

# Rapport explicatif

## relatif à l'ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT; RS 780.117)

### 1. Contexte

Pour que les types de renseignements et de surveillance qui ont été adaptés au développement de la technologie dans le cadre de la révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)<sup>1</sup> et de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT)<sup>2</sup> puissent être mis en œuvre de manière utile à la poursuite pénale, les fournisseurs de services postaux et de services de télécommunication, ainsi que les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance, doivent prendre les mesures nécessaires aux niveaux organisationnel, administratif, et technique. Selon le droit en vigueur, ces mesures de nature organisationnelle, administrative et technique et les modalités de leur mise en œuvre sont réglées dans des directives du Service de surveillance de la correspondance par poste et télécommunication (Service SCPT). Il s'agit des *directives organisationnelles et administratives pour les fournisseurs de services postaux v1.5*, des exigences techniques et administratives (*organisational and administrative requirements v2.15, OAR*) et des exigences techniques relatives à la surveillance des télécommunications (*technical requirements for telecommunication surveillance v3.2, TR TS*).

À l'avenir, ce ne seront plus des instructions du Service SCPT, mais des dispositions inscrites dans une ordonnance du Département fédéral de justice et police (DFJP) qui régleront les aspects organisationnels, administratifs et techniques garantissant la mise en œuvre la plus avantageuse possible en termes de coûts des types de renseignements et de surveillance ayant fait l'objet d'une standardisation. Ce changement permet de tenir compte du principe de précision des normes et d'inscrire les réglementations applicables à un niveau normatif supérieur.

Conformément aux dispositions de la loi sur les publications officielles (LPubl)<sup>3</sup>, cette ordonnance du département sera publiée dans les trois langues officielles. Vu leur caractère particulier, ses annexes ne seront pas publiées dans le Recueil officiel (RO ; art. 5 LPubl). En outre, comme c'est déjà le cas aujourd'hui, les détails relatifs aux prescriptions techniques pertinents pour les fournisseurs ne seront disponibles qu'en anglais. Cette rédaction en langue anglaise exclusivement se justifie par le fait premièrement, que l'Institut européen des normes de télécommunication (*European Telecommunications Standards Institute, ETSI*) ne publie ses normes qu'en anglais, et deuxièmement, par le fait que l'anglais est la langue utilisée par les spécialistes et les techniciens dans le secteur des télécommunication (art. 14, al. 2, LPubl en relation avec l'art. 33, al. 1, de l'ordonnance sur les publications officielles, OPubl<sup>4</sup>).

1 RS 780.1

2 RS 780.11

3 RS 170.512

4 RS 170.512.1

## 2. Commentaire article par article

### *Préambule*

Le droit en vigueur confère la compétence au Service SCPT de régler, pour chaque cas, les modalités organisationnelles, administratives et techniques pour la mise en œuvre de mesures de surveillance. Ces modalités sont définies dans les *OAR* et les *TR TS*. La décision a été prise dans le cadre de la révision totale de la LSCPT que ces aspects de nature organisationnelle, administrative et technique ne figureraient plus à l'avenir dans des directives du Service SCPT, mais qu'ils seraient inscrits dans une ordonnance du DFJP. La norme de délégation en matière de télécommunication se trouvait jusqu'ici dans une ordonnance (art. 17, al. 1, OSCPT dans sa teneur du 31 octobre 2001). Avec la révision totale de la LSCPT, cette norme a été relevée au niveau de la loi : c'est l'art. 31, al. 3, LSCPT qui fournira à l'avenir la base légale de la délégation de compétences pour la définition des dispositions organisationnelles, administratives et techniques nécessaires pour garantir une fourniture standardisée des renseignements et une mise en œuvre standardisée des types de surveillance courants dans le domaine des télécommunications. L'art. 68 OSCPT entièrement révisée crée la base légale pour la définition des autres exigences d'ordre organisationnel, administratif et technique nécessaires en matière de correspondance par poste et de correspondance par télécommunication.

### **Section 1 Dispositions générales**

#### *Art. 1* Champ d'application

Les destinataires de l'ordonnance sont le Service SCPT d'une part et les personnes obligées de collaborer au sens de l'art. 2 LSCPT d'autre part, y compris celles visées aux *let. e* et *f* de cette disposition (c'est-à-dire les personnes qui mettent leur accès à un réseau public de télécommunications à la disposition de tiers et les revendeurs professionnels de cartes ou de moyens semblables qui permettent l'accès à un réseau public de télécommunications).

#### *Art. 2* Obligation d'informer du cadre légal

La surveillance de la correspondance par poste et télécommunication doit être traitée de manière strictement confidentielle, de manière à garantir que la mesure atteigne son but, à savoir le succès de la poursuite pénale. Les données de la correspondance par poste et télécommunication sont soumises au secret postal et au secret des télécommunications. Les personnes obligées de collaborer sont par conséquent tenues d'informer leurs collaborateurs chargés de la surveillance du caractère confidentiel de la mesure et d'attirer leur attention sur le secret postal et le secret des télécommunications (*let. a* et *b*). Elles doivent également les rendre attentifs aux conséquences pénales selon l'art. 321<sup>er</sup> du code pénal (CP)<sup>5</sup> et l'art. 39 LSCPT en cas de violation de leurs obligations (*let. c*). Cette disposition doit permettre de réduire les risques d'un comportement fautif.

<sup>5</sup> RS 311.0

### Art. 3 Sécuration de la communication

Les données de la correspondance par poste et télécommunication sont des données sensibles, d'où la nécessité de règles strictes concernant les voies et les modalités de communication entre les personnes obligées de collaborer et le Service SCPT. Ainsi, seules des personnes définies au préalable sont autorisées à envoyer et à recevoir des communications confidentielles (*let. a*) et les courriels doivent toujours être cryptés et signés (*let. b*). Le cryptage garantit que des tiers ne puissent pas prendre connaissance du contenu d'un message électronique durant son transport de l'expéditeur vers le destinataire. La signature permet quant à elle au destinataire d'avoir la certitude que le courriel provient bel et bien de l'expéditeur indiqué.

### Art. 4 Mode de transmission des mandats

L'art. 4 définit le mode de transmission des mandats. Le Service SCPT doit transmettre le mandat écrit par voie électronique aux personnes obligées de collaborer (*al. 1*). Dans les cas d'urgence, le Service SCPT est autorisé à transmettre un mandat relatif à une surveillance ou à une demande de renseignements par téléphone dans un premier temps. Le mandat écrit doit ensuite être transmis par voie électronique le jour ouvré suivant (*al. 2*).

### Art. 5 Service à contacter

Les fournisseurs de services postaux (art. 2, let. a, LSCPT), les fournisseurs de services de télécommunication (art. 2, let. b, LSCPT) et les fournisseurs de services de communication dérivés (art. 2, let. c, LSCPT) doivent désigner, dès le début de l'exploitation commerciale, un service avec lequel le Service SCPT peut prendre contact en cas de besoin. À la demande du Service SCPT, les exploitants de réseaux de télécommunication internes (art. 2, let. d, LSCPT), les personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers (art. 2, let. e, LSCPT) et les revendeurs professionnels de cartes ou de moyens semblables qui permettent l'accès à un réseau public de télécommunication (art. 2, let. e, LSCPT) doivent aussi désigner un tel service. Il doit être possible de joindre le service désigné par téléphone (*al. 1*).

Les fournisseurs doivent indiquer les coordonnées des interlocuteurs compétents (nom, prénom et fonction), y compris les numéros de téléphone (directs) et les adresses électroniques, de même que les clés cryptographiques (*al. 2*). Toutes ces informations doivent être communiquées par voie électronique. Tout changement doit être notifié sans délai au Service SCPT. Les clés cryptographiques servent à crypter les courriels que le Service SCPT envoie aux personnes obligées de collaborer et, de la même manière, à vérifier la signature des courriels que les personnes obligées de collaborer adressent au Service SCPT.

Les personnes obligées de collaborer doivent aussi fournir une adresse de correspondance en Suisse, à laquelle seront envoyées de manière juridiquement valable notamment les communications, les mandats de comparution, les mandats de surveillance et toute autre décision (*al. 3*).

### Art. 6 Délais de traitement

L'*al. 1* dispose que le Service SCPT et les personnes obligées de collaborer doivent traiter dans les meilleurs délais les ordres, les requêtes et les mandats qui leurs sont

transmis, mais au plus tard avant l'échéance des délais concrets fixés dans l'ordonnance pour la fourniture des renseignements et l'exécution des surveillances.

Si le Service SCPT ou tiers mandaté par lui exécute un mandat de surveillance pour le compte d'un fournisseur, les délais de traitement fixés pour les personnes obligées de collaborer (par ex. aux 16 à 18) ne s'appliquent pas. L'exécution de la surveillance entraîne un surcroît de travail pour le Service SCPT ou le tiers mandaté par lui, car il faut analyser le système externe pour décider si la surveillance peut être activée via un accès à distance ou si elle doit être activée sur place, auquel cas il faut prendre en compte le temps de trajet, sans oublier le temps nécessaire pour trouver une solution permettant d'exécuter la mesure (*al. 2*).

#### *Art. 7* Assurance de la qualité de la transmission des données

Le Service SCPT effectue des contrôles en collaboration avec les fournisseurs de services de télécommunication et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance dans le but de garantir le bon déroulement de la surveillance des télécommunications et de faire en sorte que la transmission des données recueillies dans ce cadre réponde aux exigences de qualité requises. Ces contrôles prennent essentiellement la forme d'un monitoring automatisé, qui peut au besoin être complété par des tests spécifiques supplémentaires. Le Service SCPT conçoit à cet effet un programme de test, après avoir entendu les fournisseurs (*al. 1*). Pour la réalisation de ces tests, les fournisseurs mettent à la disposition du Service SCPT, conformément à l'annexe 1, des données de test (*al. 3, let. a*). Ils doivent aussi lui donner accès, sur place ou à distance, à leurs infrastructures pour permettre le raccordement d'équipements de test ou l'exécution de tests relatifs à la fourniture de renseignements et la mise en place de branchements de test (*al. 3, let. b*). Ils apportent leur soutien, au besoin sur place, au Service SCPT (*al. 4*).

Pour garantir la qualité de la transmission dans un cas particulier également, le Service SCPT, après avoir entendu les fournisseurs, fixe les détails de l'assurance de la qualité spécialement adaptés au cas en question (*al. 2*).

#### *Art. 8* Dérangements affectant les systèmes des fournisseurs

La surveillance des télécommunications contribue à l'efficacité de la poursuite pénale. Pour garantir la disponibilité de cette prestation, les fournisseurs de services de télécommunication et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance doivent dès lors signaler immédiatement au Service SCPT tout dérangement affectant leurs systèmes. Vu l'urgence de la situation, l'annonce peut d'abord être faite par téléphone. Le fournisseur a ensuite cinq jours ouvrés pour envoyer une communication écrite, dans laquelle il indique la durée de la défaillance, ses causes et ses répercussions, ainsi que les mesures mises en œuvre pour y remédier.

Il est de la responsabilité des fournisseurs de régler les dysfonctionnements qui affectent leurs systèmes et de rétablir leur capacité à exécuter des surveillances et à fournir des renseignements. Concrètement, les fournisseurs doivent lever les dérangements dans les meilleurs délais et, dans un souci de transparence, tenir le Service SCPT informé de l'avancement des travaux. Cette obligation de lever au plus vite les dérangements et d'informer régulièrement le Service SCPT ne dispense toutefois pas les

fournisseurs de leur obligation d'exécuter des surveillances et des demandes de renseignements (*al. 2 et 3*).

*Art. 9*                    Dérangements affectant le réseau de transmission

Voir aussi le commentaire de l'art. 8.

De la même manière qu'il appartient aux fournisseurs de services de télécommunication et aux fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance de lever les dérangements qui affectent leurs systèmes, il est de la responsabilité du Service SCPT de remédier aux dysfonctionnements qui touchent son système. Cependant, si le dérangement concerne des parties du réseau de transmission qui relèvent du domaine de responsabilité commun des fournisseurs et du Service SCPT, le problème doit être réglé conjointement par toutes les parties concernées, conformément au processus défini à cette fin avec le Service SCPT. Les parties se tiennent informées des mesures qu'elles ont prises ou qu'elles prévoient de prendre.

## **Section 2      Surveillance de la correspondance par poste**

*Art. 10*                  Surveillance en temps réel

Cet article traite des dispositions à observer lors de la mise en œuvre d'une surveillance en temps réel de la correspondance par poste.

*L'al. 1* définit la notion d'« interception des envois postaux » selon l'art. 16, let. a, OSCPT. Cette mesure comprend l'identification et le tri de l'envoi postal, sa mise à disposition pour le retrait par l'autorité qui a ordonné la surveillance, ainsi que, le cas échéant, sa reprise en charge une fois le contrôle effectué et sa distribution.

Aux termes de *l'al. 2*, la transmission de données selon l'art. 16, let. b, OSCPT consiste en la communication en continu des données disponibles, sans toutefois interrompre le processus de distribution de l'envoi postal concerné. Ces données sont l'identité de l'expéditeur et du destinataire, ainsi que le type d'envoi et son statut de distribution. Seules doivent être livrées les données secondaires effectivement disponibles. Les fournisseurs de services postaux ne sauraient être tenus de saisir et de conserver intégralement ces données. Ils doivent en revanche communiquer toutes les données en leur possession qui permettent d'identifier les usagers, ainsi que les données relatives au trafic et à la facturation. La condition de la communication en contenu est réputée remplie dès lors que les informations demandées parviennent au moins une fois par jour à l'autorité désignée dans le mandat transmis par le Service SCPT.

*L'al. 3* fixe le délai imparti aux fournisseurs de services postaux pour mettre en place une surveillance en temps réel.

La formule « le fournisseur de services postaux dispose d'un jour ouvré » signifie que la réponse doit parvenir au Service SCPT à 17 heures au plus tard le jour ouvré suivant.

Exemple 1 : Un ordre de surveillance parvient au Service SCPT à 8 heures. Si le Service SCPT utilise entièrement le délai de traitement dont il dispose, à savoir une heure, le mandat arrive chez le fournisseur à 9 h 01. Dans cet exemple, le fournisseur a jusqu'à 17 heures le jour ouvré suivant pour mettre en œuvre la surveillance.

Exemple 2 : Un ordre de surveillance parvient au Service SCPT un jeudi à 16 h 01. Si le Service SCPT utilise entièrement le délai de traitement dont il dispose, à savoir une heure, le mandat arrive chez le fournisseur à 17 h 02, le fournisseur a jusqu'au vendredi à 17 heures pour mettre en place la surveillance.

#### *Art. 11* Surveillance rétroactive

Conformément à l'art. 11, les fournisseurs de services postaux ont trois jours ouvrés suivant la réception du mandat pour exécuter une surveillance rétroactive de la correspondance postale.

### **Section 3 Renseignements sur la correspondance par télécommunication**

#### *Art. 12* Demande de renseignements

Pour la fourniture de renseignements, l'état déterminant des informations est celui qui existe au moment indiqué dans la demande, ou durant la période qu'elle couvre (al. 1). Faute d'une indication temporelle, c'est le moment auquel la demande de renseignements a été transmise qui est déterminant. Si des informations ont changé durant la période précisée dans la demande, la personne obligée de collaborer livrera un enregistrement incluant plusieurs saisies, correspondant à chacun des états des informations, en indiquant pour chaque état la durée de validité. Si la structure prédéfinie des enregistrements ne permet pas d'inclure plusieurs saisies, la personne obligée de collaborer livrera plusieurs enregistrements.

#### *Art. 13* Recherche exacte et recherche flexible de nom

L'al 1 prescrit la manière d'effectuer une recherche exacte, qui ne tient cependant compte que des 26 lettres majuscules de l'alphabet latin (A à Z) et des chiffres 0 à 9. Dans la pratique, une recherche exacte à 100 % ne mènerait souvent pas aux résultats souhaités, parce que les systèmes des personnes obligées de collaborer et le système de traitement du Service SCPT n'utilisent pas forcément les mêmes jeux de caractères. En outre, les personnes obligées de collaborer ne peuvent pas toujours rendre correctement tous les caractères lorsqu'elles saisissent les informations d'un client. Des fautes sont également souvent commises concernant les signes typographiques (par ex. virgule, point, trait d'union, apostrophe, espace, guillemet, barre oblique) figurant dans les noms. La chaîne de recherche et les données correspondantes dans la banque de données des clients (index de recherche) doivent donc être normalisées selon les critères exposés à l'al. 2. Le principe de base consiste à éliminer tous les signes qui ne sont ni des lettres, ni des chiffres, puis à remplacer les lettres qui ne font pas partie des 26 lettres de l'alphabet latin par une ou deux lettres latines, selon la translittération recommandée que l'on trouve dans l'annexe 2 « Transcription des caractères spéciaux » de la directive du DFJP du 1<sup>er</sup> janvier 2012 sur la détermination et l'orthographe des noms de ressortissants étrangers. Cette directive se fonde sur les recommandations de l'Organisation de l'aviation civile internationale (OACI) concernant

les documents de voyage lisibles par machine. La translittération ignore largement les signes diacritiques, ces petits ajouts tels que trait, point, crochet, arc de cercle, cercle, qui sont placés au-dessus, au dessous ou au travers d'une lettre. Citons comme exemples de signes diacritiques le tréma, l'accent, la brève, la cédille, les signes marquant l'accent tonique ou le ton, le rond, le caron (hatchek), le point médian, l'ogonek, le macron, la barre inscrite oblique, le point au-dessus ou au-dessous, la barre inscrite à travers le fût. La prononciation n'est pas prise en considération lors de la translittération, sauf pour les voyelles à umlaut et l'eszett (ß).

L'al. 2 définit les critères pour une recherche flexible. La recherche intelligente est la combinaison d'une recherche phonétique et d'une recherche tolérante à l'erreur. La recherche phonétique signifie que la chaîne de recherche et les données correspondantes dans la banque de données clients (index de recherche) sont transformées, par un algorithme, en chaînes phonétiques qui sont ensuite comparées. L'accent n'est pas sur une correspondance phonétique exacte avec la langue d'origine du nom recherché, mais une correspondance approximative selon les sonorités de la langue anglaise et, si possible, des trois langues officielles que sont l'allemand, le français et l'italien. Les fonctions de recherche phonétique pour l'anglais sont déjà incluses dans les principaux systèmes de gestion de banques de données.

La recherche tolérante à l'erreur couvre les fautes de frappe et d'orthographe, par exemple l'inversion de lettres, l'omission ou l'ajout d'une lettre ou d'un signe, l'inversion ou l'omission de parties d'un nom, car celles-ci ont peut-être déjà été confondues lors de leur saisie, ou saisies de manière incomplète (par ex. inversion du nom et du prénom).

Le résultat d'une recherche flexible doit livrer tous les noms qui, phonétiquement, correspondent ou ressemblent à une partie au moins du nom recherché. On utilisera dans la mesure du possible les fonctions de recherche incluses dans les systèmes usuels de gestion de banques de données et qui sont spécialisées dans la recherche de noms. Compte tenu de la tolérance à l'erreur, la recherche flexible livre davantage de résultats que la recherche exacte selon l'al. 1, mais seule la personne habilitée à l'origine de la demande peut décider lesquels de ces résultats sont pertinents. Pour prendre cette décision, elle doit avoir accès à tous les résultats.

#### *Art. 14* Délais de traitement des demandes de renseignements

Le Service SCPT a une heure pour transmettre les demandes de renseignements pour exécution aux personnes obligées de collaborer visées à l'art. 2, let. b à d, LSCPT (al. 1).

Comme les demandes portant sur les types de renseignements indiqués doivent être traitées de manière automatisée, les temps de réaction impartis aux personnes obligées de collaborer sont réduits en conséquence. Les fournisseurs de services de télécommunication, à l'exception de ceux ayant des obligations restreintes en matière de surveillance, et les fournisseurs de services de communications dérivés ayant des obligations étendues en matière de fourniture de renseignements doivent traiter les demandes ayant pour objet les types de renseignements IR\_4\_NA (art. 35), IR\_5\_NA\_FLEX (art. 27 et 35), IR\_6\_NA (art. 36), IR\_7\_IP (art. 37), IR\_10\_TEL (art. 40), IR\_11\_TEL\_FLEX (art. 27 et 40), IR\_12\_TEL (art. 41), IR\_13\_EMAIL (art. 42) et IR\_14\_EMAIL\_FLEX (art. 27 et 42) dans les meilleurs délais, mais au

plus tard dans un délai d'une heure<sup>6</sup>. Pour tous les autres types de renseignements, elles disposent d'un jour ouvré suivant la réception du mandat (*al. 2*).

Les fournisseurs de services de télécommunication ayant des obligations restreintes en matière de surveillance, les fournisseurs de services de communication dérivés – à l'exception de ceux qui ont des obligations étendues en matière de fourniture de renseignements – et les exploitants de réseaux de communication internes traitent quant à eux les demandes de renseignements dans un délai de deux jours ouvrés suivant leur réception (*al. 3*).

Le terme « un jour ouvré » signifie là aussi que la réponse doit parvenir au Service SCPT à 17 heures au plus tard le jour ouvré suivant (voir exemple dans le commentaire de l'art. 10).

## **Section 4    Surveillance de la correspondance par télécommunication**

### *Art. 15*            Exécution

L'autorité qui ordonne une mesure transmet au Service SCPT un ordre de surveillance, qui doit être approuvé par l'autorité habilitée à autoriser la surveillance. Si l'ordre respecte les exigences formelles fixées, le Service SCPT transmet un mandat de surveillance au fournisseur de services de télécommunication concerné ou au fournisseur concerné de services de communication dérivés ayant des obligations étendues en matière de surveillance. Les fournisseurs de services de télécommunication ayant des obligations restreintes en matière de surveillance sont dispensés de l'obligation d'exécuter ou de faire exécuter par des tiers des surveillances en temps réel, des surveillances rétroactives, des recherches en cas d'urgence et des recherches de personnes condamnées (voir le commentaire des art. 49, al. 1, et 50 OSCPT). Ils doivent néanmoins s'acquitter des obligations prévues à l'art. 26, al. 2, LSCPT et fournir les données secondaires de télécommunication de la personne surveillée dont ils disposent, mais ils ne sont pas liés par les types de surveillance ayant fait l'objet d'une standardisation énumérés sous le chap. 3, section 10, OSCPT.

Le déroulement d'une surveillance en temps réel comprend trois phases : la phase d'activation, la phase de surveillance proprement dite (également appelée phase active) et la phase de désactivation. La phase d'activation consiste en la transmission du mandat en vue de la mise en place de la surveillance et de son déclenchement (début de la surveillance). La phase de surveillance désigne l'interception et la transmission en temps réel de la correspondance par télécommunication surveillée. Enfin, la phase de désactivation désigne la transmission du mandat de désactivation et la mise hors service de la surveillance en temps réel (fin de la surveillance).

Pour activer une surveillance en temps réel, le Service SCPT transmet un mandat au fournisseur concerné. Celui-ci confirme la réception du mandat au Service SCPT et met en place lui-même la surveillance en temps réel ou en charge un tiers. Il confirme ensuite la mise en place de la mesure au Service SCPT au moyen d'une quittance qui indique le moment précis de l'activation (date et heure).

La surveillance en temps réel est à présent active. À partir de ce moment, la correspondance par télécommunication surveillée est interceptée et déviée vers le système

<sup>6</sup> Corrigé le 18.09.2019.



de traitement du Service SCPT, où elle est mise à la disposition des autorités habilitées. La surveillance en temps réel reste active aussi longtemps que le Service SCPT ne transmet pas un mandat de désactivation au fournisseur.

Le Service SCPT fait procéder à la désactivation de la surveillance en temps réel conformément aux instructions de l'autorité qui l'a ordonnée. Pour ce faire, il transmet le mandat de désactivation au fournisseur concerné via le système de traitement. Le fournisseur confirme au Service SCPT la réception du mandat de désactivation puis son exécution en lui transmettant une quittance qui indique précisément le moment (date et heure) auquel la mesure a été mise hors service. La surveillance prend alors fin (*al. 1 et 2*).

La surveillance rétroactive se déroule quant à elle en deux phases : la phase d'octroi du mandat et la phase de l'exécution. La phase d'octroi décrit la transmission du mandat par le Service SCPT, via le système de traitement, au fournisseur concerné, lequel confirme au moyen d'une quittance au Service SCPT la réception du mandat. Dans la phase d'exécution, le fournisseur exécute lui-même la surveillance ou en charge un tiers. Concrètement, la surveillance rétroactive consiste à récupérer les données secondaires conservées des télécommunications passées visées dans le mandat de surveillance pour les transmettre au Service SCPT via le système de traitement. Pour terminer, le fournisseur confirme au Service SCPT l'exécution de la surveillance rétroactive au moyen d'une quittance qui indique le moment précis (date et heure) auquel les données secondaires ont été envoyées (*al. 3*).

Compte tenu de la multitude des services pouvant faire l'objet d'une surveillance, des renseignements pouvant être demandés, dans des surveillances en temps réel ou rétroactives, de nombreuses combinaisons sont, par nature, possibles. Le Service SCPT établira une vue d'ensemble complète, qu'il publiera sur son site internet.

#### *Art. 16* Délais de traitement pour les surveillances en temps réel

Voir aussi le commentaire de l'art. 15.

Les délais de traitement ont été raccourcis par rapport à la pratique actuelle. Cette réduction ne concerne pas que les surveillances en temps réel, mais aussi, de manière générale, tous les types de surveillance. Les différents degrés de priorité utilisés jusqu'ici sont aussi abandonnés dans un souci d'harmonisation (mêmes délais pour un même type de surveillance).

Les délais de traitement diffèrent en fonction du moment où une surveillance en temps réel est ordonnée. Il faut faire ici une distinction entre les ordres transmis pendant les heures normales de travail et ceux transmis en dehors de ces heures. Les heures normales de travail sont définies à l'art. 10 OSCPT.

Que l'ordre lui parvienne pendant les heures normales de travail ou en dehors, le Service SCPT dispose toujours d'une heure pour transmettre le mandat aux fournisseurs concernés (*al. 1*).

Lorsqu'un mandat de surveillance en temps réel leur est transmis pendant les heures normales de travail, les fournisseurs doivent l'exécuter dans un délai d'une heure (*al. 2*). Le délai commence à courir à la réception du mandat. Lors de la consultation, certaines réserves ont été exprimées concernant ce délai jugé trop bref. Compte tenu de son expérience, et du nombre d'avis sur ce point, le Service SCPT considère cependant qu'un délai d'une heure est en principe réaliste. Un dépassement de ce délai,

dans des cas exceptionnels et dûment motivés, ne devrait toutefois pas mener directement à une procédure de contrôle.

L'al. 3 se rapporte au cas de figure dans lequel la surveillance en temps réel doit être mise en place à partir d'un moment déterminé. Le mandat doit alors indiquer une date et une heure précises. Il y a lieu de noter que ce type de mandat n'est exécuté que pendant les heures normales de travail.

Lorsqu'un mandat d'exécution d'une surveillance en temps réel leur est transmis en dehors des heures normales de travail, les fournisseurs doivent mettre en place la surveillance dans un délai de deux heures (al. 4). Là encore, comme pour l'al. 2, quelques participants ont exprimé le souhait que ce délai soit allongé. Mais ici aussi, le Service SCPT estime que deux heures sont en principe suffisantes, un dépassement exceptionnel, dûment motivé, ne déclenchant pas non plus automatiquement une procédure de contrôle.

Les délais de traitement valent non seulement pour l'activation d'une mesure, mais aussi pour sa désactivation. L'al. 5 dispose à cet égard que le Service SCPT transmet les mandats de désactivation exclusivement pendant les heures normales de travail. Les fournisseurs ont un jour ouvré pour procéder à la désactivation.

Lorsqu'un ordre de désactivation d'une surveillance parvient au Service SCPT un vendredi à 16 heures et que celui-ci utilise entièrement le délai d'une heure dont il dispose pour transmettre le mandat correspondant au fournisseur, cela signifie que le fournisseur reçoit le mandat à 17 h 01. Dans ce cas, le fournisseur a jusqu'à lundi à 17 heures pour exécuter la désactivation.

Pour calculer le délai global de traitement, il faut additionner le délai de traitement imparti au Service SCPT et celui imparti au fournisseur. Il peut donc arriver qu'un ordre de surveillance en temps réel parvienne au Service SCPT pendant les heures normales de travail, mais que le fournisseur ne puisse exécuter le mandat correspondant que pendant le service de piquet. C'est le cas par exemple lorsqu'un ordre de mise en place d'une surveillance en temps réel est transmis au Service SCPT à 16 heures. Le Service SCPT a une heure pour le traiter, soit jusqu'à 17 heures. S'il transmet le mandat à ce moment, cela signifie que le fournisseur réceptionne le mandat à 17 h 01. Le délai de traitement imparti au fournisseur se situe alors en dehors des heures normales de travail. Dans ces circonstances, sont aussi dus les émoluments et les indemnités supplémentaires selon l'art. 6 OEI-SCPT<sup>7</sup> pour des prestations en dehors des heures normales de travail.

#### *Art. 17* Délais de traitement pour les surveillances rétroactives

Voir aussi le commentaire des art. 15 et 16.

L'al. 2 pose comme règle que les mandats concernant une surveillance rétroactive doivent être transmis pendant les heures normales de travail. Une transmission en dehors de ces heures est aussi possible exceptionnellement, dans les cas urgents, par exemple une alerte à la bombe ou un enlèvement.

Les personnes obligées de collaborer ont trois jours ouvrés pour exécuter une surveillance rétroactive. Ce délai est ramené à six heures dans les situations d'urgence et pour les mandats transmis en dehors des heures normales de travail. Il convient de

<sup>7</sup> Ordonnance du 15.11.2017 sur les émoluments et les indemnités en matière de surveillance (OEI-SCPT; RS 780.115.1)

signaler à cet égard qu'en fonction de la manière dont est configuré le système installé chez le fournisseur, le traitement et la mise à disposition des données secondaires des 24 dernières heures peut prendre plus d'un jour. Si la mesure revêt un caractère d'urgence, les données secondaires les plus récentes risquent donc de ne pas être encore disponibles. Elles devront être livrées dès que possible, après entente avec le Service SCPT (*al. 3*).

Le délai de traitement commence là aussi à courir à la réception du mandat par le fournisseur. Le Service SCPT a une heure suivant la transmission de l'ordre par l'autorité pour confier le mandat de surveillance rétroactive au fournisseur concerné.

Dans les procédures accélérées, la transmission des données et des enregistrements ne peut pas satisfaire aux mêmes exigences de qualité que dans une procédure usuelle. Bien souvent, une perte de qualité est inévitable dans les surveillances rétroactives déclarées urgentes. On ne peut pas non plus exclure que les données secondaire relatives aux 24 dernières heures ne soient pas complètes, en raison de retards dû à la technologie dont est équipé le fournisseur pour le traitement et la mise à disposition des données secondaires de communication.

*Art. 18* Délais de traitement pour les recherches en cas d'urgence et les recherches de personnes condamnées

Voir aussi le commentaire des art. 15 à 17

Les recherches en cas d'urgence comme les recherches de personnes condamnées doivent être exécutées dans les plus brefs délais. Dans le premier cas, il faut partir du principe que la vie et l'intégrité corporelle de la personne disparue sont en danger, alors que dans le second, c'est la vie et l'intégrité corporelle non seulement de la personne condamnée, mais aussi de tiers non impliqués, qui peuvent être en jeu.

*L'al. 1* donne un délai maximal d'une heure au Service SCPT pour transmettre aux fournisseurs les mandats concernant des recherches en cas d'urgence ou des recherches de personnes condamnées. Cette exigence de célérité se vérifie dans la pratique, puisque la plupart des mandats de ce type sont traités en l'espace de quelques minutes.

Pour permettre de sauvegarder le bien juridique le plus précieux qu'est la vie, les délais impartis pour l'exécution des recherches en cas d'urgence et des recherches de personnes condamnées sont très courts. Les fournisseurs mandatés doivent mettre en œuvre les surveillances dans les plus brefs délais, mais en règle générale au plus tard dans un délai d'une heure (pour les types de surveillance EP\_30\_PAGING, EP\_31\_RT\_CC+IRI, EP\_32\_RT\_IRI) ou, selon le cas, de quatre heures (pour le type de surveillance EP\_33\_HD) (*al. 2 et 3*).

Dans les procédures accélérées, la transmission des données et des enregistrements ne peut pas satisfaire aux mêmes exigences de qualité que dans une procédure usuelle. Bien souvent, une perte de qualité est inévitable dans les surveillances rétroactives déclarées urgentes et concernant la recherche d'une personne condamnée ou concernant une recherche d'urgence du type EP\_34\_HD. On ne peut pas non plus exclure que les données secondaire relatives aux 24 dernières heures ne soient pas complètes, en raison de retards dus à la technologie dont est équipé le fournisseur pour le traitement et la mise à disposition des données secondaires de communication (*al. 3*).

## *Art. 19* Annulation de mandats de surveillance

Voir aussi le commentaire des art. 15 à 18.

L'annulation d'une surveillance en temps réel est possible tant que le fournisseur mandaté n'a pas confirmé l'activation de la mesure (*al. 1*). Par contre, si l'activation a déjà été confirmée, seule une désactivation proprement dite est possible (*al. 4*). S'il apparaît, ultérieurement, qu'une des conditions pour ordonner la surveillance n'est plus remplie, la mesure ne peut pas, là non plus, être annulée, mais doit être désactivée.

Aux termes de l'*al. 2*, une surveillance rétroactive ne peut être annulée que tant que le fournisseur n'a pas transmis les données demandées et confirmé la transmission.

L'*al. 3* décrit les étapes de l'annulation : le Service SCPT transmet par écrit aux fournisseurs le mandat d'annulation de la surveillance ou, exceptionnellement, les charge par téléphone d'annuler la surveillance et leur fait suivre le mandat écrit (*let. a*). Les fournisseurs de leur côté confirment au Service SCPT la réception du mandat d'annulation (*let. b*), l'exécutent (*let. c*) et confirment enfin l'annulation au Service SCPT (*let. d*).

Comme le dispose l'art. 4 OEI-SCPT, les annulations selon les al. 1 et 2 n'entraînent pas de coûts. Ni émoluments, ni indemnités ne sont en effet dus. Les critères fixés pour l'exécution de l'annulation peuvent pénaliser le Service SCPT et les personnes obligées de collaborer s'ils ont déjà entamé les travaux pour mettre en œuvre la mesure et qu'ils doivent les interrompre. Mais comme le Service SCPT et, en partie aussi les personnes obligées de collaborer, ne perçoivent pas aujourd'hui déjà d'émolument et d'indemnité en cas d'annulation, décision a été prise de maintenir cette pratique.

## **Section 5 Disponibilité à renseigner et à surveiller**

### *Art. 20* Raccordement des systèmes des fournisseurs au système de traitement du Service SCPT

Dans le cadre de la surveillance de la correspondance par télécommunication, le Service SCPT a une fonction d'intermédiaire entre, d'un côté, les fournisseurs de services de télécommunication et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance et, de l'autre côté, les autorités de poursuite pénale. Les données issues de renseignements et de surveillances sont mises à la disposition des autorités de poursuite pénale dans le système de traitement du Service SCPT, où elles peuvent les consulter via un accès en ligne. Les fournisseurs mandatés téléversent quant à eux les données collectées dans le système de traitement du Service SCPT grâce au raccordement qui relie leurs propres systèmes au système de traitement.

Pour établir la disponibilité à renseigner et à surveiller, les fournisseurs mentionnés doivent informer le Service SCPT des services qu'ils offrent, en précisant pour chacun d'eux les modalités d'exécution des demandes de renseignements et des surveillances ayant fait l'objet d'une standardisation (*al. 1*). Le Service SCPT fixe, après avoir entendu les fournisseurs, les détails relatifs à l'exécution du mandat et au réseau de transmission et détermine, pour chaque type de renseignements et de surveillance, les identifiants pertinents comme le type ou le format (*al. 2*). Les fournisseurs mettent en place le réseau de transmission conformément à l'annexe 2 de l'ordonnance et aux prescriptions définies dans la convention de raccordement (*al. 3*).

*Art. 21* Obligation d'information réciproque

La surveillance des télécommunications contribue à l'efficacité de la poursuite pénale. Pour garantir la disponibilité de cette prestation, les fournisseurs de services de télécommunication et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance doivent être en tout temps en mesure, notamment du point de vue technique, de livrer les renseignements demandés et de mettre en œuvre les surveillances ordonnées. L'*al. 1* leur fait obligation de communiquer au Service SCPT tout changement susceptible d'affecter la transmission des données ou leur disponibilité à renseigner ou à surveiller. La communication doit être faite au moins cinq jours ouvrés à l'avance. L'*al. 2* prévoit la même obligation pour le Service SCPT. Lui aussi doit avertir les fournisseurs cinq jours ouvrés au plus tard avant le changement. L'*al. 3* prévoit que les fournisseurs et le Service SCPT doivent aussi indiquer, lors de la communication, les effets prévisibles et le degré de priorité des changements qu'ils prévoient d'opérer.

*Art. 22* Contrôle de la disponibilité à renseigner et à surveiller

Voir aussi le commentaire des art. 20 et 21.

Pour chaque nouveau service de télécommunication ou service de communication dérivé pour lequel la disponibilité à renseigner et à surveiller doit être garantie, le Service SCPT doit s'assurer que le fournisseur sera en mesure, le moment venu, de fournir des renseignements ou d'exécuter une surveillance concernant le nouveau service en question. Le Service SCPT fixe à cette fin les conditions à mettre en place, établit une liste de scénarios de test et définit, d'entente avec les fournisseurs, un calendrier contraignant pour la réalisation des tests (*al. 1*). Par conditions à mettre en place, il faut entendre par exemple les liaisons qui doivent être établies avec certains systèmes et réseaux de transmission. Les fournisseurs exécutent eux-mêmes les tests ou en confient l'exécution à des tiers. Le Service SCPT encadre la phase de test et contrôle les résultats (voir aussi le commentaire de l'art. 16).

La commercialisation d'un nouveau service peut rendre nécessaire une adaptation du réseau de transmission et des paramètres techniques. Pour ces derniers, le Service SCPT les détermine après avoir entendu le fournisseur, tandis que pour le réseau de transmission, c'est au fournisseur qu'il appartient de procéder aux adaptations requises. Le Service SCPT vérifie ensuite avec le fournisseur que la transmission fonctionne correctement (*al. 2*).

La disponibilité à renseigner et à surveiller doit faire l'objet d'un nouveau contrôle lorsqu'un service de télécommunication ou un service de communication dérivé est exploité depuis un certain temps déjà. Ces contrôles périodiques visent à garantir que la disponibilité à renseigner et à surveiller est assurée en permanence (*al. 3*). Même des adaptations mineures dans les systèmes d'un fournisseur ou dans le système de traitement du Service SCPT peuvent avoir une influence sur la disponibilité à renseigner et à surveiller. Si des changements ont été opérés, du côté des fournisseurs ou du côté du Service SCPT, un nouveau contrôle peut être nécessaire. Le Service SCPT décide, sur la base des informations transmises par le fournisseur ou sur la base de ses propres constatations, s'il y a lieu d'effectuer un nouvel examen et, dans l'affirmative, selon quelles modalités et à quel moment. Les contrôles périodiques sont régis par les mêmes conditions que le contrôle initial selon les *al. 1* et *2*.

*Art. 23* Tests pour contrôler la disponibilité à renseigner

Voir aussi le commentaire des art. 20 à 22

L'art. 19 définit la manière dont les tests prévus à l'art. 22 doivent être préparés et menés à bien pour contrôler la disponibilité à renseigner. La mise en place des services de télécommunication ou des services de communication dérivés nécessaires est du ressort des fournisseurs de services de télécommunication et des fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance. Cet article fixe les étapes pour préparer et exécuter les tests : les fournisseurs doivent tout d'abord mettre à disposition dans leurs systèmes, conformément aux instructions du Service SCPT, les données de test nécessaires pour répondre aux demandes de renseignements durant les tests (*al. 1*). Le Service SCPT leur envoie à cet effet le questionnaire visé à l'art. 31, al. 2, let. b, OSCPT et les demandes à traiter (*al. 2*). Élaboré par le Service SCPT, ce formulaire permet aux fournisseurs de confirmer qu'ils satisfont aux exigences liées aux demandes de renseignements standard qui ne sauraient faire l'objet de tests. Les fournisseurs remplissent ensuite le questionnaire et livrent les renseignements issus des tests (*al. 3*) au Service SCPT.

*Art. 24* Tests pour contrôler la disponibilité à surveiller

Voir aussi le commentaire des art. 20 à 23.

L'art 24 définit la manière dont les tests prévus à l'art. 22 doivent être préparés et menés à bien pour contrôler la disponibilité à surveiller. La mise en place des services de télécommunication ou des services de communication dérivés nécessaires est, ici aussi, du ressort des fournisseurs de services de télécommunication et des fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance. Concrètement, les fournisseurs communiquent au Service SCPT les identifiants (par ex. numéro de téléphone) des services qu'ils ont mis en place (*al. 1*). Le Service SCPT leur fait ensuite parvenir le questionnaire et la liste des mandats de surveillance à mettre en œuvre pour les branchements de test (*al. 2*). Élaboré par le Service SCPT, ce formulaire permet aux fournisseurs de confirmer qu'ils satisfont aux exigences liées aux surveillances standard qui ne sauraient faire l'objet de tests. Les fournisseurs mettent en place les branchements de test et exécutent les tests de manière autonome selon la liste des scénarios de test (*al. 3*). Ils complètent la liste (en précisant par ex. la date, l'heure, la durée des communications et les identifiants des participants à la communication) et la renvoient au Service SCPT avec le questionnaire dûment rempli (*al. 4*).

*Art. 25* Evaluation et confirmation de la disponibilité à renseigner ou à surveiller

Une fois les tests terminés, le Service SCPT examine les questionnaires et les listes des scénarios de test renvoyés par les fournisseurs et analyse les données livrées concernant la surveillance et les renseignements (*al. 1*). Au besoin, il demande aux fournisseurs de répéter certains scénarios de test ou d'effectuer de nouveaux tests (*al. 2*). S'il apparaît qu'il ne sera pas possible de conclure les tests, le Service SCPT peut décider de les interrompre et engager une nouvelle procédure de contrôle (*al. 3*).

Enfin, si le résultat des tests est concluant, le Service SCPT confirme par écrit aux fournisseurs leur disponibilité à renseigner ou à surveiller (*al. 4*).

## **Section 6 Prescriptions techniques**

### *Art. 26*

Les prescriptions techniques relatives à la mise en œuvre de la surveillance et à la fourniture de renseignements sont définies dans les annexes 1 et 2. L'article se contente donc de renvoyer à ces annexes et ne contient pas d'explications détaillées.

## **Section 7 Dispositions finales**

### *Art. 27*            Disposition transitoire

Comme le nouveau système de traitement ne sera pas encore en service au moment de l'entrée en vigueur de l'OSCPT révisée, les demandes de renseignements ne pourront pas encore être exécutées de manière automatisée. Un délai plus long est dès lors accordé aux FST et aux fournisseurs de services de communication dérivés pour le traitement des demandes portant sur les types de renseignements IR\_6\_NA et IR\_12\_TEL.

### *Art. 28*            Entrée en vigueur

L'ordonnance entre en vigueur en même temps que la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication<sup>8</sup> et ses autres ordonnances d'exécution.

<sup>8</sup> RS 780.1

### Vue d'ensemble des délais de traitement<sup>9</sup>

Mandat	Type de mesure	Service SCPT	Fournisseurs de services de télécommunication Fournisseurs de services de communication dérivés	Autres personnes obligées de collaborer
<b>Surveillance en temps réel, correspondance par poste</b> (pendant les heures de bureau)	PO_1_RT_INTERCEPTION PO_2_RT_DELIVERY	≤ une heure	≤ un jour ouvré	
<b>Surveillance rétroactive, correspondance par poste</b> (pendant les heures de bureau)	PO_3_HD	≤ une heure	≤ trois jours ouvrés	
<b>Renseignements</b>	IR_4_NA IR_5_NA_FLEX IR_6_NA IR_7_IP IR_10_TEL IR_11_TEL_FLEX IR_12_TEL IR_13_EMAIL IR_14_EMAIL_FLEX	≤ une heure	≤ une heure	≤ deux jours ouvrés
	IR_8_IP (NAT) IR_9_NAT IR_15_COM IR_16_COM_FLEX IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH	≤ une heure	≤ un jour ouvré	≤ deux jours ouvrés
<b>Surveillance en temps réel</b> (pendant les heures de bureau)	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ une heure	≤ une heure	
<b>Surveillance en temps réel, activation à une date déterminée</b> (pendant les heures de bureau)	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ une heure	Exécuter à la date notée sur l'ordre de surveillance	
<b>Surveillance en temps réel</b> (pendant le service de piquet)	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ une heure	≤ deux heures	

<sup>9</sup> Actualisé le 01.02.2018.



Mandat	Type de mesure	Service SCPT	Fournisseurs de services de télécommunication Fournisseurs de services de communication dérivés	Autres personnes obligées de collaborer
<b>Surveillance rétroactive</b> (pendant les heures de bureau)	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV AS_33_PREP_REF AS_34	≤ une heure	≤ trois jours ouvrés	
<b>Surveillance rétroactive</b> dans les cas d'urgence (pendant les heures de bureau ou le service de piquet)	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV* AS_33_PREP_REF AS_34	≤ une heure	≤ six heures	
<b>Recherches en cas d'urgence</b> pendant les heures de bureau et le service de piquet	EP_35_PAGING EP_36_RT_CC_IRI EP_37_RT_IRI	≤ une heure	≤ une heure	
	EP_38_HD	≤ une heure	≤ quatre heures	
<b>Recherche de personnes condamnées</b> <b>Surveillance en temps réel</b> pendant les heures de bureau et le service de piquet	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ une heure	≤ une heure	
<b>Recherche de personnes condamnées</b> <b>Surveillance rétroactive</b> pendant les heures de bureau et le service de piquet	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV* AS_33_PREP_REF AS_34	≤ une heure	≤ quatre heures	
<b>Désactivations</b> pendant les heures de bureau uniquement	PO_1_RT_INTERCEPTION RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_IRI_CC RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_36_RT_CC_IRI EP_37_RT_IRI	≤ une heure	≤ un jour ouvré	

\* AS\_32\_PREP\_COV (art. 64 OSCPT) n'est pas possible durant le piquet (art. 11 al. 1 let. d OSCPT).