usager. Ce numéro permet ensuite de rechercher 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.

En fonction du type de procédure de traduction d'adresses utilisée, les fournisseurs ne doivent conserver que pendant six mois les adresses IP et les numéros de port de destination de tous les usagers, dès lors que ces informations sont considérées comme étant des données secondaires de télécommunication au sens de la LSCPT et de l'OSCPT (art. 21, al. 2, 2e phrase, art. 22, al. 2, 2e phrase, et al. 4, LSCPT et art. 20, al. 2).

Art. 37 Type de renseignements IR_5_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. 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 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 de destination et le numéro de port correspondant (*let. c et d*) du serveur de destination.

- 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 de destination et le numéro de port correspondant (*let. c et d*) du serveur de destination.

Exemple de recherche selon la première possibilité : lorsqu'une demande portant sur le type de renseignements IR_4_IP (NAT) selon l'*art. 36* 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. 38 Type de renseignements IR_6_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 de l'identifiant du service (al. 2, let. l).

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_7_TEL (art. 39) permet de recueillir des indications spécifiques supplémentaires sur cette catégorie de services.

L'*art. 38* s'applique aussi bien aux services sur abonnement qu'aux services à prépaiement. Il est structuré de la même manière que l'art. 33. Le commentaire de l'art. 33 vaut donc aussi pour cet article.

L'*al. 1* définit, sur le modèle de l'art. 33, 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 données de localisation de l'accès au réseau fixe et leur période de validité respective (*ch. 5*), les données qui doivent être livrées sont celles qui sont enregistrées chez le fournisseur (par ex. adresse de l'emplacement), pour autant qu'il s'agisse d'un service téléphonique ou multimédia du réseau fixe. Comme l'emplacement s 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[40] arrête à son art. 9, al. 1, que les fournisseurs de services téléphoniques publics sur réseau fixe 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. 33, 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. 33, al. 2).

40 RS **784.101.112**

Une distinction est faite entre les identifiants (let. h, j, k et l) et les ressources d'adressage (let. i). Les identifiants ont pour fonction, comme leur nom l'indique, d'identifier sans ambiguïté des services de téléphonie et multimédia déterminés. À la différence des ressources d'adressage, 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[41] 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. 39 Type de renseignements IR_7_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. 38.

L'*al. 1* définit, sur le modèle de l'art. 34, 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*), il y a lieu de préciser que le fournisseur doit fournir la liste des identifiants des équipements effectivement utilisés pendant la période couverte par la requête. Il doit récupérer ces informations dans les données secondaires de télécommunication conservées, sans toutefois communiquer les données secondaires elles-mêmes. Concrètement, cela signifie qu'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. Le fournisseur livrera donc, par exemple, une liste des numéros IMEI des appareils de téléphonie mobile effectivement utilisés (quelle que soit la durée d'utilisation) pendant la période précisée dans la demande de renseignements, sans spécifier toutefois quand précisément les équipements ont été utilisés.

La durée de conservation des identifiants des équipements effectivement utilisés (par ex. adresses MAC, numéros IMEI) est limitée à six mois, car il s'agit de données secondaires au sens de l'art. 26 LSCPT (art. 21, al. 2, 2e phrase, art. 22, a. 2, 2e phrase, et al. 4, LSCPT et art. 20, al. 2).

L'*al. 2* énumère, sur le modèle de l'art. 34, 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. 34, al. 2).

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

41 RS **784.104**

Art. 40 Type de renseignements IR_8_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. 37. Le commentaire de l'art. 37 vaut donc aussi pour cet article.

L'*al. 1* définit, sur le modèle de l'art. 37, al. 1, 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.

Une adresse au sens du *ch. 5* peut être 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. L'usager peut aussi envoyer des courriels en tant qu'expéditeur à partir de l'adresse 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. 38, 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. 38, al. 2).

Art. 41 Type de renseignements IR_9_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 de services téléphoniques et multimédia. 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. 38 à 40. 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.

L'*al. 2* énumère, sur le modèle des art. 38 à 40, 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. 38, al. 2).

Section 6 Autres types de renseignements

Art. 42 Type de renseignements IR_10_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 utilisés 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. 43 Type de renseignements IR_11_ID: copie de la pièce d'identité

L'art. 19 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. 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. L'autorité à l'origine de la demande de renseignements doit préciser 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*). La copie de la pièce d'identité doit être transmise par voie électronique.

Art. 44 Type de renseignements IR_12_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. 45 Type de renseignements IR_13_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 doit préciser ici aussi 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. 46 Type de renseignements IR_14_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). Ce type de renseignements correspond à l'actuel type A3.

L'*al. 1* mentionne des exemples types de données techniques, comme des indications relatives à des antennes de téléphonie mobile qui ne sont pas liées à une localisation fixe ou des indications relatives à des points d'accès mobile au réseau WLAN, par exemple dans des avions (compagnie aérienne, immatriculation de l'aéronef), des trains (compagnie ferroviaire et numéro de train) ou des bus (compagnie de transport et numéro de bus), ou à bord de bateaux de croisière (armateur, nom du navire).

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.

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 en outre préciser dans sa demande la période sur laquelle porte sa requête et les indications selon l'al. 1 qu'elle souhaite obtenir. 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 d'éléments réseau. Le fournisseur doit quant à lui livrer les indications souhaitées sur tous les éléments réseau se trouvant à la localisation indiquée. Il 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_27_PREP_COV (art. 64).

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

Art. 47 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[42]. 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 cible, un nouvel ordre est nécessaire. Les émoluments et les indemnités usuels s'appliquent.

42 RS **780.11**

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.

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 et 273 CPP.

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 ressources d'adressage 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 mention 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.

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. 48 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. 50. 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. 29 à 32).

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'ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT).

L'*al. 4* définit quelle partie de la correspondance par télécommunication doit être surveillée et pendant combien de temps. Le Service SCPT communique aux personnes obligées de collaborer la période indiquée par l'autorité dans son ordre de surveillance. Pour les surveillances en temps réel, il leur transmet 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 (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 l'exploitation technique usuelle. Si, en revanche, celui-ci contrôle l'infrastructure étrangère, il doit transmettre le contenu des communications et les données secondaires dans leur intégralité. 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 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 l'exploitation usuelle (routage, signalisation, voir aussi l'art. 51, al. 1, let. h) 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 téléphonie 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 (cf. *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 cible soient aussi surveillés.

Aux termes de l'*al. 7* enfin, lorsqu'une communication était déjà en cours au moment de l'activation d'une surveillance en temps réel, les données disponibles s'y rapportant doivent être livrées sans délai.

Art. 49 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 les données secondaires de télécommunication de la personne surveillée dont ils disposent (art. 26, al. 2, LSCPT).

L'*al. 1* définit les conditions qui doivent être remplies pour qu'un FST ne doive pas exécuter des obligations autres que les obligations minimales prévues par la loi. Concrètement, un fournisseur est considéré comme ayant des obligations restreintes en matière de surveillance s'il offre ses services exclusivement dans le domaine de l'éducation ou s'il ne remplit pas les deux conditions suivantes : au moins dix mandats de surveillance au cours des douze mois écoulés (date de référence arrêtée au 30 juin) et chiffre d'affaires annuel inférieur à 100 millions pendant deux exercices consécutifs. Concernant ce dernier critère, seule est prise en compte la facturation correspondant aux services de télécommunication et aux services de communication dérivés pour le calcul du chiffre d'affaires déterminant. Le fait d'offrir ses services de télécommunication exclusivement dans le domaine de l'éducation suffit à dispenser un FST des obligations étendues en matière de surveillance. 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 450 selon le droit en vigueur à un nombre compris entre 20 et 50. La dispense de certains fournisseurs d'obligations étendues en matière de surveillance n'entraînera cependant aucune lacune dans la 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. Le Service SCPT prend les mesures nécessaires pour que la mesure ordonnée puisse être mise en œuvre (art.17, let. e, LSCPT).

L'*al. 2* décrit, par analogie avec l'art. 21, al. 2, le cas des fournisseurs qui contrôlent une ou plusieurs entreprises tenues d'établir des comptes. Le fournisseur et les entreprises contrôlées sont considérées, ici aussi, comme formant une unité (voir le commentaire de l'art. 21 pour plus de précisions).

Si ses obligations changent parce qu'il dépasse ou, à l'inverse, parce qu'il n'atteint plus les valeurs selon l'al. 1 ou parce qu'il n'offre plus ses services exclusivement

dans le domaine de l'éducation, le FST concerné a trois mois suivant la fin de l'exercice pour le communiquer au Service SCPT (*al. 3*), en lui faisant parvenir les justificatifs requis.

S'il arrive à la conclusion, après examen des documents produits, que les conditions de l'al. 1 sont remplies, le Service SCPT en informe le fournisseur, qui ne doit plus, à partir de ce moment, garantir la disponibilité à surveiller (*al. 4*).

À l'inverse, comme prévu également à l'art. 21, al. 4, 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 leur confirme qu'ils ne sont plus considérés comme des FST ayant des obligations restreintes en matière de surveillance (*al. 5*).

C'est le Service SCPT qui décide si un FST remplit ou ne remplit plus les conditions pour être considéré comme ayant des obligations restreintes (*al. 6*).

Art. 50 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. 21, 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. 49 traite spécifiquement des surveillances. La seule différence par rapport à l'art. 21 concerne la condition alternative du nombre de mandats, qui est ici de dix. Pour le reste, les dispositions sont identiques. Le commentaire de l'art. 21 vaut donc aussi pour cet article.

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. 51 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. 49), 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. En pareil cas, le Service SCPT exécute lui-même l'ordre de surveillance ou le fait exécuter par des tiers (art. 26, al. 2 et 6, et art. 34 LSCPT). Dans un cas comme dans l'autre, l'accès aux installations de la personne obligée de collaborer concernée doit être garanti.

L'*art. 50* 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 (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.

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

Art. 52 Type de surveillance RT_15_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). A la différence du type de surveillance défini à l'art. 53, le type de surveillance visé dans cet article porte uniquement sur les données secondaires de télécommunication. Il est utilisé principalement pour des accès mobiles à Internet, 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. Un type de surveillance spécifique est prévu pour les applications. Il en va de même des messages MMS : dans le cadre d'une surveillance du type RT_15_NA_IRI selon l'art. 52, 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). Les données secondaires concernant spécifiquement les MMS et le contenu des messages sont néanmoins disponibles dans les données relatives au contenu obtenues dans le cadre d'une surveillance du type RT_16_NA_CC_IRI selon l'art. 53.

L'*al. 1* 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. Le numéro d'un raccordement téléphonique relié à un raccordement DSL, pour autant que cette information soit disponible, est un exemple de ressource d'adressage visée à l'*al. 1, let. e.* Les « changements techniques » selon l'*al. 1, 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 support (*bearer modification*) et l'actualisation de la position (*location update*). Enfin, l'expression « exploitation technique usuelle » (*al. 1, let. h*) signifie que les modalités de l'exploitation technique (par ex. la signalisation, le routage) ne diffèrent pas fondamentalement entre une cible surveillée et une cible ne faisant pas l'objet d'une surveillance.

L'*al. 2* précise le contenu des données de localisation selon l'al. 1, let. h. Trois options s'offrent aux personnes obligées de collaborer. Quelle que soit la solution qu'ils privilégient, ils ne peuvent dans tous les cas livrer que des données vérifiées, c'est-à-dire des données qui ont été déterminées par le réseau. Les données émanant d'un équipement terminal ou d'une application peuvent en effet avoir été falsifiées.

Conformément à la *let. a*, la personne obligée de collaborer doit fournir, notamment la direction principale d'émission de la cellule momentanément utilisée, pour autant que cette information soit disponible et correcte. 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. 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, ce champ de données peut comprendre plusieurs directions principales d'émission. S'il s'agit d'une cellule omnidirectionnelle, c'est-à-dire qui émet à 360° degrés, ce champ est vide.

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. 53 Type de surveillance RT_16_NA_CC_IRI: surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau

Le type de surveillance défini à l'*art. 53* 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. 52 doivent être transmis en temps réel.

Comme relevé dans les explications relatives à l'art. 47, 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.

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. 54 Type de surveillance RT_17_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. 55, qui traite de la surveillance en temps réel des données secondaires et du contenu de services de téléphonie et multimédia. A la différence toutefois du type de surveillance défini à l'art. 55, 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 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 momentanément disponibles dans le cadre de l'exploitation technique usuelle (let. e, ch. 9), lesquelles sont décrites en détail à l'al. 2. Des précisions sur le contenu des données de localisation figurent dans le commentaire de l'art. 52, al. 2.

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. 55 Type de surveillance RT_18_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[43]). Dans le domaine de la téléphonie 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 téléphonie mobile (accès dit non-3GPP). Il ne s'agit là que de quelques exemples de situations

43 RS **784.101.112**

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. 54.

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.

Art. 56 Type de surveillance RT_19_EMAIL_IRI: surveillance en temps réel des données secondaires de services de courrier électronique

Cet article définit, de manière analogue à l'art. 57, 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[44]). 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. 73).

A la différence 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 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

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

surveillé (pour des précisions sur les alias de messagerie et les listes de distribution, voir le commentaire de l'art. 40).

Art. 57 Type RT_20_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. 56), en veillant à supprimer les cryptages qu'ils ont opérés (art. 26, al. 2, let. c, LSCPT).

Art. 58 Type de surveillance RT_21_COM_IRI: surveillance en temps réel des données secondaires d'autres services de télécommunication ou de services de communication dérivés

Le type de surveillance défini dans cet article se fonde sur le principe sur l'actuel type PS 4 (surveillance en temps réel des données secondaires d'une application). Il concerne principalement les services dits « hors offre du fournisseur d'accès à Internet » (over the top, OTT). La définition de cette catégorie de services n'est toutefois pas suffisamment précise pour pouvoir les distinguer nettement des services visés par les autres types de surveillance.

On peut mentionner à titre d'exemple les services de communication intégrés dans des services d'informatique en nuage ou dans des réseaux sociaux ou fondés sur un service de serveur mandataire. Comme il n'existe pas encore de norme internationale spécifique pour ce type de surveillance, le Service SCPT traite pour l'heure ces ordres comme des surveillances spéciales, tant pour l'exécution que pour la facturation. Le Service SCPT continuera d'observer l'évolution de l'activité de normalisation au niveau international et complètera en temps utile les ordonnances d'application de la LSCPT au cas où de nouvelles normes seraient publiées.

À la différence du type de surveillance RT_22_COM_CC_IRI (art. 59), dans cette surveillance le fournisseur ne doit livrer en temps réel que les données secondaires des communications, mais en aucun cas leur contenu (voir aussi la fin du commentaire de l'art. 59). Les données secondaires qui doivent être fournies en temps réel sont définies de manière sommaire aux *let. a* à *e.*

Art. 59 Type de surveillance RT_22_COM_CC_IRI: surveillance en temps réel du contenu et des données secondaires d'autres services de télécommunication ou de services de communication dérivés

Comme le type de surveillance RT_20_EMAIL_CC_IRI (art. 57), ce type de surveillance se fonde, sur le principe, sur l'actuel type PS 3 (surveillance en temps réel d'une application). Pendant une phase transitoire, le contenu et les données secondaires peuvent être soit surveillés soit en tant que service d'accès au réseau, soit en tant que services de téléphonie et multimédia (voir commentaire de l'art. 58).

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*.

En vertu de la compétence conférée au Conseil fédéral par l'art. 31 LSCPT, la *section 10* 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 aux sections 4 et 5 du chapitre 3.

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

45 FF **2013** 2739

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.

On parle en revanche de tentative de connexion ou de tentative d'établissement de l'accès au réseau lorsque l'authentification de l'utilisateur a fonctionné, mais que la connexion ou l'accès au réseau n'a pas pu être établi pour une raison, par exemple un crédit de communication insuffisant.

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. 48, 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 qu'elle ne les possède pas.

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 (identifiant cible), puisque ces informations ne seraient pas complètes ou ne seraient pas disponibles.

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_23_NA: surveillance rétroactive des données secondaires de télécommunication 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 données secondaires relatives aux tentatives d'établissement de l'accès au réseau doivent aussi être conservées (voir les remarques introductives à la section 10 ci-dessus pour des précisions sur le terme de tentative d'établissement de l'accès au réseau).

Les *let. a* à *g* énumèrent les données que les personnes obligées de collaborer doivent conserver et livrer : la date et l'heure de l'établissement ou de la tentative d'établissement de l'accès au réseau, ainsi que le moment de la déconnexion (*let. a*) ; la nature de l'accès au réseau (*let. b*) ; les données d'authentification, d'autorisation et de comptabilité utilisées (*let. c*) ; les adresses ou plages d'adresses IP attribuées par le fournisseur d'accès au réseau, ainsi que la date et l'heure de leur attribution (*let. d*) ; les ressources d'adressage relatives au service

d'accès au réseau (*let. e*), comme le numéro du raccordement téléphonique rattaché à un raccordement DSL ou le numéro MSISDN d'un accès mobile au réseau ; les identifiants des équipements terminaux (let. *f*) ; pour autant que ces données soient disponibles, les volumes de données téléchargées et téléversées pendant la session (*let. g*) ; dans le cas de services mobiles, en plus des données selon les let. a à g, les données de localisation disponibles dans le cadre de l'exploitation technique usuelle au début et, le cas échéant, à la fin de la session (*let. h*). Une définition de l'expression « exploitation technique usuelle » figure dans le commentaire de l'art. 52, al. 1, let. h. Pour la transmission des données de localisation selon la let. h, la personne obligée de collaborer a le choix entre trois options. Elle ne peut cependant livrer que des données vérifiées, c'est-à-dire des données qui ont été déterminées par le réseau. Les données de localisation provenant de l'équipement terminal ou d'une application ne sont pas acceptées, car elles peuvent être falsifiées.

Art. 61 Type de surveillance HD_25_TEL: surveillance rétroactive des données secondaires de télécommunication 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. 55.

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. 55. 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.

Les *let. a* à *d* énumèrent les données que les personnes obligées de collaborer doivent conserver et livrer. Le terme « tentative d'établissement de la communication » (*let. b*) est expliqué dans les remarques introductives à la section 10 ci-dessus. Les « adresses disponibles » visées à la *let. b, ch. 5* comprennent aussi, dans le cas de services VoIP, l'adresse du serveur mandataire SIP. Comme prescrit aussi à l'art. 60, dans le cas de services mobiles, les personnes obligées de collaborer doivent également transmettre les données de localisation disponibles dans le cadre de l'exploitation technique usuelle au début et, le cas échéant, à la fin de la session (*let. d*). Une définition de l'expression « exploitation technique usuelle » figure dans le commentaire de l'art. 52, al. 1, let. h.

Pour la transmission des données de localisation selon la *let. d, ch. 1*, la personne obligée de collaborer a le choix entre trois options. Elle ne peut cependant livrer que des données vérifiées, c'est-à-dire des données qui ont été déterminées par le

réseau. Les données de localisation provenant de l'équipement terminal ou d'une application ne sont pas acceptées, car elles peuvent être falsifiées.

Dans le cas d'autres services mobiles (*let. d, ch. 2*), comme les services nomades de transport de la voix via le protocole internet (VoIP), les fournisseurs doivent conserver et livrer les données de localisation de l'accès au service surveillé. Il est possible d'utiliser des services nomades à partir pratiquement de tous les points d'accès à Internet, d'où l'appellation de services mobiles. Les données de localisation de l'accès au réseau ne doivent être conservées et livrées que dans la mesure où elles sont disponibles.

Art. 62 Type de surveillance HD_25_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. L'événement consistant dans le téléchargement d'un message englobe ainsi, dans certains cas, le téléversement. 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_26_COM: surveillance rétroactive des données secondaires d'autres services de télécommunication et de services de communication dérivés

Cet article définit un type nouveau de surveillance rétroactive. Les progrès techniques et la diffusion de ces nouveaux services rendent nécessaire une extension des types de surveillance rétroactive. Comme il n'existe pas encore de norme ETSI pour la surveillance de cette catégorie de services, seules devront dans un premier temps être livrées les données disponibles. Le format pour la livraison des données se fonde sur celui utilisé pour des services de télécommunication et des services de communication dérivés comparables qui ont déjà fait l'objet d'une standardisation. Les personnes obligées de collaborer pourront néanmoins aussi utiliser d'autres formats dans le cas où elles se seraient déjà dotées de processus et de systèmes à cette fin, par exemple pour se conformer aux prescriptions édictées par d'autres États.

Art. 64 Type de surveillance AS_27_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 suite à une demande d'analyse de la couverture réseau.

Art. 65 Type de surveillance AS_28_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 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_29: 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).

L'art. 66 détaille les indications que les FST doivent livrer.

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 – et par cellule et le tribunal des mesures de contrainte doit valider chaque ordre. 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.

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 cibles spécifiés.

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'actuelle OSCPT, 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 (qui peut remonter à six mois au plus), et définit la composition des données que les personnes obligées de collaborer doivent livrer. L'*identifiant du réseau de téléphonie mobile* est composé du code pays du réseau de téléphonie 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* décrit 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. 53 et 55, 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_31_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 type RT_18_TEL_CC_IRI pour le service de téléphonie et une surveillance en temps réel du type RT_16_NA_CC_IR 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. 52 et 54, 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. 61 et 62, 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.

La let. e permet de faire effectuer une recherche par champ d'antennes (art. 66) et les mesures préalables (art. 64 et 65) dans le cadre d'une recherche en cas d'urgence également.

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 et pour chaque fournisseur et chaque identifiant cible (voir l'OEI-SCPT).

Section 12 Identifiants externes au réseau

Art. 69

L'*art. 69* règle, de manière similaire aux art. 16*b* et 24*c* de l'OSCPT en vigueur, 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.

Cet article s'applique aux surveillances en rapport avec une ressource d'adressage étrangère (surveillance d'un raccordement téléphonique avec un numéro d'appel étranger). La surveillance en rapport avec une ressource d'adressage étrangère n'a toutefois fait l'objet d'une standardisation que pour les applications et non pour les services d'accès au réseau. Des restrictions s'appliquent en outre en ce qui concerne les identifiants cibles (par ex. pas d'IMSI, ni d'IMEI). Celles-ci sont détaillées dans l'OME-SCPT. 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[46]. La procédure pour ce type de mesure se distingue de la pratique actuelle en ce sens qu'il n'est pas nécessaire de faire figurer une mention particulière sur l'ordre et le mandat de surveillance. L'art. 48, al. 4, définit de manière générale quelles sont les communications qui doivent être surveillées.

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[47].

Cet article crée, avec l'art. 31, al. 3, LSCPT[48], la base légale de l'ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT). L'ordonnance du DFJP 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, concrètement sur l'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.

---

46 FF **2013** 2444, 2445 [s.]
47 RS **780.11**
48 Voir le message du 27 février 2013 concernant la LSCPT, ad. art. 2, let. e, FF **2013** 2445/2446

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[49] ; voir www.li.admin.ch).

D'autres normes de délégation au DFJP figurent aux art. 31 (procédure de réception), 47, al. 2 (indications techniques dans l'ordre de surveillance) et 27, 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'*art. 71, al. 1*, reprend pour l'essentiel les art. 33, al. 2, OSCPT dans sa teneur du 31 octobre 2001[50]. 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.

Art. 72 Abrogation et modification d'autres actes

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

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)[51] ; il s'agit d'une adaptation de nature formelle de l'art. 25.

- l'ordonnance du 9 mars 2007 sur les services de télécommunication[52] ; les modifications concernent l'art. 3, al. 1, let. d, et al. 2, et l'art. 80.

Art. 73 Dispositions transitoires

Les dispositions transitoires de l'*art. 75* sont nécessaires pour que les personnes obligées de collaborer et le Service SCPT disposent de suffisamment de temps pour appliquer les nouvelles normes. Une entrée en vigueur échelonnée des ordonnances de mise en œuvre de la LSCPT n'est ainsi pas nécessaire.

---

49 RS **780.11**
50 RS **780.11**
51 RS **780.11**
52 RS **784.101.1**

L'*al. 1* 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[53]). Les systèmes actuels, principalement le CCIS, dont le contrat de maintenance ne peut plus être adapté, ne permettent pas d'établir les statistiques souhaitées.

Conformément à l'*al. 2*, après que le Service SCPT aura mis en service l'interface automatisée pour la fourniture des renseignements, les personnes obligées de collaborer auront six mois au plus pour procéder aux adaptations requises de leurs systèmes. Ensuite, elles devront transmettre leurs renseignements via la nouvelle interface.

Les fournisseurs de services de communication dérivés ayant des obligations étendues visés à l'art. 21 ne sont pas tous en mesure, en l'état actuel, de fournir les renseignements selon les nouveaux types définis. Certains doivent en effet adapter leurs logiciels ou leurs systèmes. L'*al. 2* leur donne un délai de douze mois pour effectuer les travaux nécessaires.

De la même manière, une phase transitoire de 24 mois est prévue pour que les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 50 puissent adapter leurs systèmes et être ainsi en mesure d'enregistrer et de livrer des données secondaires relatives aux *tentatives* d'établissement de communications et aux tentatives de connexion, comme ils y sont désormais astreints (*al. 3*).

L'OME-SCPT ne reconnaît pas les procédures et les mécanismes de transmission, aujourd'hui dépassés, en vigueur en Suisse pour la surveillance des services de courrier électronique. Le système de traitement du Service SCPT ne les prendra en charge que durant une période limitée, et uniquement si les systèmes concernés étaient déjà opérationnels lors de l'entrée en vigueur de l'OSCPT révisée. Un délai approprié (24 mois) est là aussi accordé aux FST pour configurer leurs systèmes conformément aux prescriptions de l'OSCPT et de l'OME-SCPT relatives à la surveillance des services de courrier électronique (*al. 4*).

Art. 74 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.

53 FF **2015** 2809

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[54] (ou domaine éducation), art. 26, al. 6,	21/22	18, al. 1 et 3 20 29 (conformité)	A	26, al. 2 et 6	49	B
	NORMAL	21/22	11, al. 2 18, al. 1 et 2 19, 20 29 (conformité) 73 (disp. trans.)	C	26, al. 1 à 5	11, al. 2 48 29 (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[55] (obligations étendues)	22, al. 4	18, al. 1 et 2 29 (conformité) 73 (disp. trans.)	G	27, al. 3 26, al. 1 à 5	11, al. 2 29 (conformité) 48 50	H

54 Réduction (Downgrade)
55 Renforcement (Upgrade)

A. Obligations des FST ayant des obligations retreintes en matière de fourniture de renseignements (FST de taille modeste)
Condition = Les FST offrent des services de télécommunication de faible importance économique ou dans le domaine de l'éducation

- Ils ont les mêmes obligations que les FST de taille dite normale pour ce qui est de la fourniture de renseignements (pas de réduction des obligations).
- Conformément à l'art. 11, al. 2, OSCPT, ils sont dispensés de l'obligation d'assurer un service de piquet.
- S'agissant du traitement automatisé des demandes de renseignements selon les art. 33 à 46, ils sont dispensés de l'obligation, conformément à l'art. 18, al. 3, OSCPT (= ils peuvent aussi répondre par écrit).

B. Obligations des FST ayant des obligations restreintes (FST de taille modeste) en matière de surveillance, 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 l'éducation

- Ils sont libérés des obligations selon l'art. 26, al. 1 et 3 à 5, LSCPT.
- 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 (selon l'art. 26, al. 2, LSCPT) :
  - livrer les informations nécessaires à l'exécution de la surveillance ;
  - tolérer la surveillance ;
  - supprimer les cryptages qu'ils ont opérés.

C. Obligations des FST (de taille normale) en matière de fourniture 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)
- Être en mesure de traiter les demandes de renseignements selon les art. 33 à 46 OSCPT (art. 18, al. 1, OSCPT).
- Pour autant que l'interface de consultation du système de traitement le permette, traiter de manière automatisée les demandes de renseignements selon les art. 33 à 40 ; les demandes selon les art. 41 à 46 peuvent aussi être traitées manuellement (art. 18, al. 2, OSCPT).
- Respecter les délais de conservation selon les art. 21 et 22 LSCPT et l'art. 20 OSCPT.
- Art. 11, al. 2, OSCPT

Obligations des FST (de taille normale) en matière de surveillance, de recherches d'urgence et de recherche de personnes condamnées

- Art. 26 LSCPT (obligations des fournisseurs de services de télécommunication)

1 Les fournisseurs de services de télécommunication livrent au Service ou, selon l'art. 17, let. c, à l'autorité qui a ordonné la surveillance ou à l'autorité désignée par celle-ci, sur demande:
   a. le contenu des communications de la personne surveillée;
   b. les données secondaires de télécommunication de la personne surveillée.
2 Ils doivent en outre:
   a. livrer les informations nécessaires à l'exécution de la surveillance;
   b. tolérer les surveillances exécutées par le Service ou par les personnes man-datées par celui-ci; à cet effet, ils doivent sans délai garantir l'accès à leurs installations;
   c. supprimer les cryptages qu'ils ont opérés.
3 Les fournisseurs de services de télécommunication qui participent à l'exploitation du service de télécommunication à surveiller livrent les données en leur possession au Service ou à celui d'entre eux qui est chargé de la surveillance.
4 L'ordre de surveillance peut prévoir l'exécution de celle-ci en temps réel ou la remise des données secondaires de télécommunication conservées concernant des communications passées (surveillance rétroactive).
5 Les fournisseurs de services de télécommunication conservent les données secon-daires de télécommunication durant six mois.

- Ils ont des obligations pendant le service de piquet (art. 11, al. 2, OSCPT).
- Art. 48 OSCPT

E. Obligations des fournisseurs de services de communication dérivés (de taille normale) en matière de fourniture de renseignements

- Les fournisseurs de services de communication dérivés livrent au Service les indications dont ils disposent (art. 22, al. 3, LSCPT)
- Art. 11, al. 2, OSCPT
- Art. 18, al. 4, OSCPT

F. Obligations des fournisseurs de services de communication dérivés (de taille normale) en matière de surveillance, de recherches d'urgence et de recherche de personnes condamnées

- Tolérer la surveillance (art. 27, al. 1, LSCPT)
- Art. 27, al. 2, LSCPT
- Art. 11, al. 2, OSCPT

G. Obligations des fournisseurs de services de communication dérivés ayant des obligations étendues (fournisseurs de grande taille) en matière de fourniture de renseignements

Condition = Le fournisseurs offrent des services d'une grande importance économique ou à un grand nombre d'utilisateurs.

- Ils ont les mêmes obligations que les FST de taille dite normale.
- Livrer des renseignements visant à identifier les auteurs d'infractions par Internet (art. 22 LSCPT).
- Être en mesure de traiter les demandes de renseignements selon les art. 31 à 44 OSCPT (art. 18, al. 1, OSCPT).
- Pour autant que l'interface de consultation du système de traitement le permette, traiter de manière automatisée les demandes de renseignements selon les art. 33 à 40 ; les demandes selon les art. 41 à 46 peuvent aussi être traitées manuellement (art. 18, al. 2, OSCPT).
- Respecter les délais de conservation des données selon les art. 22 LSCPT et 20 OSCPT.
- Art. 11, al. 2, OSCPT

H. Obligations des fournisseurs de services de communication dérivés ayant des obligations étendues (fournisseurs de grande taille) en matière de surveillance, 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.

- Ils ont les mêmes obligations que les FST de taille dite normale (art. 27, al. 3, LSCPT)
- Ils ont des obligations pendant le service de piquet (art. 11, al. 2, OSCPT).
- Ils exécutent les obligations selon l'art. 26, al. 1 à 5 LSCPT.
- Art. 48 OSCPT