Berne, le 16.02.2022

Révision partielle de quatre ordonnances d'exécution de la LSCPT (OSCPT, OEI-SCPT, OME-SCPT, OST-SCPT)

Rapport explicatif
en vue de l'ouverture de la procédure de consultation

Table des matières

1 Contexte

À l'occasion de la modification du 22 mars 2019 de la LTC[1], un deuxième alinéa a été ajouté à l'art. 2 de la LSCPT[2]. Ce nouvel alinéa[3] donne au Conseil fédéral la compétence de préciser les catégories de personnes obligées de collaborer (POC), en particulier celles visées à l'al. 2, let. b, c et e, LSCPT. Les travaux de mise en œuvre passent par une révision partielle de l'OSCPT[4], ce qui nécessite dans la foulée des révisions partielles de l'OEI-SCPT[5], de l'OME-SCPT[6] et de l'OST-SCPT[7]. Une première consultation des offices a été réalisée en mars 2021. Le 29 avril 2021, le Tribunal fédéral a rendu un arrêt[8] par lequel il a qualifié un fournisseur de fournisseur de services de communication dérivés (FSCD; art. 2, let. c, LSCPT) et non de fournisseur de services de télécommunication (FST; art. 2, let. b, LSCPT), comme l'avait fait le Service SCPT. Une analyse approfondie des conséquences de cet arrêt sur la pratique du Service SCPT va prendre quelque temps, de sorte qu'il a été décidé de scinder en deux la révision partielle de l'OSCPT. Ce premier paquet de la révision (OSCPT, OEI-SCPT, OME-SCPT et OST-SCPT) rassemble toutes les dispositions qui ne touchent pas aux définitions des POC. Il s'agit de dispositions qui adaptent l'OSCPT à la technologie 5G et qui doivent entrer en vigueur rapidement. Les définitions des POC (en particulier la distinction entre FST et FSCD) seront l'objet d'une seconde révision partielle.

Le 19 mars 2021, dans le cadre de la loi fédérale sur des allégements administratifs et des mesures destinées à soulager les finances fédérales, le Parlement a adopté une modification de la LSCPT permettant de calculer au cas par cas ou sous forme de forfaits les indemnités et les participations aux frais (art. 38*a* LSCPT)[9]. Cette modification entraînera une modification de l'OEI-SCPT qui sera présentée dans un projet distinct.

Il faut également mentionner ici le projet de révision en cours en lien avec l'ordonnance sur les mesures policières de lutte contre le terrorisme (OMPT)[10]. La possibilité

1 Loi du 30 avril 1997 sur les télécommunications (**LTC**; RS **784.10**)
2 Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (**LSCPT**, RS **780.1**; voir RO **2020** 6180)
3 RO **2020** 6180. Le Conseil fédéral a décidé le 18.11.2020 que la modification du 22.03.2019 de la LTC entrerait en vigueur le 1.01.2021, mais a remis à une date ultérieure encore non spécifiée l'entrée en vigueur de l'art. 2, al. 1, let. b et 2 LSCPT (RO **2020** 6177).
4 Ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (**OSCPT**, RS **780.11**)
5 Ordonnance du 15 novembre 2017 sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication (**OEI-SCPT**, RS **780.115.1**)
6 Ordonnance du DFJP du 15 novembre 2017 sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (**OME-SCPT**; RS **780.117**)
7 Ordonnance du 15 novembre 2017 sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication (**OST-SCPT**, RS **780.12**)
8 2C_544/2020
9 FF **2021** 669, p. 4/5
10 Procédures de consultation =>Procédures de consultation en cours =>DFJP =>Mise en vigueur partielle de la loi fédérale sur les mesures policières de lutte contre le terrorisme; ordonnance sur les mesures policières de lutte contre le terrorisme =>Projet mis en consultation pour l'OME-SCPT et Projet mis en consultation-2 (OMPT) pour l'OSCPT (p. 12), l'OEI-SCPT (p. 14) et l'OST-SCPT (p. 14)

que donne l'art. 23*q* nLMSI[11] d'utiliser la localisation par téléphonie mobile pour déterminer où se trouve une personne nécessite une adaptation de l'OSCPT, de l'OEI-SCPT, de l'OME-SCPT et de l'OST-SCPT. Toutes ces modifications entraîneront encore, le moment venu, des travaux de coordination avec le présent projet.

2 Procédure préliminaire, notamment procédure de consultation

[sera complété après la consultation]

Texte …

3 Grandes lignes du projet

3.1 Modification de l'OSCPT

La technologie de la téléphonie mobile a évolué depuis l'entrée en vigueur de la LSCPT et de ses ordonnances d'exécution le 1er mars 2018. Elle en est aujourd'hui à la cinquième génération (5G). Il faut donc adapter l'OSCPT aux nouveaux identifiants de la technologie 5G (ressources d'adressage, numéros d'équipements terminaux, numéros d'usagers, etc.) et à l'utilisation d'identifiants temporaires. À cette fin, deux nouveaux types de renseignements sont créés: IR_53_ASSOC_PERM (renseignements sur les identifiants attribués pour une longue durée), dans le nouvel art. 48*a*, et IR_54_ASSOC_TEMP (renseignements immédiats sur les identifiants attribués pour une courte durée), dans le nouvel art. 48*b*.

Trois autres types de renseignements sont également créés à l'occasion de la présente révision de l'OSCPT:

- IR_51_EMAIL_LAST, renseignements sur les services de courrier électronique (art. 42*a*), qui fournit le moment de la dernière activité d'un service de courrier électronique pertinente en termes d'accès. Cette donnée permet de déterminer à quel moment une procédure de communication se termine.
- IR_52_COM_LAST, renseignements sur d'autres services de télécommunication ou services de communication dérivés (art. 43*a*), qui fournit des indications sur la dernière activité d'un autre service de télécommunication ou service de communication dérivé pertinente en termes d'accès.
- IR_55_TEL_ADJ_NET, détermination des réseaux voisins de services de téléphonie et multimédia (art. 48*c*), qui résout des problèmes spécifiques d'identification de l'auteur d'un acte punissable tels qu'ils se posent lorsque le numéro de téléphone de l'appelant est usurpé (*spoofing*) ou inconnu.

11 Dans la loi fédérale du 25 septembre 2020 sur les mesures policières de lutte contre le terrorisme (**MPT**; FF **2020** 7504)

Pour utiliser les nouvelles possibilités qu'offre le «Lawful Access to Location Services» (LALS) pour déterminer la position dans la téléphonie mobile, quatre nouveaux types de surveillances sont créés. Ils permettent la détermination unique ou récurrente de la position par le réseau pour une surveillance en temps réel (art. 56*a* et 56*b*) ou pour une recherche en cas d'urgence (art. 67, al. 1, let. b et c).

Il faut par ailleurs mentionner le nouvel art. 4*a* (début et fin de la surveillance rétroactive), qui vient préciser les règles pour le calcul du délai de six mois et trancher les controverses auxquelles ce calcul a donné lieu dans la pratique. L'art. 20 (saisie d'indications relatives aux personnes dans le cas de services de téléphonie mobile) est complété et restructuré avec désormais un article pour les personnes physiques (art. 20*a*) et un autre pour les personnes morales (art. 20*b*). L'art. 20*a*, al. 5, prévoit désormais une exception à l'obligation de vérifier l'identité et d'enregistrer les données de l'usager. Peuvent exiger d'en bénéficier les autorités de police, le Service de renseignement de la Confédération (SRC) et d'autres groupes de personnes, lorsqu'il existe une base légale les autorisant à ne pas révéler leur véritable identité.

À cette fin, des modifications ponctuelles sont apportées à différentes dispositions et de nouveaux termes et abréviations sont ajoutés à l'annexe.

3.2 Modification de l'OEI-SCPT

L'annexe de l'OEI-SCPT doit être modifiée pour y intégrer les cinq nouveaux types de renseignements et quatre nouveaux types de surveillances qui font leur entrée dans l'OSCPT. Pour les types de renseignements et de surveillances existants, rien ne change.

D'autres modifications ponctuelles sont faites dans les art. 3, 15, 17, al. 3, 18 et 19, al. 1, OEI-SCPT.

3.3 Modification de l'OME-SCPT

Comme le prévoit l'art. 1, al. 2, let. a à f, l'OME-SCPT s'appliquera désormais aussi aux autorités, et non plus uniquement aux POC. L'art. 3 de l'OME-SCPT, qui règle la communication sécurisée, est modifié en conséquence.

Par ailleurs, l'introduction des nouveaux types de renseignements dans l'OSCPT nécessite d'adapter l'art. 14 OME-SCPT, qui fixe les délais de traitement des demandes de renseignements.

Dans la pratique, par ailleurs, le délai d'un jour ouvré prévu par l'actuel art. 14, al. 2, let. b, OME-SCPT est considéré comme trop long par les autorités habilitées à obtenir des renseignements, en particulier pour des demandes faites le week-end ou un jour férié et concernant des renseignements urgents. Pour les « grands » FST et FSCD, le délai est donc ramené à six heures pour le traitement des demandes faites en dehors des heures normales de travail ou les jours fériés (service de piquet). Ce délai correspond à celui prévu pour les surveillances rétroactives urgentes. L'expérience montre qu'il n'y a que peu de demandes de renseignements ou d'ordres de surveillance durant

les heures de piquet, de sorte que ce délai plus court ne devrait pas entraîner une surcharge de travail pour les POC. Pour les autorités de poursuite pénale, en revanche, il est vital de pouvoir obtenir les renseignements dont elles ont un besoin urgent également en dehors des heures ordinaires, afin de ne pas entraver les investigations de la police et la poursuite pénale.

À l'art. 14, al. 3, le délai pour la livraison de renseignements simples par les petites POC diminue également par rapport au droit actuel, puisqu'il est ramené de deux à un jour ouvré, ce qui répond au besoin urgent des autorités de poursuite pénale d'avoir des délais plus courts.

D'autres modifications ponctuelles sont faites dans les art. 10, al. 4 (nouveau), 11, al. 2, 12 et 18, al. 2 et 3, OME-SCPT.

3.4 Modification de l'OST-SCPT

Le présent projet offre pour finir l'occasion de procéder également à une révision partielle de l'OST-SCPT. Outre les accès à l'affichage de la situation des parties du système de traitement auxquelles la personne a accès (PTSS-Dashboard), qui permet de visualiser l'état des composants de surveillance, la révision règle les accès du Service SCPT aux données se trouvant dans le système de traitement (art. 8, al. 3 à 6) et la durée de conservation des fichiers de journalisation des destructions de données (art. 10, al. 4). À l'art. 3, al. 2, let. a à c, une référence à la section 1 du chap. 3 de l'OSCPT est ajoutée (voir ch. 5.4), puisque sont notamment concernés les surveillances et renseignements spéciaux (art. 25) et les types de surveillances avec recherche flexible de nom (art. 27). Enfin un terme est adapté à l'art. 11.

4 Conséquences pour la Confédération, les cantons et les POC

Les modifications prévues des quatre ordonnances (OSCPT, OEI-SCPT, OME-SCPT, OST-SCPT) ne devraient pas avoir de conséquences financières notables, ni pour la Confédération, ni pour les cantons, ni pour les POC. Il faut néanmoins mentionner les conséquences financières minimales suivantes:

- Les nouveaux types de renseignements et de surveillances, ainsi que les adaptations à la technologie 5G, pourront avoir des conséquences financières et économiques pour les POC en fonction des adaptations qu'elles devront apporter à leurs systèmes suite à cette révision partielle. Les POC auront notamment des frais d'investissement pour assurer la mise en œuvre des nouveaux types de renseignements et de surveillances. Les autorités de poursuite pénale contribuent aux coûts d'exploitation des POC par les émoluments qu'elles paient.
- L'intégration des nouveaux types de renseignements et de surveillances dans les composants du système de traitement du Service SCPT nécessitera certaines adaptations du système (nouvelles procédures, modifications des

fonctions, éventuellement nouveaux serveurs, etc.). Des dépenses supplémentaires sont donc à prévoir pour le Service SCPT, mais il devrait pouvoir y faire face avec ses ressources actuelles.

- Les nouveaux types de renseignements et de surveillances seront sans doute assez rarement utilisés, en tout cas beaucoup moins souvent que les types actuels. La charge supplémentaire pour les budgets des cantons sera ainsi vraisemblablement faible. Les émoluments prévus sont du même ordre de grandeur que ceux pratiqués pour les types de renseignements et de surveillances existants. La charge effective pour les autorités de poursuite pénale des cantons dépendra du nombre de mesures de ces nouveaux types qui seront ordonnées, ce qu'on ne peut ni prévoir, ni influencer.
- La contribution de la Confédération à la couverture des coûts devrait elle aussi rester globalement inchangée avec les nouveaux émoluments et indemnités.
- Selon le nouvel art. 15, al. 2, OEI-SCPT, la Confédération peut verser une indemnité aux POC qui apportent leur soutien au Service SCPT mais ne sont pas tenues de fournir elles-mêmes des renseignements ou d'exécuter elles-mêmes des surveillances. Cette nouvelle disposition n'aura toutefois guère de conséquences financières pour les POC ou pour la Confédération, parce que ce cas de figure est assez rare dans la pratique.

5 Commentaire des dispositions

5.1 Ordonnance sur la surveillance de la correspondance par poste et télécommunication

Remarque préliminaire

Le texte de l'ordonnance utilise des formulations du type «le cas échéant», «si disponible», «lorsque ces données sont connues», etc. Ces formulations expriment que les règles énoncées doivent être considérées dans un contexte donné et concernent des fonctions ou des paramètres optionnels, des technologies, des fonctions ou des normes ou versions de normes spécifiques qu'il est impossible de traiter de manière plus détaillée au niveau de l'OSCPT. Dans le cadre de leur obligation de collaborer, les fournisseurs doivent livrer, sur demande du Service SCPT, un exposé détaillé des raisons pour lesquelles ils ne disposent pas de certains paramètres, données ou fonctions, ou sont incapables de les livrer.

Remplacement d'expressions

Al. 1: La pratique a montré que l'identification d'un accès au réseau WLAN donné n'est souvent possible qu'au niveau de la zone d'accès sans fil (*hotspot*), et non du point d'accès lui-même. Le terme «point d'accès au réseau WLAN» est donc remplacé par celui d'«accès au réseau WLAN», qui couvre aussi bien le point d'accès que la zone d'accès sans fil.

Al. 2: La révision de l'OSCPT offre l'occasion d'y introduire le sigle *FSCD*, qui est déjà courant dans la pratique aux côtés de *FST* (voir également la modification de l'art. 1, al. 2, let. j).

Art. 1, al. 1, et al. 2, let. j

À l'*al. 1*, la préposition «à» est ajoutée avant «l'octroi». Cette adaptation rédactionnelle permet de signifier plus clairement que «l'organisation et la procédure» sont applicables également à l'octroi de renseignements.

À l'*al. 2, let. j* le sigle *FSCD* est introduit (cf. le sigle *FST* déjà utilisé à la let. i). Le passage repris de la loi (art. 2, let. c, LSCPT) «fournisseurs de services qui se fondent sur des services de télécommunication et qui permettent une communication unilatérale ou multilatérale» est abandonné, d'une part pour éviter de répéter inutilement le texte de la loi dans l'ordonnance et, d'autre part, parce qu'un nouvel art. 2*b* sera créé pour décrire plus précisément la catégorie des *FSCD*. Le contenu matériel de la disposition n'est en rien modifié.

Art. 3 **Communication au Service SCPT**

La phrase introductive est modifiée pour inclure les autorités qui autorisent les surveillances. La disposition couvre également la possibilité d'utiliser une procédure d'appel pour la saisie de l'autorisation d'une surveillance et des éventuelles conditions posées par l'autorité qui l'autorise. L'autorisation fait partie de l'exécution et du suivi des affaires au sens de l'art. 6, let. f, OST-SCPT, en lien avec l'art. 7, let. e, LSCPT.

À la *let. a,* le moyen de transmission sûr est autorisé non plus par le Service SCPT, mais par le DFJP, concrètement à l'art. 3 OME-SCPT (ordonnance départementale).

Il n'y a pas de changements matériels aux *let. b* et *c*.

La norme étant aujourd'hui l'accès en ligne, l'actuel al. 2 est abrogé car il n'est plus d'actualité.

Art. 4a **Début et fin de la surveillance rétroactive**

Le nouvel art. 4*a* s'appliquant tant à la correspondance postale qu'à la correspondance par télécommunication, il a été placé dans la section 2 «Ordre de surveillance».

La durée maximale d'une surveillance rétroactive est fixée dans la loi. L'autorité qui ordonne la surveillance peut aussi prévoir une durée plus courte. Quelle que soit la durée de la surveillance, les données secondaires peuvent être demandées avec effet rétroactif sur une période de six mois au plus (art. 273, al. 3, CPP[12]). Les fournisseurs doivent donc conserver pendant six mois les données secondaires postales (art. 19, al. 4, LSCPT) et de télécommunication (art. 26, al. 5, LSCPT), ainsi que les données secondaires saisies aux fins de l'identification (art. 21, al. 2, OSCPT, en lien avec art. 21, al. 2 et art. 22, al. 2, LSCPT). L'ordonnance n'a cependant jamais défini ce que ce délai de six mois signifie exactement dans la pratique pour le début et la fin d'une

12 Code de procédure pénale suisse du 5 octobre 2007 (code de procédure pénale, **CPP**; RS **312.0**)

surveillance rétroactive, ni comment ce délai doit être calculé, ce qui a entraîné certaines discussions.

L'*al. 1* définit le «dies a quo»: ce jour à partir duquel le délai de six mois est calculé pour les surveillances rétroactives est celui où le Service SCPT reçoit l'ordre. Ce n'est donc pas le jour où l'autorité émet son ordre, ni celui où elle le transmet[13] qui sont déterminants.

Le choix de calculer le délai à partir de la réception de l'ordre, plutôt qu'à partir de sa transmission, a été fait pour les motifs suivants: lorsque l'ordre est transmis via le WMC[14], ce qui est le cas normal, il ne fait aucune différence que le délai soit calculé à compter de la transmission ou de la réception de l'ordre, vu qu'une poignée de secondes à peine s'écoulent entre le moment où l'autorité transmet son ordre et celui où le Service SCPT le reçoit. Cet écart est en revanche bien plus important pour un ordre envoyé par la poste lorsqu'un moyen de transmission sûr autorisé par le DFJP n'est pas disponible pour des raisons techniques (art. 3 OSCPT): il peut atteindre un jour entier, voire plusieurs jours (voir l'exemple 4 ci-après). Un tel écart pose problème parce que les fournisseurs ont aussi l'obligation d'effacer les données à l'issue du délai de conservation. Dans l'exemple 4 ci-après, le risque serait ainsi plus grand que le fournisseur ait déjà détruit les données requises par l'autorité. Choisir le moment de la réception de l'ordre permet ainsi de réduire au minimum le temps qui s'écoule entre le moment où l'ordre arrive au Service SCPT et celui où le mandat est donné aux fournisseurs concernés.

Il convient de relever que c'est le jour de la transmission de l'ordre au Service SCPT par l'autorité qui en est à l'origine que commence à courir le délai de 24 heures pour la remise de documents au tribunal des mesures de contrainte conformément à l'art. 274, al. 1, CPP[15].

Si l'ordre est téléversé dans le système de traitement du Service SCPT (WMC), c'est ce moment qui est considéré comme le jour de la transmission et de la réception de l'ordre par le Service SCPT (voir l'exemple 2 ci-après). Lorsque l'ordre est donné par téléphone, le moment déterminant est celui de l'appel et non celui de la réception de la confirmation écrite ultérieure (voir l'exemple 3 ci-après).

La surveillance commence ainsi au plus tôt six mois avant le jour de la réception de l'ordre par le Service SCPT, à minuit (00 h 00 et 0 s[16], heure suisse). Pour rappel, l'art. 273, al. 3, CPP prévoit un délai calculé en mois, et non en heures.

13 L'ordre est considéré comme transmis lorsqu'un des moyens prévus à l'art. 3 OSCPT est utilisé (SYLVAIN MÉTILLE, in KUHN/ JEANNERET, Commentaire romand du Code de procédure pénale suisse, Helbling Lichtenhahn, 2e édition 2019, Bâle, ad art. 274, p. 1794, ch. marg. 12).

14 Warrant Management Component (WMC): composant du système de traitement pour la surveillance des télécommunications, en fonction depuis le 18 mars 2019

15 MARC JEAN-Richard-DIT-BRESSEL, in Basler Kommentar, NIGGLI, HEER, WIPRÄCHTIGER, Helbling Lichtenhahn, 2e édition 2014, Bâle, ad art. 274, p. 2168, ch. marg. 4 in fine; SYLVAIN MÉTILLE, op.cit. ad art. 274, p. 1796, ch. marg. 23 («Le délai [de vingt-quatre heures] se compte à la minute près, dès la transmission de l'ordre de surveillance au Service SCPT»)

16 Pour les surveillances rétroactives, le temps est donné à la seconde près, c'est-à-dire arrondi à la seconde.

Le calcul du délai de six mois se fonde sur la doctrine[17] et sur la jurisprudence[18]: «Le délai fixé en mois expire le jour qui correspond, par son quantième, au jour qui l'a déclenché, ou le dernier jour du mois, si le mois en question n'a pas de jour correspondant.»[19] Pour la surveillance rétroactive, cela signifie en d'autres termes qu'un délai fixé en mois commence le jour qui, par son quantième, correspond au jour où le Service SCPT a reçu l'ordre. Le jour du début de la surveillance rétroactive a donc en général le même quantième que le jour (JJ) de la date (JJ.MM.AAAA) de la réception de l'ordre par le Service SCPT.

Le cas particulier dans lequel le mois où débute la surveillance rétroactive n'a pas de quantième équivalent est réglé dans la *deuxième phrase*. Si par exemple le Service SCPT reçoit l'ordre le 31 d'un mois, la surveillance rétroactive débute au plus tôt le trente-et-unième jour du mois, six mois plus tôt. Mais si le mois en question n'a pas 31 jours (par ex. avril), le délai commence le dernier jour dudit mois (en l'occurrence le 30 avril, voir les exemples 2 et 3 ci-après).

Selon l'*al. 2*, une surveillance rétroactive se termine normalement au plus tard le jour de la réception de l'ordre par le Service SCPT, c'est-à-dire ce jour-là à 23 h 59 et 59 secondes[20] heure suisse (voir les exemples 1 à 4 ci-après). Si la surveillance rétroactive est exécutée le jour même – donc avant 23 h, 59 min, 59 s –, l'autorité à l'origine de la requête ne reçoit que les données disponibles jusqu'au moment de l'exécution. Il n'y a pas de deuxième livraison ultérieure du reste des données (données secondaires générées entre le moment de l'exécution de la surveillance et la fin du jour en question). Ce point est important notamment lorsqu'une surveillance rétroactive est déclarée urgente (voir l'exemple 5 ci-après). Si des données pertinentes ne sont disponibles que plus tard en raison de retards habituels (par ex. les données provenant de l'itinérance), le fournisseur n'est pas non plus tenu de les livrer ultérieurement. Si l'autorité qui a donné l'ordre de surveillance a besoin de ces données, elle doit envisager d'ordonner une nouvelle surveillance rétroactive à une date ultérieure (voir l'exemple 5 ci-après).

Les fournisseurs concernés doivent s'assurer de conserver les données secondaires suffisamment longtemps. Ils doivent pour ce faire tenir compte de la règle exposée ci-dessus sur la manière de calculer exactement jusqu'où une surveillance rétroactive peut remonter, et des délais de traitement prévus aux art. 17 et 18 OME-SCPT (voir plus loin le commentaire de l'art. 21, al. 4, OSCPT). Le fournisseur exécute la surveillance rétroactive dans un délai de trois jours ouvrés, dans les cas d'urgence dans un délai de six heures (art. 17, al. 3, OME-SCPT).

Quelques exemples de calcul du délai de six mois sont présentés ci-après. Il faut noter que par défaut, la surveillance commence à 00 h 00, 0 seconde et se termine à 23 h 59, 59 secondes. Les surveillances exécutées le jour même font exception, puisqu'elles se

17 Notamment DANIEL STOLL, in KUHN/ JEANNERET, Commentaire romand du Code de procédure pénale suisse, Helbling Lichtenhahn, 2e édition 2019, Bâle, ad art. 90, p. 430 et 431, ch. marg. 12

18 En particulier ATF 144 IV 161 (arrêt 6B_80/2018 du 25.04.2018)

19 Voir aussi par ex. art. 22, al. 2, de l'ordonnance du 30 août 1995 sur la taxe d'exemption de l'obligation de servir (**OTEO**; RS **661.1**)

20 Pour les surveillances rétroactives, le temps est donné à la seconde près, c'est-à-dire arrondi à la seconde.

terminent à l'heure de leur exécution plus 59 secondes. Les données qui doivent être livrées sont celles qui sont disponibles au moment de l'exécution de l'ordre.

Exemple 1: Ordre daté du mardi 10 novembre 2020, reçu par courriel chiffré au Service SCPT le jeudi **12 novembre 2020** à 9 h 00
→ Début **JJ = 12**, MM: 11 - 6 = 5 → **MM = 5**, **AAAA = 2020**
La surveillance débute au plus tôt le 12 mai 2020, à 00 h 00;
elle se termine au plus tard le 12 novembre 2020, à 23 h 59.

Exemple 2: Ordre téléversé dans le WMC lundi **31 août 2020,** à 18 h 00
→ Début **JJ = 31**, MM: 8 – 6 = 2 → **MM = 02**, **AAAA = 2020**
Le mois de février n'ayant pas 31 jours, on «arrondit» la date au dernier jour de février 2020.
La surveillance débute au plus tôt le 29 février 2020, à 00 h 00;
elle se termine au plus tard le 31 août 2020 , à 23 h 59.

Exemple 3: Ordre donné par téléphone au Service SCPT le dimanche **31 mai 2020**, à 16 h 50
→ Début **JJ = 31**, MM: 5 - 6 = -1 + 12 → **MM** = **11** de l'année précédente, AAAA: 2020 - 1 → **AAAA = 2019**
Le mois de novembre n'ayant pas 31 jours, on «arrondit» la date au dernier jour de novembre 2019.
La surveillance débute au plus tôt le 30 novembre 2019, à 00 h 00;
elle se termine au plus tard le 31 mai 2020, à 23 h 59.

Exemple 4: L'ordre date du mercredi 8 avril 2020, envoyé par la poste le 09 avril 2020 (cachet de la poste), pas de préavis téléphonique. Le Service SCPT reçoit l'ordre après le week-end pascal, mardi **14 avril 2020**, à 9 h 00. Le mandat de surveillance est transmis aux fournisseurs le 14 avril 2020, à 9 h 50.
→ Début **JJ = 14**, MM: 4 - 6 = -2 + 12 → **MM** = **10** de l'année précédente, AAAA: 2020 - 1 → **AAAA = 2019**
La surveillance débute au plus tôt le 14 octobre 2019, à 00 h 00;
elle se termine au plus tard le 14 avril 2020, à 23 h 59.
Remarque : lorsque l'ordre est donné par téléphone, le moment déterminant est celui de l'appel et non celui de la réception de la confirmation écrite ultérieure (cf. l'exemple 3).

Exemple 5: Ordre pour une surveillance rétroactive urgente, téléversé dans le WMC par l'autorité le vendredi **28 août 2020**, **à 16 h 00**, transmis aux POC par le Service SCPT à 16 h 30.
→ Début **JJ = 28**, MM: 8 - 6 = 2 → **MM = 02**, **AAAA = 2020**
La surveillance débute au plus tôt le 28 février 2020, à 00 h 00;
elle se termine au plus tard le 28 août 2020.

L'heure exacte de la fin de la surveillance est le moment où celle-ci est exécutée par la POC (dans un délai maximal de six heures à compter du moment où elle a reçu l'ordre, en l'occurrence à 22 h 30 au plus tard). Pour des raisons techniques, les données secondaires qui viennent d'arriver chez la POC ne sont pas encore prêtes à être livrées. L'autorité qui émet l'ordre de surveillance doit donc faire une pesée d'intérêts entre la rapidité de la livraison et la disponibilité des données secondaires qu'elle souhaite obtenir. La POC peut ne disposer de données secondaires qu'à l'issue d'un délai

de quelques heures. Il faut alors demander une surveillance rétroactive à un moment ultérieur (attention toutefois à la perte des données les plus anciennes) ou, si le temps presse, envisager une surveillance en temps réel «uniquement données secondaires».

Art. 11 Prestations en dehors des heures normales de travail et les jours fériés

Cette disposition règle les prestations du Service SCPT et des POC mentionnées en dehors des heures normales de travail, c'est-à-dire du lundi au vendredi de 17 h 01 à 7 h 59 et toute la journée les week-ends et les jours fériés (cf. art. 10). Durant ces périodes, le Service SCPT et les POC mentionnées assurent un service de piquet. Les délais d'exécution des prestations par le Service SCPT et les POC sont fixés dans l'OME-SCPT, pour les services de piquet comme pendant les heures normales de travail.

L'*al. 1* est adapté et restructuré. Il n'y a que peu de changements matériels pour le Service SCPT, les autorités et les POC. Notamment pour les POC, la levée de dérangements figure déjà dans l'actuelle version de l'art. 11 (al. 1, let. e, en lien avec l'al. 2), de même que la joignabilité 24 heures sur 24 et 7 jours sur 7 («en tout temps», al. 2 in fine). Les FST, à l'exception de ceux qui ont des obligations restreintes en matière de surveillance (art. 51), et les FSCD ayant des obligations étendues en matière de surveillance (art. 52) doivent fournir pendant le service de piquet toutes les prestations mentionnées à l'al. 1, let. a à e. Ne sont en revanche pas tenus d'assurer un service de piquet les FST ayant des obligations restreintes en matière de surveillance (art. 51), les FSCD n'ayant pas d'obligations étendues (c'est-à-dire ceux qui ne remplissent pas les conditions de l'art. 22 ou de l'art. 52), les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22) et les POC visées à l'art. 1, al. 2, let. k, l et m.

Les prestations à assurer durant le service de piquet sont mentionnées exhaustivement aux let. a à e. On notera que pendant les services de piquet, le Service SCPT limite ses prestations de conseil. La *let. a* prévoit la fourniture de certains renseignements standardisés. D'autres renseignements standardisés sont mentionnés à la *let. b*. La *let c* dit quels types de surveillances peuvent être activées pendant un service de piquet, et la *let d*, quels types de surveillances rétroactives peuvent être déclarées urgentes. La *let. e* spécifie les types de recherches en cas d'urgence et de recherches de personnes condamnées qui sont exécutées pendant les services de piquet.

L'*al. 2* consolide la pratique actuelle qui veut qu'en dehors des heures normales de travail, les autorités annoncent tous les mandats par téléphone via le numéro de piquet du Service SCPT, à l'exception des renseignements fournis automatiquement. C'est la seule manière de garantir que les collaborateurs du Service SCPT soient informés à temps des mandats, qu'ils puissent les traiter dans les délais prévus et qu'ils puissent à leur tour informer les POC concernées de ces mandats.

L'*al. 3* reste matériellement inchangé, avec une simple modification rédactionnelle pour reprendre la formule de l'al. 1 («en dehors des heures normales de travail et les jours fériés»). L'al. 3 exclut des services de piquet les surveillances et les renseignements spéciaux (cas spéciaux selon l'art. 25). Il s'agit de renseignements ou de surveillances non standardisés, ne correspondant à aucun des types mentionnés dans

l'ordonnance et qui requièrent l'intervention du Service SCPT ou d'un tiers par lui mandaté. La fourniture de ces renseignements ou l'exécution de ces surveillances sont considérablement plus complexes que pour les types standardisés. Ils ne sont pas planifiables et les ressources en personnel nécessaires sont difficiles à estimer à l'avance. Avoir le personnel nécessaire de piquet au Service SCPT ou chez un tiers entraînerait donc des coûts disproportionnés.

Art. 18 Obligations concernant la fourniture de renseignements par les FST et les FSCD ayant des obligations étendues

L'actuel art. 18 est scindé en quatre (art. 18, 18*a*, 18*b* et 18*c*) pour en améliorer la lisibilité. Ces articles précisent les obligations en matière de fourniture de renseignements.

L'*art. 18, al. 1*, pose le principe selon lequel les catégories de POC suivantes fournissent les renseignements via l'interface de consultation du système de traitement du Service SCPT (IRC[21]):

- les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance (art. 51),
- les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22) et
- les FSCD ayant des obligations étendues en matière de surveillance (art. 52).

Les actuels al. 1 et 4 précisent que les POC fournissent les renseignements «concernant les services qu'[elles] proposent», une redondance qui est abandonnée à la faveur de la révision, bien que l'obligation de fournir des renseignements continue à l'évidence de ne concerner que les services offerts par une POC.

L'*al. 2* indique les renseignements que les POC mentionnées à l'al. 1 doivent livrer de manière automatisée, leur laissant le choix entre la livraison manuelle ou automatisée pour tous les autres renseignements. L'automatisation est imposée pour les renseignements fréquents, simples ou dont il est essentiel qu'ils soient livrés rapidement. Pour les autres renseignements, le choix entre manuel et automatisé est offert par respect pour la liberté économique des POC concernées. L'automatisation nécessite des investissements, mais permet ensuite d'économiser sur les coûts d'exploitation. Un même type de renseignements peut ainsi être livré manuellement par une POC, tandis qu'une autre préférera automatiser la procédure. Concernant les cinq nouveaux types de renseignements, l'automatisation est requise pour les renseignements visés aux art. 42*a* (IR_51_EMAIL_LAST), 43*a* (IR_52_COM_LAST), 48*a* (IR_53_ASSOC_PERM) et 48*b* (IR_54_ASSOC_TEMP), tandis que le choix entre manuel et automatisé est laissé pour les renseignements visés à l'art. 48*c* (IR_55_TEL_ADJ_NET). La fourniture automatisée de renseignements a lieu sans intervention humaine, ni au Service SCPT, ni chez la POC: l'autorité habilitée à obtenir des renseignements saisit sa demande dans l'IRC et les systèmes des POC lui envoient la réponse dans un délai d'une heure au maximum. Pour les procédures manuelles via l'IRC, l'autorité saisit sa demande dans l'IRC et la POC concernée reçoit

21 IRC: *Information Request Component* du système de traitement du Service SCPT; en fonction depuis le 18 mars 2019

alors un avis l'informant qu'une demande doit être traitée. Le collaborateur de la POC se connecte à l'IRC et remplit manuellement le masque de réponse. L'autorité reçoit également la réponse via l'IRC. Pour la fourniture manuelle des renseignements en dehors du système de traitement, l'autorité saisit sa demande dans l'IRC et le Service SCPT la relaie à la POC par écrit, via un moyen de transmission sûr autorisé par le DFJP. La POC peut fournir les renseignements sans forme particulière, et envoie sa réponse au Service SCPT par écrit via un moyen de transmission sûr autorisé par le DFJP. Le Service SCPT répercute la réponse à l'autorité, toujours via un moyen de transmission sûr.

L'*al. 3* prévoit que les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22) sont dispensés de livrer les renseignements visés à l'art. 48*b*. Pour la mise en œuvre de ce type de renseignements à livrer en temps réel, une POC doit investir dans une nouvelle interface et dans le système de fourniture automatisée de renseignements. Compte tenu du principe de proportionnalité, ces charges supplémentaires ne peuvent être imposées qu'aux «grands» FST et aux «grands» FSCD (art. 52). L'al. 3 prévoit également que les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22) ne livrent, pour les renseignements visés aux art. 38, 39 et 48*c*, que les informations dont ils disposent: en effet, l'art. 21, al. 6, let. b et c, ne les oblige pas à conserver les données secondaires en question. Ils doivent fournir ces renseignements pendant les heures normales de travail et peuvent les fournir pendant le service de piquet (art. 11).

L'*al. 4* concerne la fourniture de renseignements par les FST ayant des obligations restreintes en matière de surveillance (art. 51). Eux aussi sont dispensés de fournir les renseignements visés à l'art. 48*b*, pour les mêmes motifs que les FSCD ayant des obligations étendues en matière de fourniture de renseignements (voir commentaire de l'al. 3). L'exigence minimale est la livraison manuelle des renseignements en dehors du système de traitement (voir le commentaire de l'al. 2). Les renseignements peuvent toutefois également être transmis manuellement mais via le système de traitement (IRC, voir le commentaire de l'al. 2). Un FST ayant des obligations restreintes en matière de surveillance (art. 51) peut aussi demander à pourvoir fournir certains renseignements sous forme automatisée. Le Service SCPT décide alors, après concertation, si une mise en œuvre dans l'IRC est possible.

Art. 18a Obligations concernant la fourniture de renseignements par les FSCD n'ayant pas d'obligations étendues et par les exploitants de réseaux de télécommunication internes

Créé pour une meilleure lisibilité, le nouvel art. 18*a* règle les obligations en matière de fourniture de renseignements incombant aux FSCD n'ayant pas d'obligations étendues, ni en matière de fourniture de renseignements (art. 22), ni en matière de surveillance (art. 52), et aux exploitants de réseaux de télécommunication internes.

L'*al. 1* prévoit qu'ils ne sont pas obligés, pour livrer des renseignements, de s'en tenir aux types prévus dans l'ordonnance. Comme ils ne sont pas tenus d'assurer une disponibilité à fournir des renseignements, ils ne doivent livrer que les données dont ils disposent.

L'*al. 2* précise la manière dont ces données peuvent être livrées. L'exigence minimale est que les FSCD n'ayant pas d'obligations étendues et les exploitants de réseaux de

télécommunication internes livrent les données dont ils disposent par écrit, en dehors du système de traitement, en utilisant un moyen de transmission sûr autorisé par le DFJP.

Selon l'al. 3, ils peuvent également livrer ces données via l'interface de consultation du système de traitement, manuellement ou, d'entente avec le Service SCPT, de manière automatisée.

Art. 18b Concours de tiers pour la fourniture de renseignements

Le nouvel art. 18*b*, créé pour une meilleure lisibilité, reprend la possibilité pour les POC de faire appel à des tiers pour la fourniture de renseignements, qui est prévue dans le droit actuel à l'art. 18, al. 1, 2e phrase, et al. 4, 2e phrase.

Art. 18c Communication du nombre d'enregistrements lors de la fourniture de renseignements

Cet article a aussi été créé pour une meilleure lisibilité et reprend la règle figurant jusqu'ici à l'art. 18, al. 6.

Art. 20 Vérification des données relatives aux personnes dans le cas des services de communication mobile

Pour les services de communication mobile, les règles relatives à l'identification sont plus strictes que pour d'autres services tels que les réseaux WLAN (cf. art. 19). Cet article, ainsi que les art. 20*a* et 20*b*, s'appuient sur les normes de délégation au Conseil fédéral que l'on trouve dans les art. 21, al. 1, let. d, 22, al. 2 et 23, al. 1, LSCPT. Les différentes dispositions relatives aux personnes physiques (art. 20*a*) et aux personnes morales (art. 20*b*) sont complétées et clarifiées.

L'*al. 1* pose le principe. Lors de la remise du moyen d'accès à des services de communication mobile (par ex. GSM, GPRS, UMTS, LTE, VoLTE, VoWiFi, 5G) ou, si les services doivent être activés pour que l'usager puisse les utiliser, lors de la première activation du service, les FST ou les revendeurs (al. 2) doivent vérifier, pour les personnes physiques, l'identité de l'usager (let. a), et pour les personnes morales, les indications que celles-ci fournissent (let. b).

L'activation d'un service est le moment à partir duquel un usager peut utiliser le service en question. Pour les moyens d'accès utilisables immédiatement, l'activation a normalement lieu lors de leur remise. Pour une carte SIM intégrée dans un appareil (*embedded SIM*, SIM embarquée; eSIM), le profil correspondant est en général activé par le fournisseur. Il peut aussi activer le service en retirant un éventuel dispositif de blocage. Par exemple, lorsqu'un commerce d'appareils électroniques vend une tablette dotée d'une eSIM permettant d'accéder à la communication mobile, le client qui l'achète ne peut pas l'utiliser pour accéder à l'internet avant que l'eSIM soit activée ou débloquée. Le client doit donc faire activer l'eSIM de sa tablette par un fournisseur de services de communication mobile avant de pouvoir utiliser ce moyen d'accès au réseau téléphonique mobile. Le moyen d'accès fait partie intégrante de la tablette et il est «remis» au client au moment de la vente. Mais comme il ne peut pas encore fonctionner au moment de sa remise, c'est le moment où il est activé, et donc utilisable

dans le réseau téléphonique mobile, qui intéresse les autorités de poursuite pénale. Il est par ailleurs important de savoir qui doit vérifier l'identité de l'usager et enregistrer les données le concernant. Dans cet exemple, ce n'est pas le commerce d'appareils électroniques qui active le moyen d'accès au réseau mobile. Il n'est donc pas tenu d'enregistrer les données du client, puisqu'il n'est pas considéré comme un revendeur professionnel de cartes ou de moyens semblables (art. 2, let. f, LSCPT). Cette tâche incombe à l'opérateur de téléphonie mobile, en sa qualité de FST, lorsqu'il charge puis active le profil de l'usager sur l'eSIM (carte SIM virtuelle comme moyen d'accès au réseau de téléphonie mobile).

L'*al. 2* précise que la vérification de l'identité d'un usager ou des indications fournies par une personne morale incombe au revendeur professionnel (art. 2, let. f, LSCPT) lorsque c'est lui qui remet le moyen d'accès ou qui active directement le service pour la première fois. Lorsque par exemple le moyen d'accès est remis dans la boutique d'un revendeur professionnel, c'est à lui de procéder à la vérification de l'identité de l'usage, de faire une copie du moyen d'identification présenté (par ex. carte d'identité) et de transmettre ensuite au FST les données requises concernant la personne et la copie électronique de la pièce d'identité, conformément à l'art. 20*a*, al. 4. Dans ce cas, le FST n'a pas d'autres vérifications à faire concernant les données de l'usager. Le FST doit toutefois veiller d'une manière appropriée à ce que les revendeurs professionnels identifient et enregistrent correctement les usagers, et lui transmettent ensuite ces données. Il doit en effet être en mesure de livrer ces informations si on les lui demande, et il ne peut invoquer les manquements du revendeur pour se soustraire à ses obligations.

On peut supposer que lors de contacts ultérieurs dans le courant de leurs relations commerciales avec leurs clients, les FST vérifient et mettent à jour les données les concernant, parce qu'ils ont un intérêt à le faire. Lorsqu'un client déménage, par exemple, et que le FST en est informé, il enregistrera la nouvelle adresse dans son fichier clients. Lors d'une éventuelle demande de renseignements, il livrera, en plus des données clients prescrites, d'autres coordonnées (par ex. nouvelle adresse) et leur période de validité. Il n'y a cependant pas d'obligation de vérifier en continu ces données et de les maintenir à jour en tout temps. La mise à jour de données concernant la personne qui auraient changé depuis l'enregistrement initial n'est en particulier pas exigée. Le FST qui aurait connaissance d'un changement des données relatives à client doit simplement le communiquer lors d'une éventuelle demande de renseignements.

Art. 20a Preuve d'identité des personnes physiques pour les services de communication mobile

L'*al. 1* contient la liste exhaustive des moyens d'identification admis. D'autres documents, par exemple un permis de conduire, ne sont pas admis. Le passeport (*let. a*) et la carte d'identité (*let. b*) peuvent être suisses ou étrangers. La vérification de l'identité du client au moyen d'un de ces documents est impérative pour les services de téléphonie mobile. Cette règle valait autrefois uniquement pour les services de téléphonie mobile à prépaiement, mais elle a été étendue à tous les services de téléphonie mobile, quelles que soient les modalités de paiement (abonnement, prépaiement, gratuit), lors

de la révision totale de la LSCPT[22]. Dans la pratique, les opérateurs de téléphonie mobile exigent depuis longtemps déjà la présentation d'une pièce d'identité lors de la conclusion d'un abonnement. Le fournisseur ou le revendeur professionnel n'a pas l'obligation d'examiner minutieusement le document présenté pour s'assurer de son authenticité. Il en serait d'ailleurs incapable, car il n'a pas les moyens de vérification dont dispose par exemple une autorité de police. Il est cependant tenu de n'accepter le document présenté que si son authenticité paraît plausible. Un fournisseur ou un revendeur professionnel qui accepte un document d'identité pouvant facilement être reconnu comme un faux, ou n'étant manifestement pas celui de la personne qui le présente, s'expose à des sanctions de droit pénal administratif (cf. art. 39 LSCPT).

Les *let. a* à *c* reprennent les documents d'identité qui figurent dans l'actuel art. 20, al. 1. Un client qui souhaite s'identifier auprès d'un opérateur au moyen d'un de ces documents devra généralement se présenter en personne. La procédure de vérification d'identité elle-même n'étant pas réglementée, une identification par vidéo ou en ligne est cependant possible[23]. Dans ce cas, il y a lieu de respecter les normes de sécurité et de qualité définies dans la circulaire de la FINMA 2016/7 «Identification par vidéo et en ligne»[24] pour l'identification en ligne dans le domaine bancaire.

Le document d'identité (let. a à c) doit être valable le jour de sa saisie. Ce jour est celui où ce document est présenté au fournisseur ou au revendeur. Une identification sûre ne peut être garantie qu'avec un document en cours de validité. Dans la pratique, on a constaté que des documents périmés pouvaient donner lieu à des enregistrements non valables.

Les indications citées à l'*al. 2* correspondent à celles qui se trouvent dans l'actuel art. 20, al. 2, et s'appuient sur l'art. 21, al. 1, LSCPT. Le FST ou le revendeur doit veiller à ce que les données relatives à la personne soient saisies correctement, sur la base du document présenté. Pour les documents physiques, la copie de la pièce d'identité présentée servira au contrôle. Si le document d'identité présenté dispose d'une zone de lecture optique (*machine-readable zone*, MRZ), il est recommandé de l'utiliser et de saisir les données qu'elle contient comme suit:

- Nom(s) et prénom(s) de la MRZ comme alias ou identité secondaire. Comme ces noms sont donnés dans un jeu de caractères latins réduit (translitération), ils peuvent être utilisés directement pour une recherche de nom normale, c'est-à-dire lettre à lettre (voir art. 35).

Pour les indications suivantes concernant la personne ou le document d'identité présenté, il est préférable d'utiliser les données issues de la MRZ, si elles sont disponibles, plutôt que de procéder à une saisie manuelle:

- Pays ou organisation qui a établi le document (sigle de trois lettres);
- Numéro du document d'identité;

22 Selon l'arrêt de la CourEDH du 30.01.2020 (Az. 50001/12) dans la procédure Breyer c. Allemagne, l'identification obligatoire lors de l'achat de cartes SIM prépayées ne constitue pas une violation du droit au respect de la vie privée garanti par l'art. 8 CEDH.

23 Cf. également art. 6, al. 4, let. b, de l'ordonnance du DFJP sur le blanchiment d'argent **(OBA-DFJP**; RS **955.022)** et art. 5, al. 1, let. e, de l'ordonnance de la CFMJ sur le blanchiment d'argent (**OBA-CFMJ**; RS **955.021**)

24 finma.ch =>Documentation => Circulaire

- Nationalité (sigle de trois lettres);
- Date de naissance;
- Sexe (H=homme / F=femme / <=pas d'indication).

L'adresse (*let. b*) et la profession (*let. c*), qui ne figurent pas dans les documents d'identité, doivent être saisies selon les indications données par le client. Le FST ou le revendeur doit s'assurer que ces indications sont plausibles et qu'il ne s'agit pas de renseignements manifestement faux ou fantaisistes.

L'*al. 3* correspond à l'actuel art. 20, al. 4. Pour les relations commerciales sans abonnement (prépaiement, offres gratuites), les FST et les revendeurs professionnels doivent également enregistrer d'autres indications. Ne sont ici pas concernées les simples cartes prépayées qui permettent de téléphoner mais qui ne sont pas des cartes SIM. Ces indications supplémentaires doivent être enregistrées pour qu'il soit possible, le cas échéant, de retrouver qui a procédé à des enregistrements non valables (voir la disposition pénale à l'art. 39, al. 1, let. c, LSCPT). On notera qu'un FST doit bloquer l'accès aux services de télécommunication lorsqu'une relation commerciale sans abonnement (prépaiement, offre gratuite) repose sur un enregistrement non valable (art. 6*a* LTC). Le nom et l'adresse mentionnés à la *let. b* doivent être saisis de manière complète et dépendent de qui procède à la saisie, par exemple le point de vente d'un revendeur, un centre d'appels du FST qui active le moyen d'accès, ou un bureau de poste qui réalise la vérification d'identité. Pour les identifications par vidéo ou en ligne, on saisira le nom et l'adresse du service responsable. La *let. c* impose enfin la saisie complète des noms et prénoms de la personne qui a procédé à la saisie ou de la personne responsable d'une identification par vidéo ou en ligne. On entend par-là la personne qui a concrètement saisi les indications visées à l'al. 3 ou, si la saisie est automatisée, la personne qui a la responsabilité de la saisie (voir aussi la disposition pénale à l'art. 39, al. 1, let. c, LSCPT).

L'*al. 4, première phrase,* exige du FST ou du revendeur qu'il fasse une copie du document d'identité présenté, comme c'est déjà le cas aujourd'hui. Cette mesure reste nécessaire en raison des nombreux enregistrements non valables des indications relatives aux personnes constatés dans le passé. La copie de la pièce d'identité semble actuellement le meilleur moyen de prévenir ce type d'enregistrements non valables. Il doit s'agir d'une copie électronique (par ex. photo, scan) clairement lisible. Les simples photocopies ne permettent plus de répondre aux nouvelles exigences. La durée de conservation pour les FST est réglée à l'art. 21, al. 3. La *deuxième phrase* fixe un délai au revendeur pour la transmission au FST des indications saisies conformément aux al. 2 et 3, et de la copie de la pièce d'identité. Ce délai est de 14 jours, afin qu'il soit raisonnable même pour un petit revendeur. L'objectif de cet alinéa est de délimiter plus clairement les responsabilités (voir aussi la disposition pénale à l'art. 39, al. 1, let. c, LSCPT).

L'*al. 5* prévoit désormais une exception à l'obligation de vérifier l'identité et de saisir les informations correspondantes. Peuvent demander à en bénéficier les autorités de police de la Confédération et des cantons, ainsi que le Service de renseignement de la Confédération (SRC), pour des personnes de leur organisation ou pour d'autres groupes de personnes que des dispositions légales autorisent à ne pas révéler leur véritable identité.

La vérification de l'identité prévue à l'al. 1 ne souffre aujourd'hui aucune exception, ce qui, dans la pratique, s'est révélé particulièrement problématique ces dernières années pour les membres d'autorités de police et les collaborateurs du SRC. Chez les FST et les revendeurs professionnels, un nombre de personnes important et difficile à contrôler a en effet accès aux systèmes et donc aux données nécessaires à la fourniture des renseignements. L'identité des usagers n'est ainsi pas suffisamment protégée, ce qui est un problème en particulier pour les membres d'autorités de police et les collaborateurs du SRC.

Les agents affectés aux recherches secrètes (art. 298*a* ss CPP) sont chargés par la loi d'élucider des crimes et des délits. À cette fin, ils ont le droit de conclure des transactions fictives ou de donner l'illusion de vouloir conclure de telles transactions (art. 298*a*, al. 1, CPP). La loi prévoit que leur véritable identité et leur fonction ne doivent pas être reconnaissables durant toute l'intervention. La révélation de l'identité d'un agent affecté à des recherches secrètes non seulement compromet l'objectif de sa mission (qui est d'élucider des infractions graves), mais peut aussi l'exposer à un danger considérable pour sa vie et son intégrité corporelle, en particulier lorsque les infractions sur lesquelles il enquête sont le fait d'une organisation criminelle au sens de l'art. 260ter CP. Or les lacunes de sécurité concernant les autorisations d'accès chez les FST sont précisément de nature à mener à des situations dangereuses pour les agents concernés.

Les agents infiltrés (art. 151 et 285*a* ss CPP) sont dotés d'une identité d'emprunt, ce qui n'est pas le cas des agents affectés à des recherches secrètes (art. 298*a*, al. 2, CPP). Cette différence est justifiée par la proportionnalité, des agents infiltrés n'étant engagés que dans la poursuite d'infractions particulièrement graves dont la liste se trouve à l'art. 286, al. 2, CPP.

Les agents du SRC interviennent dans diverses fonctions dans des situations où la divulgation de leur identité réelle et de leur appartenance au SRC peut entraîner une menace directe pour leur intégrité personnelle ou celle de personnes de leur entourage; leur mission peut aussi s'en trouver compromise. Ils peuvent d'abord être menacés directement par les personnes qu'ils ont contactées. Ils peuvent aussi, dans le contexte d'une mission de contre-espionnage, subir des inconvénients graves pouvant aller jusqu'à leur arrestation lors d'un déplacement dans un pays visé par une action de contre-espionnage du SRC

Dans leurs activités de recrutement et de gestion d'informateurs, les collaborateurs du SRC ont besoin de numéros de téléphonie mobile anonymisés, renouvelés fréquemment ou destinés à un usage unique. Les personnes qui utilisent ces raccordements ne doivent pas pouvoir être identifiées facilement. Pour l'observation de personnes gravitant dans l'environnement des services de renseignement, le SRC doit aussi changer fréquemment les raccordements de communication utilisés, afin de ne pas être reconnaissable trop aisément. La partie adverse peut recourir – en toute illégalité – à un IMSI-Catcher et tenter d'identifier l'utilisateur d'un numéro trop voyant.

La possibilité donnée par la loi au SRC de travailler sous des identités d'emprunt ne suffit pas pour l'acquisition du grand nombre de raccordements mobiles anonymisés dont il a besoin. Le SRC doit pouvoir se fournir auprès des opérateurs de téléphonie mobile pour obtenir des raccordements anonymisés en grandes quantités (plusieurs

centaines par année). Selon l'art. 18 de la loi fédérale sur le renseignement (LRens), ce ne sont pas uniquement les collaborateurs du SRC qui peuvent être dotés d'une identité d'emprunt, mais également les collaborateurs des autorités d'exécution cantonales et, sous certaines conditions, les informateurs du SRC.

Les FST ne sont aujourd'hui pas tous en mesure de garantir que leurs systèmes ne présentent pas des failles qui pourraient être exploitées pour identifier des agents sous couverture, posant ainsi une menace à leur vie et à leur mission. Les FST doivent donc mettre en place des solutions techniques garantissant que les autorités de police et les agents du SRC puissent effectuer leur travail sans être entravés ou mis en danger. Aujourd'hui, la simple absence d'un document d'identité dans le système d'un FST permet parfois de conclure que l'usager est en fait un agent d'une autorité de sécurité.

Art. 20b Preuve d'identité des personnes morales pour les services de communication mobile

L'*al. 1* règle les indications à saisir concernant les personnes morales. Elles correspondent à celles de l'actuel art. 20, al. 3. En général, ces indications proviennent d'un extrait du registre du commerce ou du registre d'identification des entreprises (IDE) tenu par l'Office fédéral de la statistique. La nouveauté est la saisie désormais possible du *Legal Entity Identifier* (LEI), selon le système international d'identification des acteurs des marchés financiers (let. b). Pour les personnes morales, on saisira en principe l'UID ou le LEI. La personne visée à la let. c qui utilisera les services du fournisseur peut être par exemple le collaborateur d'une entreprise qui reçoit une carte SIM de son employeur.

L'*al. 2* correspond à l'art. 20*a*, al. 4, deuxième phrase.

Enfin l'*al. 3* renvoie à l'art. 20*a*, al. 3 («relations commerciales sans abonnement»).

Art. 21 Délais de conservation

Cet article a été complètement remanié afin de mieux structurer, de compléter et de clarifier les règles relatives aux périodes de conservation pour les différentes catégories de données. Pour la présente révision, l'expression compacte *FSCD ayant des obligations étendues* est utilisée, que ces obligations étendues concernent la fourniture de renseignements (art. 22) ou la surveillance (art. 52). Les principaux délais ne sont pas modifiés: les données clients (*subscriber data*) doivent être conservées pendant la durée de la relation commerciale ainsi que six mois après la fin de celle-ci (al. 1 et 3), les données d'utilisation, pendant six mois (al. 2 et 4) et les données relatives à l'identification des utilisateurs finaux d'accès publics au réseau WLAN, pendant la durée de l'autorisation d'accès ainsi que six mois après la fin de celle-ci (al. 5).

Les indications relatives aux identifiants attribués à long terme selon l'art. 48*a* ont été ajoutées à l'*al. 1*.

Le nouvel *al. 2* règle les délais de conservation des données d'utilisation relatives aux accès à des services de courrier électronique et à d'autres types de services de télécommunication ou services de communication dérivés. Ces indications sont requises pour les nouveaux types de renseignements prévus aux art. 42*a* et 43*a*.

La formule générale *indications saisies aux fins de l'identification*, utilisée jusqu'ici, est désormais précisée dans les différents alinéas. Il s'agit le plus souvent des données clients (al. 1 et 3), mais aussi, dans certains cas, des données d'utilisation (al. 2, 4 et 5). Suite à la précision de la formule générale *indications saisies aux fins de l'identification*, l'al. 3 a été ajouté pour régler explicitement, pour la téléphonie mobile, les délais de conservation des indications sur les usagers et de la copie du document d'identité. Il s'agit concrètement des indications relatives à la personne saisies lors de l'enregistrement et, pour les personnes physiques, également la copie électronique du document d'identité présenté. Ces points étaient jusqu'ici réglés de manière implicite dans l'actuel al. 1.

Les données relatives à l'attribution et à la traduction d'adresses IP et de numéros de ports étaient jusqu'à présent mélangées dans l'actuel al. 2, let. b. Elles seront désormais réglées séparément, selon que l'attribution est ou non univoque: les données relatives à l'attribution univoque d'adresses IP dans le nouvel *al. 4* et les données relatives à l'attribution non univoque et à la traduction (NAT) d'adresses IP et de numéros de ports dans le nouvel *al. 6, let. b*. Parmi les adresses IP attribuées de manière univoque, on distingue les attributions fixes des attributions dynamiques. Les premières, comme toutes les données clients, doivent être conservées pendant la toute durée de la relation commerciale et six mois au-delà. Les secondes sont des données d'utilisation, pour lesquelles la durée de conservation est de six mois.

L'*al. 5* reprend la deuxième phrase de l'actuel al. 1, en remplaçant l'expression «point d'accès public au réseau WLAN» par «accès public au réseau WLAN» (voir le commentaire sur le remplacement d'expressions, al. 1).

Les données visées à l'*al. 6* sont des données d'identification selon l'art. 22, al. 2, deuxième phrase, LSCPT. L'*al. 6* reprend l'actuel al. 2 et lui ajoute une *let. c* fixant la durée de conservation des données secondaires permettant de déterminer les réseaux immédiatement voisins pour les renseignements selon l'art. 48*c* (voir le commentaire de cet article). La mention de la livraison des données est abandonnée afin qu'il soit clair que ces données doivent être conservées à des fins d'identification, mais qu'il ne s'agit pas de les livrer dans le cadre d'une demande de renseignements, puisqu'il s'agit de données secondaires. La POC ne fait qu'analyser ce type de données secondaires pour identifier un utilisateur. Elle livre ensuite les indications requises selon la demande de renseignements. Une POC ne peut livrer les données secondaires elles-mêmes que dans le cadre d'une surveillance (en temps réel ou rétroactive), même si les données secondaires visées à la let. b ne font pas partie d'un type de surveillance standardisé.

L'*al. 7* correspond à l'actuel al. 3, avec un renvoi désormais à l'al. 6 (plutôt qu'à l'al. 2), et règle la destruction des données secondaires dont il est question.

Remarque : Il n'est pas nécessaire de conserver des indications concernant les identifiants attribués pour une courte durée visés à l'art. 48*b*. En raison de la dynamique très fluctuante de ces attributions, les demandes pour ce type de renseignements ne sont possibles qu'en temps réel (voir le commentaire de l'art. 48*b*.)

Art. 26 Types de renseignements en général

L'*al. 1* est tout d'abord restructuré, la liste des types de renseignements comprenant désormais uniquement des lettres, et non plus un mélange de chiffres et de lettres. Les quatre nouveaux types de renseignements sont ensuite ajoutés dans la liste: l'art. 42*a* (IR_51_EMAIL_LAST, renseignements sur les services de courrier électronique) et l'art. 43*a* (IR_52_COM_LAST, renseignements sur d'autres services de télécommunication ou services de communication dérivés), à la *let. b*. La nouvelle *let. h* mentionne l'art. 48*a* (IR_53_ASSOC_PERM, renseignements sur les identifiants attribués pour une longue durée) et l'art. 48*b* (IR_54_ASSOC_TEMP, renseignements immédiats sur les identifiants attribués pour une courte durée) et la nouvelle *let. i*, l'art. 48*c* (IR_55_TEL_ADJ_NET, détermination des réseaux voisins). À la *let. d*, par ailleurs, le terme de «copie de la pièce d'identité» est remplacé par l'expression plus générale de «preuve de l'identité», puisqu'il est désormais possible d'utiliser des identités électroniques.

À l'*al. 2*, l'expression «fournisseurs» est remplacée par celle plus indiquée ici de «personnes obligées de collaborer». En effet, les exploitant de réseaux de télécommunication internes (art. 2, let. d, LSCPT) et les personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers (art. 2, let. e, LSCPT) sont eux aussi tenus de fournir des renseignements. Sans être des fournisseurs, ils sont cependant couverts par le terme générique de POC. L'obligation vaut également pour les POC qui, en raison de leurs obligations restreintes, n'ont pas besoin de respecter les types standardisés et peuvent fournir les renseignements sous la forme qu'elles souhaitent.

Art. 28 Types de surveillances

Cet article, qui présente une vue d'ensemble des différents types de surveillances, est complété pour inclure les quatre nouveaux types permettant de déterminer une position (deux pour la surveillance en temps réel et la recherche de personnes condamnées, deux pour les recherches en cas d'urgence). Quelques adaptations sont faites dans les désignations des types de surveillances existants.

Dans l'*al. 1*, les *let. a à c* restent pour l'essentiel inchangées. La *let. d* est nouvelle et renvoie aux deux nouveaux types de surveillances en temps réel visant à déterminer une position (LALS, voir art. 56*a* et 56*b*). En raison de cet ajout, l'actuelle let. d devient la *let. e*.

Le type de surveillance visé à l'*al. 2*, *let. c* se nomme désormais *détermination de la position lors de la dernière activité* (voir aussi le commentaire de l'art. 63).

À l'*al. 3, let. a*, le type de recherche en cas d'urgence visé est désormais la *détermination de la position lors de la dernière activité* (voir art. 67, al. 1, let. a). La *let. b* est nouvelle et renvoie aux deux nouveaux types de recherches en cas d'urgence visant à déterminer la position (LALS, voir art. 67, al. 1, let. b et c). Les *let. c*, *d* et *e* restent inchangées et reprennent les actuelles let. b, c et d. Seuls les renvois aux dispositions entre parenthèses sont adaptés.

Le type de surveillance visé à l'*al. 4*, *let. a* se nomme désormais *détermination de la position lors de la dernière activité* (voir aussi le commentaire de l'art. 63). La *let. b*

est nouvelle et renvoie aux deux nouveaux types de recherches de personnes condamnées visant à déterminer la position par le réseau (LALS, voir art. 68, al. 1, let. b et c). Les *let. c*, *d* et *e* restent inchangées et reprennent les actuelles let. b, c et d. Seuls les renvois aux dispositions entre parenthèses sont adaptés. La *let. f* renvoie à la recherche par champ d'antennes, qui est déjà possible aujourd'hui pour une recherche de personnes condamnées (art. 68, al. 1, let. g, actuellement let. d).

Art. 30, al. 3

L'*al. 3* est complété par une deuxième phrase qui prévoit que les POC permettent au Service SCPT de réaliser les branchements de test nécessaires. Ce complément est indispensable parce que dans certains cas, les POC ne sont pas en mesure de mettre à disposition les branchements de test, comme le prévoit la première phrase. C'est alors le Service SCPT, ou un tiers mandaté par lui, qui réalise les branchements de test. Ce cas se présente en particulier chez les POC qui n'ont pas d'obligations actives en matière de surveillance (c'est-à-dire qui ne sont pas tenues d'assurer leur disponibilité à surveiller). Des branchements de test peuvent aussi être réalisés pour des surveillances spéciales (art. 25). Les POC doivent tolérer les surveillances exécutées par le Service SCPT ou des personnes mandatées par celui-ci (art. 26, al. 2, let. b, LSCPT). Les obligations accessoires prévues dans ce cadre (voir le message du 27.02.2013 concernant la LSCPT, commentaire de l'art. 26, al. 2, FF 2013 2435) comprennent l'obligation de permettre au Service SCPT de réaliser des branchements de test en lien avec une surveillance, par exemple pour s'assurer du fonctionnement correct de ladite surveillance. Pour la réalisation de ces branchements de test, les POC doivent donner sans délai accès à leurs installations au Service SCPT ou au tiers mandaté par lui (voir art. 53, al. 1).

Art. 35, al. 1, let. b, c et d, phrase introductive (ne concerne que l'allemand), et ch. 2, 9 à 13, al. 2, phrase introductive, et let. g, i, j et k, et al. 3

À l'*al. 1, let. b, ch. 1*, les renvois aux indications actuellement réglées à l'art. 20 sont adaptés. L'art. 20 règle désormais la vérification des données des usagers des services de communication mobile, les dispositions relatives à la preuve d'identité se trouvant à l'art. 20*a* pour les personnes physiques et à l'art. 20*b* pour les personnes morales. Au *ch. 2* la précision de la période de validité est ajoutée concernant les «autres coordonnées». On entend par période de validité la période (date de début et, le cas échéant, date de fin) durant laquelle la POC a ou avait connaissance des coordonnées en question. Ces autres coordonnées sont par exemple des adresses postales ou électroniques, ou encore des numéros de téléphone qui lui auraient été communiqués. La POC fournit les données dont elle dispose. Elle n'a pas l'obligation de saisir et de tenir à jour toutes les coordonnées de ses clients.

À l'*al. 1, let. c*, les mêmes modifications sont faites qu'à la let. b. La *let. c* est applicable à tous les services d'accès au réseau qui ne sont pas des services de communication mobile. Il convient en outre de rappeler ici que, comme c'est déjà le cas aujourd'hui, les indications saisies aux fins de l'identification par des moyens appropriés, selon l'art. 19, doivent également être livrées. La pratique a montré qu'en raison des nombreuses possibilités pour cette identification et saisie de données, il n'est pas possible de prescrire une structure particulière pour les données à livrer. Elles peuvent

donc être restructurées avant la livraison, mais elles doivent être désignées de manière claire afin que les autorités qui les ont requises puissent mieux comprendre leur signification, par exemple MSISDN, numéro de carte de crédit, numéro de pièce d'identité, numéro ID, carte d'embarquement, MRZ, nom d'utilisateur IPASS.

Dans la phrase introductive de l'*al 1, let. d*, une adaptation rédactionnelle est faite dans le texte allemand pour répondre aux exigences de la formulation non sexiste.

À l'*al. 1, let. d, ch. 2,* deux modifications sont proposées. D'abord, le terme d'*identifiant du service* est remplacé par celui d'*identifiant principal du service*, car certains abonnements de téléphonie mobile proposent aujourd'hui plusieurs cartes SIM qui peuvent être utilisées simultanément dans plusieurs équipements terminaux. Dans ces offres dites multi-SIM ou multi-appareils, une hiérarchie est installée au sein de l'abonnement, avec un maître (numéro principal) et des esclaves (numéros annexes). L'usager peut parfois lui-même modifier cette hiérarchie en déterminant laquelle des cartes SIM utilise le numéro principal à un moment donné. Plusieurs MSISDN sont ainsi subordonnés à un IMSI. Dans un cas simple, un seul MSISDN est subordonné à un IMSI. Les numéros annexes sont des numéros techniques qui ne sont pas connus de l'usager. S'il n'y a qu'une seule carte SIM, c'est elle qui est le numéro principal et il n'y a pas de numéros annexes. Ces offres multi-SIM ou multi-appareils ont des conséquences pour la fourniture de renseignements, les surveillances, les recherches en cas d'urgence et les recherches de personnes condamnées.

Deuxièmement, un nouvel identifiant du système 5G, le *Generic Public Subscription Identifier* (GPSI), remplace, dans les exemples cités, l'actuel *identifiant DSL* de connexion internet à haut débit sur les réseaux fixes. Ce remplacement s'impose parce que le *GPSI* gagne proportionnellement en importance. Le *GPSI* remplace dès lors l'*identifiant DSL* dans tous les exemples cités dans l'ordonnance, puisque ces exemples doivent dans la mesure du possible être typiques et actuels. Cela ne signifie pas pour autant que l'identifiant DSL ne doit plus être livré (et il en va de même de tous les autres remplacements dans les exemples cités). Le *GPSI* est un identifiant public utilisé aussi bien dans le système 3GPP qu'en dehors de celui-ci. Il est soit un MSISDN (par ex. +41791234567), soit un identifiant externe de la forme <username>@<domain_name> (par ex. max.maier@mnc999.mcc228.csp.ch). Le GPSI est utilisé en particulier pour l'adressage d'un service 3GPP dans des réseaux en dehors du système 3GPP, par exemple lorsque l'utilisateur accède au réseau via une zone d'accès sans fil au WLAN plutôt que par le réseau téléphonique mobile. L'élément 3GPP signifie dans chaque cas qu'il s'agit d'un système de téléphonie mobile (*système 3GPP*) ou d'un service (*service 3GPP*) répondant à la norme 3GPP.

Un autre identifiant qui n'est pas cité à titre d'exemple mais qui doit être livré le cas échéant est l'OTO-ID, qui désigne de manière unique une connexion à la fibre optique dans un foyer (*fiber to the home*).

Le *ch. 9* reste inchangé quant au fond. Seul le terme de numéro SIM s'efface au profit du terme technique et universel ICCID (voir l'annexe pour une définition), parce que la fonction classique d'une carte SIM peut aujourd'hui être remplie par d'autres composants matériels (SIM embarquée, eSIM) et qu'on ne sait pas toujours ce qu'on entend exactement par numéro SIM. Le terme ICCID est en revanche univoque pour toutes les formes de SIM.

Le *ch. 10* mentionne désormais en plus de l'*IMSI* le *SUPI*, qui est son équivalent dans le système 5G. Dans le système 5G, chaque usager se voit attribuer un SUPI ou *Subscription Permanent Identifier*. Le *SUPI* est un identifiant univoque à l'échelle du monde qui est généré dans la banque de données des usagers du réseau domestique (UDM/UDR). Le *SUPI* n'est utilisé que dans le système 3GPP. L'*IMSI* peut par exemple être utilisé comme *SUPI*. L'équipement terminal ne communique son *SUPI* au réseau que sous forme chiffrée (par ex. lors de la connexion au réseau). Pour permettre l'itinérance, le *SUPI* contient l'adresse du réseau domestique (par ex. le *Mobile Country Code MCC* et le *Mobile Network Code MNC*). Le système 5G enregistre dans la banque de données des usagers la relation entre le GPSI et le SUPI correspondant, cette relation n'étant toutefois pas forcément dans un rapport 1:1 (l'actuel GPSI ou SUPI correspondant peuvent être obtenus par une demande de renseignements selon les art. 36 ou 41).

Le *ch. 11* est corrigé suite à une erreur dans la traduction de la norme ETSI rédigée en anglais: l'indication visée est un type de relation commerciale (*subscription type*) et non un type de service. Sur le fond, rien ne change.

Une précision est apportée au *ch. 12*. Comme expliqué ci-dessus pour le ch. 2, il peut y avoir d'autres ressources d'adressage ou identifiants de service qui appartiennent au service d'accès au réseau sur lequel porte la requête (par ex. abonnement de téléphonie mobile). Ces ressources d'adressage ou identifiants de service sont à communiquer dans ce champ sous forme d'une liste ou d'une plage (*range*, de... à…). Doit désormais également être indiquée la période de validité de la ressource d'adressage ou de l'identifiant.

Pour que l'autorité qui demande les renseignements puisse plus facilement interpréter les résultats livrés, et pour mieux comprendre de quel service il s'agit, un champ est ajouté, au *ch. 13*, pour indiquer la désignation du service d'accès au réseau sur lequel porte la demande. Il peut s'agir par exemple de la dénomination de vente de l'abonnement. Cette précision a été demandée par les autorités de poursuite pénale au vu de la grande diversité des produits proposés.

Les deux premières phrases de l'*al. 2* sont reprises inchangées de l'actuel al. 2. À la *let. g*, il est précisé que l'UID est un identifiant national et que la demande peut désormais aussi être faite avec l'identifiant international qu'est le Legal Entity Identifier (LEI, voir le commentaire de l'art. 20*b*, al. 1, let. b). À la *let. i*, l'*identifiant DSL* est remplacé par le *GPSI* (voir commentaire de l'al. 1, let. d, ch. 2). À la *let. j*, un nouvel identifiant du système 5G, le SUPI, est ajouté (voir commentaire de l'al. 1, let. d, ch. 10). À la *let. k*, le *numéro SIM* disparaît au profit du nouveau terme technique universel qu'est l'*ICCID* (voir commentaire de l'al. 1, let. d, ch. 9).

L'*al. 3, première phrase*, correspond à la troisième phrase de l'actuel al. 2, seule une correction y est apportée: le critère selon la let. e (numéro de la pièce d'identité) n'est pas repris dans cette disposition. Ce critère étant univoque, il n'y a pas lieu d'utiliser en même temps un deuxième critère de recherche. La *deuxième phrase* correspond à la quatrième phrase de l'actuel al. 2.

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

Dans la phrase introductive de l'*al. 1*, il est précisé que les indications à livrer doivent être valables pendant la période sur laquelle porte la demande. Cette période peut s'étendre du moment présent vers le passé, mais pas vers l'avenir. Les données visées par ce type de renseignements sont des données d'utilisation, que les POC concernées ne sont tenues de conserver que pour les six derniers mois. Pour les demandes portant sur des périodes plus éloignées dans le passé, les POC ne doivent livrer que les données dont elles pourraient encore disposer.

Pour des motifs rédactionnels, la deuxième phrase de l'*al. 1* est déplacée dans un nouvel *al. 2*.

L'*al. 1, let. a*, ne change pas.

Aux *let. b et c*, les identifiants sont désormais au pluriel, en raison des offres multi-SIM et multi-appareils (voir art. 35, al. 1, let. d, ch. 2). La précision est par ailleurs donnée que ces identifiants correspondent au service d'accès au réseau sur lequel porte la demande.

À la *let. c*, de nouveaux identifiants du système 5G sont ajoutés: le SUPI et le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10 pour le «SUPI» et de l'art. 35, al. 1, let. d, ch. 2 pour le «GPSI»).

À la *let. d*, un nouvel identifiant du système 5G est ajouté: le PEI ou *Permanent Equipment Identifier*, qui sert à identifier de manière univoque à l'échelle du monde les équipements terminaux dans les réseaux téléphoniques mobiles 5G. Le *PEI* se compose soit d'un *IMEI*, soit d'un *IMEISV*. La disposition précise encore que ces indications ne sont disponibles que pour les six derniers mois, puisqu'il s'agit de données d'utilisation.

À la *let. e*, le *numéro SIM* disparaît au profit du nouveau terme technique universel qu'est l'*ICCID* (voir commentaire de l'art. 35, al. 1, let. d, ch. 9).

La *let. f* précise désormais que les codes PUK (PUK et PUK2) doivent toujours être communiqués avec leur période de validité (voir dans le même sens l'art. 35, al. 1, let. b, ch. 2). Cette indication permet de faire une distinction lorsque plusieurs codes PUK sont livrés simultanément. Les codes PUK à livrer sont ceux qui correspondent à la carte SIM sur laquelle porte la demande.

Pour des motifs rédactionnels, la deuxième phrase de l'actuel al. 1 est déplacée dans un nouvel *al. 2*. Son contenu reste inchangé. L'actuel al. 2 devient le nouvel *al. 3*.

À l'*al. 3, let. a*, l'identifiant DSL, moins typique, est remplacé par le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2).

Dans les *let. b* et *c* sont ajoutés les nouveaux identifiants du système 5G: le SUPI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10) et le PEI (voir art. 36, al. 1, let. d).

La *let. d* reste inchangée.

Une nouvelle *let. e* est ajoutée pour organiser plus efficacement notamment les demandes de codes PUK: il faut aujourd'hui deux demandes IR_4_NA et IR_6_NA, mais à l'avenir une seule demande de type IR_6_NA suffira pour obtenir le code PUK.

Une nouvelle *let. f* est ajoutée pour permettre les demandes à partir des codes qui sont usuellement utilisés dans les offres à prépaiement pour recharger du crédit ou pour payer la prestation. Il s'agit de ces codes que l'on peut acheter par exemple dans un kiosque ou à la caisse d'un supermarché, sous forme de carte à gratter ou de ticket de caisse. La saisie du code crédite le montant en question sur le compte à prépaiement. La norme ETSI n'avait jusqu'à présent pas encore de champ de données permettant d'utiliser ce genre de code comme critère pour une demande de renseignements. Comme cette possibilité existait déjà avec l'ancienne LSCPT du 31 octobre 2001, le Service SCPT a présenté une requête de changement à l'ETSI, qui l'a entretemps acceptée et intégrée dans la norme. La disposition de l'art. 36 peut donc être complétée en ce sens.

Art. 37, al. 1, phrase introductive (ne concerne que l'allemand) et let. b

Dans la *phrase introductive* de l'*al. 1*, une adaptation rédactionnelle est faite dans le texte allemand pour répondre aux règles de la formulation non sexiste.

Le caractère univoque de l'identifiant du service (par ex. nom d'utilisateur) à la *let. b* se réfère au fournisseur. L'autorité qui souhaite obtenir des renseignements peut utiliser cet identifiant comme critère de recherche pour de nouvelles demandes. L'identifiant du service devra dans la mesure du possible être pourvu d'une désignation appropriée si sa signification ne se comprend pas immédiatement.

Dans les exemples cités à la *let. b*, l'identifiant DSL est remplacé par le GPSI, un identifiant du système 5G (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2).

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

La pratique a montré que les demandes d'identification d'usagers sur la base des adresses IP et d'autres critères n'aboutissent pas toujours à des résultats clairs dans les cas où il y a une traduction d'adresse réseau de classe transporteur, en anglais *carrier-grade NAT* (cgNAT). Cette absence de résultats clairs tient au fait qu'avec une cgNAT, le fournisseur d'accès (le *carrier*) fait de la traduction d'adresses de réseau (NAT) pour tous ses clients ou pour une grande partie de ceux-ci. Plusieurs clients peuvent dès lors apparaître sur internet simultanément avec la même adresse IP publique, voire aussi avec le même numéro de port (critères obligatoires pour une demande). Comme pour les autres types de recherches, il doit donc être possible d'admettre plusieurs résultats. La possibilité d'obtenir des résultats ambigus lorsque des procédures de traduction d'adresses de réseau entrent en jeu a déjà été signalée dans le rapport explicatif de l'actuelle OSCPT (p. 42).

Pour tenir compte de cette réalité, des adaptations rédactionnelles sont faites à l'*al. 1* et dans ses *let. a* et *b*, où les termes usagers, identifiants des usagers, identifiants du

service et services d'accès au réseau sont désormais au pluriel. Par ailleurs, une adaptation rédactionnelle est faite dans le texte allemand de l'*al. 1* pour répondre aux règles de la formulation non sexiste.

À la *let. b*, dans les exemples cités, l'identifiant DSL, moins typique, est remplacé par le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2).

Avec les modifications dans l'*al. 2, let. f*, le moment (désormais appelé moment déterminant) est redéfini. Selon l'arrêt du Tribunal administratif fédéral A-6807/2019, un FST doit conserver les données secondaires relatives à l'attribution et à la traduction d'adresses IP et de numéros de ports (cf. art. 21, al. 6, let. b, OSCPT) d'une manière qui lui permettent d'identifier les utilisateurs à chacun des moments exigés par l'autorité dans sa demande et de livrer les renseignements visés à l'art. 38, al. 1, OSCPT, pour autant que ladite autorité lui fournisse les indications spécifiées à l'art. 38, al. 2, OSCPT pour les moments en question (ch. 4.5.1, p. 24). Avec cet ajout, le texte dit clairement que l'autorité qui demande les renseignements peut choisir n'importe quel moment, au début ou à la fin d'une procédure donnée de traduction, ou pendant celle-ci. Le moment déterminant indiqué dans la demande ne doit donc en particulier pas nécessairement se situer près du début du contexte de traduction d'adresses de réseau (observé) sur lequel porte la demande.

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

Les modifications dans cet article sont analogues à celles qui sont proposées pour l'art. 38 (voir ci-dessus). Les deux demandes possibles sont par ailleurs mieux décrites:

a) lorsque l'opération de traduction s'est faite avec la ressource d'adressage source (*originating IP address*),

b) lorsque l'opération de traduction s'est faite avec la ressource d'adressage de destination (*destination IP address*).

La ressource d'adressage source doit toujours être indiquée dans la demande.

Art. 40, al. 1, let. b, c et d, phrase introductive, et ch. 2, 6, 7 et 10 à 13, al. 2, phrase introductive, et let. g, j et k, et al. 3

À l'*al. 1, let. b* et *c*, la précision de la période de validité est ajoutée concernant les autres coordonnées (voir le commentaire pour la même modification à l'art. 35, al. 1, let. b et c).

À la *let. d, ch. 2*, il est désormais précisé que c'est l'identifiant principal du service qui doit être livré, par exemple le numéro de téléphone principal. Cette précision est nécessaire parce que des opérateurs proposent des services de téléphonie mobile avec des cartes SIM supplémentaires (multi-appareils, multi-SIM), qui ont donc plus d'un identifiant (par ex. MSISDN). Les autres identifiants à livrer sont indiqués au ch. 7.

Selon la *let. d, ch. 6*, la période de validité de chaque statut de service peut désormais être livrée, comme c'est déjà le cas pour le type de renseignements IR_4_NA (version

actuelle de l'art. 35, al. 1, let. d, ch. 6). Comme la norme ETSI définit différents formats de données pour les services d'accès au réseau (NA) et les services multimédia (TEL), il a d'abord fallu présenter une requête de changement à l'ETSI pour que le paramètre de la période de validité, existant déjà pour les services d'accès au réseau, soit également défini pour les services multimédia (TEL). La norme ETSI ayant entretemps été adaptée, il est maintenant possible de proposer cette modification.

Au *ch. 7*, il est précisé que les ressources d'adressage ou identifiants recherchés peuvent aussi être ceux qui «correspondent» au service en question (*associated*), par exemple dans le cas de services de téléphonie mobile avec des cartes SIM supplémentaires. En font également partie les ressources d'adressage et les identifiants ajoutés après l'enregistrement de l'usager, lorsqu'ils font partie des données relatives aux clients (*subscriber data*). Pour les ressources d'adressage et les identifiants associés de manière temporaire en fonction de l'utilisation (données d'utilisation), ce n'est pas cette recherche qui est prévue mais la nouvelle décrite à l'art. 48*b*. Doit désormais également être indiquée la période de validité de la ressource d'adressage ou de l'identifiant.

Au *ch. 10*, le nouvel identifiant du système 5G, le SUPI, est ajouté (voir commentaire de l'al. 35, al. 1, let. d, ch. 10). La disposition précise encore qu'il s'agit de l'IMSI ou du SUPI «correspondant», afin d'exprimer qu'il peut y en avoir plusieurs (par ex. dans le cas d'un service de téléphonie mobile avec plusieurs cartes SIM).

Au *ch. 11*, le *numéro SIM* disparaît au profit du nouveau terme technique universel qu'est l'*ICCID* (voir commentaire de l'al. 35, al. 1, let. d, ch. 9). La disposition précise encore qu'il s'agit des ICCID «correspondants», afin d'exprimer qu'il peut y en avoir plusieurs (par ex. dans le cas d'un service de téléphonie mobile avec plusieurs cartes SIM).

Au *ch. 12*, il n'était jusqu'à présent pas possible de fournir le type de relation commerciale, comme à l'art. 35, al. 1, ch. 11 (en anglais: *subscription type*), car la norme ETSI en question ne contenait pas encore ce paramètre au moment des travaux sur l'OSCPT du 15 novembre 2007. La norme a entretemps été adaptée, de sorte que la transmission du «type de relation commerciale» est maintenant possible.

Au *ch. 13*, un champ est ajouté pour la transmission de la «désignation du service» (voir le commentaire de l'art. 35, al. 1, let. d, ch. 13).

L'*al. 2, let. g*, prévoit désormais que la demande peut aussi être faite avec le Legal Entity Identifier (LEI, voir le commentaire de l'art. 20*b*, al. 1, let. b).

À la *let. j*, le nouvel identifiant du système 5G, le SUPI, est ajouté (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10).

À la *let. k*, le *numéro SIM* disparaît au profit du nouveau terme technique universel qu'est l'*ICCID* (voir le commentaire de l'art. 35, al. 1, let. d, ch. 9).

L'*al. 3* correspond sur le fond aux troisième et quatrième phrases de l'actuel al. 2, qui forment désormais un alinéa séparé pour des motifs rédactionnels.

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

L'*al. 1* précise désormais que les demandes se réfèrent à une période donnée. Les réponses ne valent par conséquent que pour la période sur laquelle porte la demande. On rappellera que seules les POC qui ont des obligations en matière de surveillance doivent conserver les données secondaires des six derniers mois (obligation de conserver les données secondaires). Les indications plus anciennes ne peuvent être livrées que si les POC en disposent encore. Les POC qui n'ont pas d'obligations en matière de surveillance livrent les indications dont elles disposent, puisqu'elles ne sont pas tenues de conserver les données secondaires.

L'*al. 1, let. a*, ne change pas.

À la *let. b*, le mot «correspondants» est ajouté pour exprimer que les ressources d'adressage et les identifiants peuvent aussi être associés au service sur lequel porte la demande, par exemple dans le cas de services de télécommunication mobile proposant plusieurs cartes SIM (offre multi-appareils ou multi-SIM), qui ont plus d'un identifiant (par ex. MSISDN).

À la *let. c*, de nouveaux identifiants du système 5G sont ajoutés: le SUPI et le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10 pour le «SUPI» et de l'art. 35, al. 1, let. d, ch. 2 pour le «GPSI»). Le mot «correspondants» est par ailleurs ajouté dans chaque cas, afin d'exprimer qu'il peut y avoir plusieurs IMSI ou SUPI et que les MSISDN et GPSI correspondants doivent être livrés.

À la *let. d*, un nouvel identifiant du système 5G est ajouté: le *PEI* (voir art. 36, al. 1, let. d). La disposition précise encore que ces indications ne sont disponibles que pour les six derniers mois, puisqu'il s'agit de données d'utilisation.

À la *let. e*, le *numéro SIM* disparaît au profit du nouveau terme technique universel qu'est l'*ICCID* (voir commentaire de l'al. 35, al. 1, let. d, ch. 9). La disposition précise encore qu'il s'agit des ICCID «correspondants», afin d'exprimer qu'il peut y en avoir plusieurs (par ex. dans le cas d'un service de téléphonie mobile avec plusieurs cartes SIM).

La *let. f* précise désormais que le PUK et le PUK2 doivent toujours être communiqués avec leur période de validité (voir le commentaire sur une modification analogue à l'art. 36, al. 1, let. f).

L'*al. 2* correspond à la deuxième phrase de l'actuel 1, séparée pour des motifs rédactionnels.

À l'*al. 3, let. a*, la liste des exemples est raccourcie. Le numéro de téléphone est supprimé et le *TEL URI* est remplacé par le *GPSI* (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2), l'objectif étant de ne garder qu'un petit nombre d'exemples actuels. Cela ne signifie pas, pour autant, que le numéro de téléphone et le *TEL URI* ne peuvent plus être utilisés comme critères de demande.

Aux *let. b et c*, de nouveaux identifiants du système 5G sont ajoutés: le SUPI et le PEI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10, et de l'art. 36, al. 1, let. d).

Les *let. d* et *e* restent inchangées.

Aux *let. f et g*, le numéro SIM (ICCID) et le code pour recharger du crédit ou payer la prestation sont ajoutés comme critères de demande (voir le commentaire d'une modification analogue à l'art. 36, al. 2, let. e et f).

Art. 42, al. 1, let. c, phrase introductive et ch. 6, let. d, al. 2, phrase introductive, let. g et j, et al. 3

Comme pour les autres types de renseignements sur des services de télécommunication (art. 35, 40 et 43), un champ est ajouté, ici à l'*al. 1, let. c, ch. 6*, pour transmettre la désignation du service (voir le commentaire de l'art. 35, al. 1, let. d, ch. 13). À la *let. d*, un nouvel identifiant du système 5G, le GPSI, est ajouté (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2).

À l'*al. 2, let. g*, il est précisé que l'UID est un identifiant national et que la demande peut désormais aussi être faite avec l'identifiant international qu'est le Legal Entity Identifier (LEI, voir le commentaire de l'art. 20*b*, al. 1, let. b). À la *let. j*, les identifiants liés au service sur lequel porte la demande sont ajoutés comme critère de recherche. L'exemple donné est celui d'une ressource d'adressage de rétablissement tel que l'adresse de courrier électronique ou le numéro de téléphone.

L'*al. 3* correspond à la troisième phrase de l'actuel al. 2.

Art. 42a **Type de renseignements IR_51_EMAIL_LAST: renseignements sur des services de courrier électronique**

Ce type de renseignements est créé pour l'obtention des indications sur la *dernière activité d'un service de courrier électronique pertinente en termes d'accès* (pour la définition, voir l'annexe de l'OSCPT, n° 39). L'indication peut servir, d'une part, à identifier un utilisateur du service. Le moment du dernier accès à un service de courrier électronique est déterminant, d'autre part, pour la conclusion du processus de communication. Ce processus est en effet considéré comme terminé pour tous les messages déjà arrivés et sauvegardés dans la boîte de réception. Le ministère public peut obtenir ces messages par une ordonnance de production de pièces fondée sur l'art. 265 CPP. En revanche, les messages arrivés après le dernier accès ne peuvent être obtenus par l'autorité que dans le cadre d'une surveillance en temps réel selon l'art. 58 (RT_26_EMAIL_IRI) ou l'art. 59 (RT_27_EMAIL_CC_IRI).

Il n'est pas possible de préciser un moment déterminant dans la demande. Pour ce type de renseignements, les POC ne doivent indiquer que la dernière activité pertinente en termes d'accès, en remontant au plus à six mois. Ils ne sont pas tenus de fournir des informations sur des activités antérieures à cette dernière activité. Ce type de renseignements ne permet pas d'obtenir rétroactivement les activités d'accès au service de courrier électronique (historique). L'historique et les données secondaires historiques ne peuvent être obtenues que par une surveillance rétroactive de type HD_30_EMAIL (art. 62, voir le commentaire de cet article).

L'*al. 1* règle les indications à livrer. Selon la *let. a*, un identifiant univoque dans le domaine du fournisseur doit être communiqué (par ex. numéro de client), pour autant que le fournisseur en ait attribué un à l'usager. L'«identifiant du service» visé à la *let. b* désigne de manière univoque le service de courrier électronique (boîte de réception)

auquel se rapporte la réponse. À la *let c* sont énumérées les indications à livrer sur l'origine de la connexion lors de la dernière activité pertinente en termes d'accès.

L'*al. 2* précise ce que la demande de renseignements doit contenir. L'adresse électronique et le nom d'utilisateur sont mentionnés à titre d'exemples de critères. Le critère pour la demande doit être suffisamment précis pour que le fournisseur puisse déterminer le service de courrier électronique (boîte de réception) visé.

Art. 43, al. 1, let. c, phrase introductive, et ch. 6, al. 2, phrase introductive, let. g, i et j, et al. 3

À l'*al. 1* la référence aux services d'informatique en nuage est supprimée, car ce terme est trop imprécis. Toutes sortes de prestations peuvent être proposées sous forme de services d'informatique en nuage, dont certaines qui ne sont ni des services de télécommunication, ni des services de communication dérivés (par ex. calculs informatiques, services de traduction). La référence aux services de serveur mandataire est supprimée pour la même raison.

Comme pour les autres types de renseignements sur des services de communication (art. 35, 40 et 42), un champ est ajouté, ici à l'*al. 1, let. c, ch. 6*, pour la transmission de la désignation du service (voir le commentaire de l'art. 35, al. 1, let. d, ch. 13).

L'*al. 2, let. g*, prévoit désormais que la demande peut aussi être faite avec le Legal Entity Identifier (LEI, voir le commentaire de l'art. 20*b*, al. 1, let. b).

À la *let. i*, il est précisé qu'il s'agit d'une ressource d'adressage ou d'un identifiant du service sur lequel porte la demande (service de télécommunication ou service de communication dérivé). La demande de renseignements peut concerner par exemple un *push-token* particulier, qui doit être indiqué ici. Le push-token est un identifiant univoque spécifique à une application et à un appareil qui est utilisé pour les notifications de l'application en question. Concrètement, le push-token permet d'assurer que la notification du service concerné soit envoyée vers une application déterminée, sur un équipement spécifique (par ex. jeton d'appareil du service de notifications push d'Apple, identifiant d'enregistrement de Google Cloud Messaging, chaîne URI du service de notifications push de Windows).

À la *let. j*, les identifiants liés au service sur lequel porte la demande sont ajoutés comme critère de recherche. L'exemple donné est celui d'une ressource d'adressage de rétablissement tel que l'adresse de courrier électronique ou le numéro de téléphone.

L'*al. 3* correspond aux troisième et quatrième phrases de l'actuel al. 2.

Art. 43a **Type de renseignements IR_52_COM_LAST: renseignements sur d'autres services de télécommunication ou services de communication dérivés**

Ce type de renseignements est créé pour l'obtention des indications sur la dernière *activité pertinente en termes d'accès concernant un autre service de télécommunication ou service de communication dérivé* (pour la définition, voir l'annexe de l'OSCPT, n° 41). L'indication peut servir, d'une part, à identifier un utilisateur du service. Le moment du dernier accès au service en question est déterminant, d'autre part, pour la

conclusion du processus de communication. Comme pour le courrier électronique, la procédure de communication est considérée comme terminée pour tous les messages déjà reçus et sauvegardés avant le moment du dernier accès au service.

Le ministère public peut obtenir ces messages sauvegardés dans les services concernés par une ordonnance de production de pièces fondée sur l'art. 265 CPP.

Il n'est pas possible de préciser un moment déterminant dans la demande. Pour ce type de renseignements, les POC ne doivent indiquer que la dernière activité pertinente en termes d'accès, en remontant au plus à six mois. Ils ne sont pas tenus de fournir des informations sur des activités antérieures à cette dernière activité. Ce type de renseignements ne permet pas d'obtenir rétroactivement les activités d'accès au service (historique).

L'*al. 1* règle les indications à livrer. Selon la *let. a*, un identifiant univoque dans le domaine du fournisseur doit être communiqué (par ex. numéro de client), pour autant que le fournisseur en ait attribué un à l'usager. L'«identifiant du service» visé à la *let. b* désigne de manière univoque, dans le domaine du fournisseur, le service de télécommunication ou le service de communication dérivé auquel se rapporte la réponse. À la *let c* sont énumérées les indications à livrer sur l'origine de la connexion lors de la dernière activité pertinente en termes d'accès.

L'*al. 2* précise ce que la demande de renseignements doit contenir. Sont cités à titre d'exemples l'adresse de l'usager, le pseudonyme ou le push-token (voir le commentaire de l'art. 43, al. 2, let. i). Le critère pour la demande doit être suffisamment précis pour que le fournisseur puisse déterminer le service de télécommunication ou le service de communication dérivé visé.

Art. 44, al. 1, let. c et f, et al. 3, let. c et d (ne concerne que l'allemand)

Les modifications dans cet article ne concernent que l'allemand (adaptation aux règles du langage non sexiste). Sur le fond, rien ne change.

Art. 45 **Type de renseignements IR_18_ID: preuve de l'identité**

À l'*al. 1*, le terme de «document», que l'on trouve à l'art. 20*a*, remplace celui de «pièce d'identité». Une adaptation rédactionnelle est faite dans le texte allemand pour répondre aux règles de la formulation non sexiste.

À l'*al. 2*, un nouvel identifiant du système 5G, le SUPI, est ajouté (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10). Pour le reste, le contenu de l'alinéa est inchangé. L'abréviation *ICCID* est expliquée dans l'annexe.

Art. 46, al. 1 (ne concerne que l'allemand)

Cet alinéa est adapté pour répondre aux règles de la formulation non sexiste.

Art. 47 **Type de renseignements IR_20_CONTRACT: copie du contrat**

L'*al. 1* est adapté pour répondre aux règles de la formulation non sexiste.

À l'*al. 2*, un nouvel identifiant du système 5G, le SUPI, est ajouté (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10). Pour le reste, le contenu de l'alinéa est inchangé. L'abréviation *ICCID* est expliquée dans l'annexe.

Art. 48 Type de renseignements IR_21_TECH: données techniques

L'*al. 1* précise que cette demande de renseignements doit porter sur des éléments réseau présents «à la position indiquée dans la demande».

À l'*al. 2, let. a*, les termes génériques d'identifiant de cellule ou de zone géographique remplacent désormais la liste des différents identifiants cités à titre d'exemple. Le nouveau terme d'identifiant de cellule englobe en effet le CGI (2G et 3G), l'ECGI (4G) et le NCGI[25] (5G). Les trois exemples donnés pour une *Area Identity* (SAI[26], RAI[27] et TAI[28]) sont désormais couverts par le terme générique d'identifiant de zone géographique. Ces adaptations rédactionnelles ne changent donc rien concrètement: les CGI, ECGI, SAI, RAI et TAI devront toujours être livrés lorsqu'ils existent techniquement.

La pratique a montré que l'identification d'un réseau WLAN n'était souvent possible qu'au niveau de la zone d'accès sans fil (*hotspot*) et non au niveau du point d'accès. Une autre désignation appropriée (par ex. nom de la zone d'accès sans fil comme alternative au BSSID) est donc ajoutée à titre d'alternative aux éléments réseaux, bien qu'il ne s'agisse pas d'un identifiant univoque (voir aussi art. 48, al. 3, let. b, art. 54, al. 3, let. a, art. 56, al. 2, let. e, ch. 9, art. 60, let. h, art. 61, let. i, ch. 4, art. 64, al. 2, et art. 65, al. 3). Le fournisseur peut choisir le nom de sa zone d'accès librement. Ce nom n'est donc souvent pas univoque et ne permet pas de déduire qui en est l'opérateur. Les fournisseurs de zones d'accès sans fil publiques doivent donc mettre à la disposition des autorités une possibilité d'identification adéquate, par exemple via un site web générique (URL) auquel on peut accéder lorsqu'on est connecté à cette zone d'accès sans fil et obtenir ainsi des informations relatives au fournisseur. Si le nom de la zone d'accès sans fil n'est pas suffisamment clair, c'est-à-dire qu'il n'identifie pas la zone sur place sans risque de confusion, d'autres désignations suffisamment précises peuvent être utilisées, par exemple une brève description du lieu. Cette modification ne signifie pas pour autant que le BSSID ne doit plus être livré: s'il est connu, il doit être livré. Les *let. b, c et d* restent quasiment inchangées.

25 **NCGI** (New Radio Cell Global Identity): identifiant statique d'une cellule dans les réseaux mobiles de cinquième génération (5G), selon la spécification technique 3GPP TS 23.003, ch. 19.6A. Le NCGI est une chaîne qui reprend l'identifiant PLMN (MCC + MNC) et le *NR Cell Identity* (NCI); il est unique au niveau mondial.

26 **SAI** (Service Area Identity): identité de zone de service, c'est-à-dire l'identifiant statique associé à une zone de service (service area) qui est utilisé pour la gestion de la mobilité dans les réseaux mobiles (voir 3GPP TS 23.003, ch. 12.5).

27 **RAI** (Routing Area Identity): identité de zone de routage, c'est-à-dire l'identifiant statique associé à une zone de routage (routing area), qui est utilisé, dans les réseaux mobiles, pour la gestion de la mobilité dans le domaine de la transmission de données par paquets (voir 3GPP TS 23.003, ch. 4.2).

28 **TAI** (Tracking Area Identity): identité de zone de suivi, c'est-à-dire l'identifiant statique associé à une zone de suivi (tracking area) qui est utilisé, dans les réseaux mobiles de quatrième génération, pour la gestion de la mobilité (voir 3GPP TS 23.003, ch. 19.4.2.3).

Une *let. e* est ajoutée car dans les réseaux 5G, les indications d'emplacement des éléments réseau (par. ex. les cellules de radiocommunication mobile) peuvent être horodatées.

À l'*al. 3, let. a*, il est désormais précisé que la «position» est celle qui est «indiquée dans la demande», signifiant ainsi que la demande peut indiquer des coordonnées et concerne dans ce cas tous les éléments réseau de la POC se trouvant à l'emplacement désigné par ces coordonnées. Des demandes ciblées visant un élément réseau particulier se trouvant à l'emplacement désigné sont aussi possibles, en se fondant sur la *let. b*. Il y est ajouté qu'une demande portant sur un élément réseau déterminé peut aussi indiquer, en lieu et place d'un identifiant standardisé, une autre désignation appropriée (par ex. le nom de la zone d'accès sans fil). Par ailleurs, comme à l'al. 2, let. a, les termes génériques d'identifiant de cellule et d'identifiant de zone géographique sont utilisés (voir plus haut).

Art. 48a Type de renseignements IR_53_ASSOC_PERM: renseignements sur les identifiants attribués pour une longue durée

Lors de la fourniture de services de télécommunication fondés sur l'architecture IP Multimedia Subsystems (IMS), il est possible d'utiliser des identifiants attribués pour une longue durée, en lieu et place des identifiants de service et d'équipement, qui sont permanents. C'est le motif de la création de ce nouveau type de renseignements, qui permet d'obtenir les identifiants attribués pour une longue période à un identifiant (IMPI privé pour IMPU public et vice-versa). Comme il s'agit d'indications servant à l'identification selon l'art. 22 LSCPT, les FST et les FSCD ayant des obligations étendues selon les art. 22 ou 52 doivent conserver ces données pendant toute la durée de la relation commerciale ainsi que six mois après la fin de celle-ci, et être en mesure de les livrer (art. 21, al. 1).

Art. 48b Type de renseignements IR_54_ASSOC_TEMP: renseignements immédiats sur les identifiants attribués pour une courte durée

Lors de la fourniture de services de téléphonie mobile 5G, il est possible d'utiliser des identifiants attribués pour une courte durée (temporaires), en lieu et place des identifiants de service et d'équipement, qui sont permanents. Ce nouveau type de renseignements est créé pour obtenir en temps réel les identifiants permanents associés à un identifiant temporaire.

Les détails sont réglés dans l'annexe 1 de l'OME-SCPT. Exemple: le SUPI pour le SUCI et vice-versa.

Les principaux cas d'utilisation sont les suivants:

Pour la 5G: une autorité saisit grâce à un dispositif technique (par ex. une fausse station de base) un identifiant temporaire (par ex. 5G-S-TMSI/5G-GUTI ou un SUCI chiffré). Elle fait une demande de ce nouveau type pour obtenir immédiatement l'identifiant permanent correspondant, c'est-à-dire un SUPI.

Le délai de réponse à ce type de demande doit être très court (de l'ordre de quelques secondes), car les identifiants temporaires changent souvent (au moins à chaque requête de service ou occasion de radiomessagerie voire plus fréquemment encore). Ce

renseignement doit donc être demandé et livré de manière automatisée, via une nouvelle interface de type LI_HIQR (*Lawful Interception Handover Interface Query Response*). La demande ne peut contenir qu'un seul identifiant (al. 2, let. a). Il n'est pas possible d'indiquer un moment déterminant puisqu'il s'agit d'une demande en temps réel. C'est ainsi le moment où la demande est faite qui est pris en compte, les demandes dans le passé ne sont pas possibles.

L'emplacement doit être indiqué (al. 2, let. b) car l'identifiant temporaire n'est univoque que localement. Le même identifiant temporaire peut être attribué à un autre identifiant permanent au même moment mais à un autre endroit.

Exemples de demandes: SUCI, 5G-S-TMSI ou 5G-GUTI.

Art. 48c Type de renseignements IR_55_TEL_ADJ_NET: détermination des réseaux voisins de services de téléphonie et multimédia

Ce nouveau type de renseignements est créé pour résoudre des problèmes spécifiques qui se posent pour l'identification d'auteurs lorsque l'appelant ou l'expéditeur d'un message utilise un numéro usurpé (*spoofing*) ou inconnu. Cela peut être utile, par exemple, en cas d'alerte anonyme à la bombe, pour pouvoir suivre la trace de l'appel ou du message anonyme.

Les données secondaires historiques (HD) des connexions et tentatives de connexion conservées aux fins de permettre la surveillance rétroactive contiennent les ressources d'adressage des participants à la communication (qui, avec qui). Mais lorsque le numéro d'origine de la communication est usurpé ou inconnu, les autorités ont besoin d'un moyen pour retracer l'appel ou la communication.

Le fournisseur doit livrer les indications sur le réseau voisin «de» et sur le réseau voisin «vers», lorsqu'ils ont participé à la communication ou tentative d'établissement de la communication. Il ne doit cependant pas livrer d'indication sur des réseaux plus éloignés dans la chaîne de communication. Exemple: un appel est passé depuis le réseau du fournisseur A vers le réseau du fournisseur C en transitant par le réseau du fournisseur B. Si c'est le fournisseur B qui reçoit la demande concernant cet appel, il doit indiquer les fournisseurs A («de») et C («vers»). Si la demande est adressée au fournisseur A, il indiquera uniquement le réseau B («vers»), car il n'y a pas de réseau «de». Si la demande est adressée au fournisseur C, il indiquera uniquement le réseau B («de»), car il n'y a pas de réseau «vers».

La création de ce type de renseignements s'accompagne d'une obligation de conserver les données secondaires nécessaires pendant six mois (voir également art. 21, al. 6, let. c, et art. 61, let. j) pour les FST ayant des obligations complètes (c'est-à-dire que le Service SCPT n'a pas qualifiés de FST ayant des obligations restreintes en matière de fourniture de renseignements) et les FSCD ayant des obligations étendues en matière de surveillance (art. 52). Chaque fournisseur ne peut contrôler que ses propres interfaces avec le réseau. Pour obtenir des données fiables, seules sont demandées les indications concernant les réseaux immédiatement voisins de la communication ou tentative d'établissement de la communication. Pour retracer toute la communication, l'autorité peut interroger successivement les différents fournisseurs par lesquels cette communication a transité, en amont ou en aval.

Ce nouveau type de renseignements crée une procédure standardisée pour retracer en amont ou en aval les communications ou tentatives d'établissement de communications. Les émoluments et les indemnités sont réglés dans l'annexe de l'OEI-SCPT. Les délais de traitement sont fixés à l'art. 14 de l'OME-SCPT.

Art. 50, al. 5 à 10

L'*al. 5* reste matériellement inchangé.

Alinéa 6: Pour les services de communication mobile avec des cartes SIM supplémentaires (par ex. offres multi-appareils ou multi-SIM pour des smartphones, tablettes ou montres connectées), tous les équipement terminaux, numéros ou cartes SIM associés à l'identifiant de la cible principale doivent être surveillés, par exemple tous les numéros annexes d'un numéro principal. Ce principe vaut pour tous les types de surveillances (en temps réel, rétroactive, détermination de l'emplacement, recherche en cas d'urgence, recherche de personnes condamnées). Sont exclus les identifiants de cibles annexes (par ex. des numéros techniques) qui n'appartiennent qu'à un équipement terminal donné ou à une carte SIM donnée. Aucun émolument supplémentaire n'est dû et aucune indemnité supplémentaire n'est versée pour les équipements terminaux, numéros ou cartes SIM supplémentaires. Si nécessaire, le fournisseur peut exiger des LIID (*Lawful Interception Identifier*, c'est-à-dire des identifiants attribués spécifiquement pour la surveillance) supplémentaires auprès du Service SCPT pour mettre en place les surveillances correspondantes. Si l'autorité qui ordonne la mesure ne souhaite pas la surveillance de tous les équipements terminaux, numéros et cartes SIM rattachés à l'identifiant de la cible principale, elle doit le dire explicitement dans son ordre.

Lorsqu'un nouvel équipement terminal, une nouvelle SIM ou un nouveau numéro est ajouté pour un service concerné par une surveillance en temps réel ou une détermination de position déjà active, le nouveau terminal, la nouvelle SIM ou le nouveau numéro doivent également être surveillés. Aucun émolument supplémentaire n'est dû et aucune indemnité supplémentaire n'est versée. Si nécessaire, le fournisseur peut exiger à cette fin un LIID supplémentaire auprès du Service SCPT.

L'*al. 7* précise les obligations des FST concernant les chiffrements opérés par eux ou pour eux (art. 26, al. 2, let. c, LSCPT). On entend par «chiffrements opérés pour lui» des chiffrements créés à l'aide de la clé public du fournisseur. Même si le fournisseur n'a pas, au sens strict, opéré lui-même ces chiffrements, il est en mesure de les supprimer, puisqu'il dispose de la clé privée correspondante. Cet alinéa précise encore que l'obligation de supprimer les chiffrements s'applique également aux FSCD ayant des obligations étendues en matière de surveillance, selon l'art. 22, ou de fourniture de renseignements, selon l'art. 52. Les FSCD en question ont ainsi les mêmes obligations qu'un FST. L'obligation de supprimer les cryptages prévue à l'art. 26, al. 2, let. c, LSCPT s'applique donc également aux FSCD ayant des obligations étendues en matière de fourniture de renseignements.

Dans le cas de procédures de chiffrement asymétriques (chiffrement avec la clé publique du destinataire et déchiffrement avec la clé privée du destinataire), il n'est en général plus possible pour le fournisseur de supprimer un chiffrement qu'il a lui-même

mis en place. Seuls peuvent déchiffrer les données les destinataires dont la clé publique a été utilisée pour le chiffrement. Une clé publique supplémentaire que le fournisseur pourrait utiliser ne doit toutefois pas révéler l'existence de la surveillance.

Le fournisseur qui recourt à une procédure de chiffrement asymétrique lors de l'envoi des données doit donc le cas échéant saisir et livrer les données de surveillance avant qu'elles ne soient chiffrées.

À l'inverse, le fournisseur qui reçoit des données chiffrées asymétriquement à l'aide de sa clé publique doit saisir les données de surveillance et les déchiffrer avec sa clé privée avant de les transmettre au Service SCPT ou à l'autorité qui les a demandées.

Les «points appropriés» sont tous les points où le fournisseur a le contrôle, en fait ou en droit, de la communication ou de la sauvegarde des données et où il peut intercepter les données de surveillance sans chiffrement ou supprimer le chiffrement.

À l'*al. 8*, les obligations pour la surveillance en temps réel de services de téléphonie mobile sont étendues à la surveillance des banques de données techniques des usagers tels que le HLR[29], le HSS[30] et l'UDM[31], aux fins de la saisie et de la livraison d'importantes données secondaires de la cible. Ces données incluent des informations sur le réseau fournissant le service, sur le changement d'identifiants de service ou d'équipement attribués, sur les événements relatifs à la localisation, sur le changement de l'élément réseau fournissant le service et sur les événements d'identification et d'authentification de la cible.

L'*al. 9* prévoit que dans l'architecture IP Multimedia Subsystem (IMS), la détermination par le réseau (*network provided*) des données de localisation de la cible doit, le cas échéant, être déclenchée lors d'une surveillance en temps réel.

L'*al. 10* prévoit que la POC doit observer toute modification concernant les équipements terminaux et les cartes SIM rattachés à un abonnement ou à un service prépayé surveillé, et doit, de son propre chef, adapter la surveillance en fonction de ces changements. Ce travail supplémentaire de la POC ne donne pas droit à une indemnité. Le Service SCPT ne peut pas non plus exiger d'émolument supplémentaire dans un tel cas. Si nécessaire, le fournisseur peut exiger des LIID supplémentaires pour la mise en place d'autres surveillances nécessaires.

Art. 53, al. 1

Dans cette disposition, il est précisé que même les POC qui ne doivent que tolérer les surveillances doivent permettre l'installation de branchements de test. Les branchements de test sont réglés à l'art. 30. Un branchement de test peut être nécessaire notamment lorsqu'il faut préparer une surveillance qui a été ordonnée, ou pour contrôler

29 **HLR** (Home Location Register): dans les réseaux de téléphonie mobile de deuxième et de troisième génération, banque de données d'un fournisseur dans laquelle sont enregistrées les données caractérisant ses utilisateurs (par ex. IMSI, MSISDN, configuration, profil de service) et le réseau utilisé dans chaque cas pour fournir le service.

30 **HSS** (Home Subscriber Server): dans les réseaux de téléphonie mobile de quatrième génération, mêmes fonctions que le HLR.

31 **UDM** (Unified Data Management): dans les réseaux de téléphonie mobile de cinquième génération, mêmes fonctions que le HLR et le HSS.

la qualité d'une surveillance en cours, même si elle est mise en œuvre techniquement par le Service SCPT.

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

L'*al. 1* reste inchangé.

La 5G permet des accès multiples (*multiple registrations*) et des connexions multiples (*multiple attachments*) dans le même réseau ou dans des réseaux différents fournisseurs de services, ce qui permet également à la cible de la surveillance de changer de réseau ou de technologie[32].

L'*al. 2, let. a* est complété pour que les autorités, lors d'une surveillance en temps réel, soient informées de la technologie qu'une cible utilise et des changements de technologie ou de réseau. Doivent également être transmises, dans le cas de la téléphonie mobile, les informations relatives aux procédures d'établissement de l'accès au réseau et de déconnexion en fonction de la technologie utilisée (GPRS, EPS, 5GS): pour la GPRS en particulier les événements *GPRS Attach*, *GPRS Detach*, *PDP Context Activation* et *PDP Context Deactivation*; pour l'EPS, les événements *E-UTRAN Attach*, *E-UTRAN Detach*, *Bearer Activation* et *Bearer Deactivation*; pour la 5GS, les événements *Registration*, *Deregistration*, *PDU Session Establishment* et *PDU Session Release.*

Les *let. b* et *d* restent inchangées.

Dans les *let. c, e* et *f* sont ajoutés les nouveaux identifiants du système 5G que sont le SUPI, le GPSI et le PEI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2 pour le GPSI et ch. 10 pour le SUPI, et le commentaire de l'art. 36, al. 1, let. d pour le PEI).

À la *let. g*, il est précisé qu'il s'agit d'événements qui modifient les caractéristiques techniques du service d'accès au réseau surveillé ou sa gestion de la mobilité. Sont considérés comme des modifications des caractéristiques techniques notamment la modification du *service support*, par exemple des modifications du *PDP Context*, du *Bearer* ou de la *PDU Session*, et l'actualisation de la position de la cible, par exemple *Location Update* et *Mobility Registration Update*. Font partie de la gestion de la mobilité par exemple *GMM*, *EMM* et *Mobility Registration*.

À la *let. h*, il est désormais précisé, comme à l'art. 56, al. 2, let. e, ch. 9, qu'il s'agit des données de localisation «actuelles». Il est aussi précisé que ces données actuelles de localisation doivent dans la mesure du possible être déterminées par le réseau et signalées comme telles. Les données de localisation déterminées par le réseau sont plus fiables que celles données par l'équipement terminal, qui peuvent être falsifiées. Toutes les données de localisation disponibles doivent cependant être livrées, également celles fournies par l'équipement terminal, qui doivent être signalées comme telles. Les étiquettes «déterminé par le réseau» et «déterminé par l'équipement terminal» aident les autorités à déterminer dans quelle mesure elles peuvent se fier à ces indications de localisation. Les systèmes de téléphonie mobile de quatrième génération (EPS) et de cinquième génération (5GS) ont parfois un timbre horodateur et des

32 Cf. 3GPP TS 33.501, ch. 6.3.2

indications sur l'âge des données de localisation; le cas échéant, ces données doivent aussi être livrées. On entend par l'*âge* des données le temps qui s'est écoulé entre le moment où la position a été déterminée et le moment où cette indication a été transmise.

La nouvelle *let. i* règle la livraison de données secondaires importantes qui peuvent être saisies lors de la surveillance de bases de données techniques d'usagers telles que HLR, HSS et UDM (voir le commentaire de l'art. 50, al. 8). Ces données sont les suivantes:

- informations sur le réseau fournissant actuellement le service et sur le réseau précédent, c'est-à-dire des événements du type «serving system» (*réseau fournissant le service*, par ex. Serving PLMN, VPLMN ID);
- informations sur le changement des identifiants de service et d'équipement attribués (par ex. IMSI, MSISDN, IMEI, SIP-URI, IMPI), c'est-à-dire des événements de type *subscriber record change*;
- informations sur des événements relatifs à la localisation et, le cas échéant, sur leur motif, par exemple événements de type *register location / cancel location / register termination;*
- informations sur le changement de l'élément réseau fournissant le service (par ex. SGSN, MME, MSC, AMF);
- informations sur les événements d'identification et d'authentification de la cible (par ex. réception d'une autorisation d'accès à un réseau WLAN public).

À l'*al. 3*, une modification rédactionnelle est apportée: la formule «le type de technologie de communication mobile utilisé» figure désormais une seule fois, dans la phrase introductive, plutôt que d'être répétée à chaque lettre.

À la *let. a*, les mêmes deux modifications sont apportées qu'à l'art. 48, al. 2, let. a (voir le commentaire s'y rapportant): l'emploi du terme générique d'identifiant de cellule ou d'équipement en lieu et place de l'énumération des exemples des différents identifiants, et la mention d'une «autre désignation appropriée (par ex. nom de la zone d'accès sans fil)» comme alternative au BSSID. Une désignation suffisamment précise de l'accès au réseau WLAN suffit, ce qui signifie que la désignation livrée doit permettre d'identifier l'accès au réseau sur place sans risque de confusion (voir aussi le commentaire de l'art. 48, al. 2, let. a et al. 3, let. b). Le nom de la zone d'accès sans fil doit être transmis dans le paramètre SSID.

Les *let. b* et *c* restent inchangées sur le plan du contenu. Seul le terme «point d'accès au réseau WLAN» est remplacé par «accès au réseau WLAN» à la let. c (voir le commentaire du remplacement d'expressions, al. 1).

Les ajouts aux *let. d* et *e* concernent les indications de localisation dans le cas d'un accès non 3GPP au réseau de téléphonie mobile non digne de confiance, en anglais «untrusted» (*let. d*) ou digne de confiance, en anglais «trusted» (*let. e*). Les qualificatifs «non digne de confiance» et «digne de confiance» distinguent les types d'accès du point de vue de l'opérateur de téléphonie mobile.

Les accès dits «non dignes de confiance» sont ceux auxquels il ne se fie pas. Il s'agit le plus souvent d'accès de tiers, c'est-à-dire exploités par d'autres fournisseurs et pour

lesquels l'opérateur ne connaît que les données de connexion IP (voir aussi les explications dans l'annexe «Termes et abréviations»). Une connexion (VPN) sécurisée (chiffrée) est établie entre l'équipement terminal de la cible et la passerelle (*evolved packet data gateway*) de l'opérateur de téléphonie mobile. L'opérateur communique l'adresse IP source publique, qu'il peut voir, et, le cas échéant, le numéro de port source de l'équipement terminal de la cible.

L'ajout «digne de confiance» signifie que le fournisseur fait confiance à cet accès parce que, le plus souvent, il l'exploite lui-même. Un tel accès est aussi appelé Trusted WLAN Access Network (TWAN). Si l'adresse postale de l'accès est connue en plus de sa désignation (identifiant TWAN), elle doit aussi être livrée.

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

L'*al. 1* est simplifié et réduit à sa première phrase, qui définit les services concernés par le type de surveillance RT_24_TEL_IRI.

Le nouvel *al. 2* reprend la deuxième phrase de l'actuel al. 1 et précise quelles données secondaires doivent être livrées en temps réel. La *let. a* correspond à l'actuel al. 1, let. a. À la *let. b*, un nouvel identifiant du système 5G est ajouté: le SUPI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10). Les *let. c* et *d* correspondent aux actuelles let. c et d de l'al. 1 avec, pour l'allemand, une adaptation rédactionnelle pour respecter les règles de la formulation non sexiste.

Les *ch. 1, 3, 5, 6, 7* et *8* de la *let. e* correspondent aux mêmes chiffres de l'actuel al. 1, let. e. Aux *ch. 2* et *4*, de nouveaux identifiants du système 5G sont ajoutés: le GPSI et le PEI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10, et de l'art. 36, al. 1, let. d). Au *ch. 9*, il est précisé que la disposition ne s'applique qu'à la téléphonie mobile et aux réseaux WLAN. Il est aussi précisé que les données actuelles de localisation doivent dans la mesure du possible être déterminées par le réseau et signalées comme telles (voir le commentaire de l'art. 54, al. 2, let. h). Pour l'EPS et la 5GS, les données de localisation doivent être complétées, si ces données sont disponibles, par le timbre horodateur associé et l'âge des données (voir le commentaire de l'art. 54, al. 2, let. h). Par ailleurs, le terme «point d'accès au réseau WLAN» est remplacé par «accès au réseau WLAN» à la let. c (voir le commentaire du remplacement d'expressions, al. 1).

La *let. f* règle la livraison de données secondaires importantes qui peuvent être saisies lors de la surveillance de bases de données techniques d'usagers telles que HLR, HSS et UDM (voir le commentaire de l'art. 54, al. 2, let. i).

Plutôt que de répéter les indications relatives aux données de localisation, qui sont les mêmes qu'à l'art. 54, al. 3, un renvoi vers cette disposition à l'al. 2, ch. 9 permet de se passer ici d'un al. 3.

Art. 56a Type de surveillance RT_56_POS_IMMED: détermination unique et immédiate de la position par le réseau

La *localisation* et la *position* ont des sens différents dans la présente ordonnance. Jusqu'à présent, seules les données de localisation étaient disponibles (*location informa-*

tion). On entend par *localisation* la cellule ou la zone où se trouve la cible de la surveillance. Il ne s'agit en général que d'une approximation grossière de l'endroit où se trouve effectivement la cible (équipement terminal) et correspond le plus souvent à l'emplacement de l'antenne à laquelle la cible est ou était récemment connectée. Les données de localisation peuvent être très imprécises et dépendent de la portée de l'antenne en question. En milieu rural, l'écart entre l'emplacement de l'antenne et la position effective de la cible peut atteindre trente kilomètres. Le réseau de téléphonie mobile connaît le plus souvent déjà la *localisation*, qui n'a pas besoin d'être déterminée. Il peut cependant arriver que le réseau doive déterminer la localisation, par exemple lors d'une recherche en cas d'urgence de type EP_35_PAGING ou d'une surveillance de type HD_31_PAGING.

Le terme de *position* est en revanche utilisé pour désigner le lieu précis où se trouve la cible (équipement terminal) au moment où cette position est déterminée. La détermination de la position est une nouvelle fonction dans le réseau de téléphonie mobile. La détermination de la position selon la LSCPT (LALS, *Lawful Access to Location Services*) est désormais introduite et est considérée comme une surveillance selon l'art. 269 CPP. Elle ne sera exécutée que sur ordre d'une autorité habilitée à ordonner une surveillance. L'approbation du tribunal des mesures de contrainte est requise. Deux types de surveillances relatifs à la détermination de la position par LALS sont introduits dans l'ordonnance:

1) la détermination unique et immédiate de la position (art. 56*a*),

2) la détermination récurrente et périodique de la position (art. 56*b*).

L'*al. 1* prévoit que l'opérateur de téléphonie mobile doit réaliser une détermination unique et immédiate de la position en utilisant à cet effet une fonction du réseau (LALS). Les positions de tous les équipements terminaux associés à l'identifiant surveillé (target ID) doivent être déterminées.

Les prescriptions techniques de mise en œuvre sont édictées par le DFJP dans l'OME-SCPT et son annexe 1 (*al. 2*). Il n'y a pas encore d'expérience pratique de cette nouvelle détermination unique de la position par LALS. Suivant l'implémentation technique, la détermination de la position peut prendre un certain temps. Les opérateurs de téléphonie mobile doivent cependant transmettre immédiatement et sans délai les positions des équipements terminaux lorsqu'elles sont déterminées.

L'*al. 3* précise les indications à livrer. Les indications prévues aux *let. a et b*, de même qu'à la *let. c, ch. 1 à 3* sont obligatoires. Les indications selon la *let. c, ch. 4* doivent être livrées si elles sont disponibles.

Selon la *let. d*, lorsque la position n'a pas pu être déterminée, l'opérateur indique le motif de l'échec (code d'erreur) et, si possible, l'emplacement de la dernière cellule connue utilisée par l'équipement terminal, c'est-à-dire de la dernière antenne de la cellule qui a fourni le service.

Art. 56*b* Type de surveillance RT_57_POS_PERIOD: détermination récurrente et périodique de la position par le réseau

Les remarques introductives faites pour l'art. 56*a* valent également pour le présent art. 56*b*, consacré au deuxième type de surveillance pour la détermination de la position via LALS: la détermination récurrente et périodique de la position par le réseau.

L'*al. 1* prévoit que l'opérateur de téléphonie mobile réalise une détermination périodique et récurrente de la position en utilisant à cet effet une fonction du réseau (LALS). Les positions de tous les équipements terminaux associés à l'identifiant surveillé (target ID) doivent être déterminées.

Les prescriptions techniques de mise en œuvre sont édictées par le DFJP dans l'OME-SCPT et son annexe 1 (*al. 2*). Le DFJP peut par exemple prévoir que la position doit être déterminée à des intervalles fixes prédéterminés. Par manque d'expérience pratique avec cette nouvelle fonction LALS pour déterminer la position de manière récurrente et périodique, notamment concernant les ressources ou le temps nécessaires, il est impossible pour l'heure de donner des prescriptions concrètes pour les paramètres techniques tels que la fréquence, la période ou l'intervalle minimum entre deux déterminations successives de la position. Suivant l'implémentation technique, la détermination de la position peut prendre un certain temps. Les opérateurs de téléphonie mobile doivent cependant transmettre immédiatement et sans délai les positions des équipements terminaux lorsqu'elles sont déterminées.

Selon l'*al. 3, let. d*, lorsque la position n'a pas pu être déterminée, l'opérateur indique le motif de l'échec (code d'erreur) et, si possible, l'emplacement de la dernière cellule connue utilisée par l'équipement terminal, c'est-à-dire de la dernière antenne de la cellule qui a fourni le service.

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

Les *let. a à d et f* restent matériellement inchangées.

Dans les *let. e, g* et *h* sont ajoutés les nouveaux identifiants du système 5G que sont le SUPI, le GPSI et le PEI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2 pour le GPSI et ch. 10 pour le SUPI, et le commentaire de l'art. 36, al. 1, let. d pour le PEI).

À la *let. g, ch. 1* sont ajoutés les timbres horodateurs associés aux indications de localisation et qui peuvent être disponibles dans le système de téléphonie mobile de la quatrième génération (EPS) ou de la cinquième génération (5GS). Ces timbres horodateurs doivent dès lors également être livrés. Les *ch. 2* et *3* restent inchangés.

À la *let. h* la possibilité d'autres désignations appropriées telles que le nom de la zone d'accès sans fil est ajoutée, suite à l'expérience de la pratique, bien qu'il ne s'agisse pas d'un identifiant univoque. Une désignation suffisamment précise de l'accès au réseau WLAN suffit, ce qui signifie que la désignation livrée doit permettre d'identifier l'accès au réseau sur place de manière suffisamment précise (voir aussi le commentaire de l'art. 48, al. 2, let. a). Le nom de la zone d'accès sans fil doit être transmis dans le paramètre *SSID*.

La *let i* reprend la réglementation concernant les données de localisation de la navigation maritime ou aérienne, qui se trouve actuellement à la fin des let. g et h. La *let. j* correspond à l'actuelle let. i.

Les nouvelles *let. k* et *l* règlent la livraison des indications de localisation pour les accès non 3GPP au réseau de téléphonie mobile désignés comme dignes ou non dignes de confiance. Cet ajout correspond aux modifications apportées à l'art. 54, al. 3, let. d et e (voir le commentaire de ces dispositions).

Art. 61, let. b, d, g, g^{bis}, i et j

Dans les *let. b* et *d* sont ajoutés les nouveaux identifiants du système 5G que sont le SUPI, le GPSI et le PEI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2 pour le GPSI et ch. 10 pour le SUPI, et le commentaire de l'art. 36, al. 1, let. d pour le PEI).

Pour l'ajout à la phrase introductive de la *let. g* concernant les «données de localisation, dans la mesure du possible déterminées par le réseau et signalées comme telles», voir le commentaire de l'art. 56, al. 1, let. e, ch. 9. Au *ch. 1* sont ajoutés les «timbres horodateurs associés», comme à l'art. 60, let. g, ch. 1 (voir le commentaire s'y rapportant). Les *ch. 2* et *3* restent inchangés. Le nouveau *ch. 4* règle la livraison des indications de localisation pour les accès non 3GPP au réseau de téléphonie mobile désignés comme non dignes de confiance, comme le fait la modification apportée à l'art. 54, al. 3, let. d (voir le commentaire s'y rapportant).

La *let. g^{bis}* reprend, comme l'art. 60, let. i, la réglementation concernant les données de localisation de la navigation maritime ou aérienne, qui se trouve à la fin de la phrase introductive de l'actuelle let. g.

La *let. i* reste matériellement inchangée. Au *ch. 4, premier tiret*, une modification rédactionnelle est apportée pour indiquer clairement que le renvoi à la let. g se réfère aux données de localisation. Au *deuxième tiret*, le terme de «point d'accès au réseau WLAN» est remplacé par celui, plus générique, d'«accès au réseau WLAN» (voir le commentaire du remplacement d'expressions, al. 1). Une autre désignation appropriée (par ex. le nom de la zone d'accès sans fil) peut être livrée en lieu et place de l'identifiant de l'accès au réseau WLAN (voir le commentaire de l'art. 48, al. 2, let. a). Le nom de la zone d'accès sans fil doit être transmis dans le paramètre SSID.

Selon la *let. f*, les indications sur le réseau voisin «de» et sur le réseau voisin «vers» doivent également être livrées lorsque ces réseaux ont participé à la communication ou tentative d'établissement de la communication. Dans le cas d'un numéro inconnu ou usurpé (*spoofing*), les autorités de poursuite pénale auront ainsi la possibilité de retracer le chemin emprunté par la communication ou tentative d'établissement de la communication et d'en découvrir l'origine (voir aussi le commentaire de l'art. 48*c*). Cette approche est cependant difficile à mettre en œuvre dans le cadre d'une surveillance en temps réel et n'est pas compatible avec les normes ETSI et 3GPP. Il n'est donc pas proposé d'inclure une disposition analogue à l'art. 56, al. 1, let. e.

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

À la *let. a*, les numéros de port sont ajoutés aux adresses, afin que l'identification de ces serveurs et clients soit possible même dans les cas de traduction d'adresses de réseau.

Seules les POC ayant des obligations complètes en matière de surveillance sont tenues de conserver les données secondaires de services de courrier électronique (historique), c'est-à-dire les FST qui ne bénéficient pas d'une exemption au titre de l'art. 51 et les FSCD ayant des obligations étendues en matière de surveillance (art. 52). Les autres POC ne livrent que les données dont elles disposent.

Art. 63 Type de surveillance HD_31_PAGING: détermination de la position lors de la dernière activité

À l'*al. 1*, il est désormais précisé qu'il s'agit de la dernière activité que l'opérateur peut constater, et non de celle qu'il a effectivement constatée. Au besoin, la POC doit donc déterminer le lieu de la dernière activité. Par ailleurs, il est maintenant question des équipements terminaux mobiles, au pluriel, car la position de la dernière activité doit être déterminée pour tous les appareils (pas uniquement d'un seul) associé à l'identifiant surveillé.

Les indications à livrer sont détaillées à l'*al. 2*, sous une forme restructurée. Aucune indication nouvelle n'est ajoutée par rapport à la version actuelle de l'ordonnance, à l'exception des nouveaux paramètres équivalents du système 5G, dont les désignations ont changé (par ex. GPSI pour MSISDN, SUPI pour IMSI, PEI pour IMEI). Par ailleurs, la liste des exemples d'identifiants à la *let. h, ch. 1* est raccourcie de la même manière qu'à l'art. 48, al. 2, let. a (voir le commentaire s'y rapportant). Sont également ajoutés les «timbres horodateurs associés» (voir le commentaire de l'art. 54, al. 2, let. h) et les cellules activées sont désormais mentionnées au pluriel (aussi au *ch. 3*), car dans les réseaux 4G et 5G, un équipement terminal peut recevoir un service de plusieurs cellules (nœud maître et un ou plusieurs nœuds secondaires), ce qui sert à augmenter la bande passante grâce à ce qu'on appelle une agrégation de porteuses.

Art. 64, al. 2

À l'*al. 2*, les termes génériques d'identifiants de cellule ou de zone géographique remplacent la liste des différents identifiants cités à titre d'exemples (voir le commentaire de l'art. 48, al. 2, let. a). Par ailleurs, le terme de «point d'accès au réseau WLAN» est remplacé par celui, plus générique, d'«accès au réseau WLAN» (voir le commentaire du remplacement d'expressions, al. 1). Une autre désignation appropriée (par ex. nom de la zone d'accès sans fil) peut désormais être utilisée en lieu et place de l'identifiant de l'accès au réseau WLAN (voir commentaire de l'art. 48, al. 2, let. a). Le nom de la zone d'accès sans fil doit être transmis dans le paramètre *SSID*.

Art. 65, al. 2, phrase introductive, et al. 3

À l'*al. 2*, la phrase introductive subit une modification rédactionnelle.

À l'al. 3, le terme de «point d'accès au réseau WLAN» est remplacé par celui, plus générique, d'«accès au réseau WLAN» (voir le commentaire du remplacement d'expressions, al. 1). En outre, les termes génériques d'identifiants de cellule ou de zone géographique remplacent la liste des différents identifiants cités à titre d'exemples (voir le commentaire de l'art. 48, al. , let. a). Une autre désignation appropriée (par ex. nom de la zone d'accès sans fil) peut désormais être utilisée en lieu et place de l'identifiant de l'accès au réseau WLAN (voir commentaire de l'art. 48, al. 2, let. a). Le nom de la zone d'accès sans fil doit être transmis dans le paramètre SSID.

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

L'*al. 1* a une nouvelle structure. Deux nouveaux types de surveillances en temps réel ont été ajoutés pour les recherches en cas d'urgence. Les autres types de surveillances possibles n'ont fait l'objet d'aucun changement.

Il y a lieu de se référer également au commentaire des modifications apportées à l'art. 50, al. 6 concernant les services de téléphonie mobile utilisés avec des cartes SIM supplémentaires (par ex. options multi-appareils ou multi-SIM pour des équipements supplémentaires, smartphone, tablette, montre connectée, etc.).

La *let. a* définit, comme dans la version en vigueur, le type de recherche d'urgence *paging*, qui correspond au type de surveillance HD_31_PAGING (voir le commentaire de l'art. 63). La nouveauté est qu'il y est désormais précisé que les POC doivent déterminer la localisation lors de la dernière activité pour tous les équipements terminaux mobiles associés à l'identifiant surveillé (target ID) de la personne disparue ou de tiers. Cette précision concerne principalement les abonnements mobiles avec carte SIM supplémentaire (offres multi-appareil ou multi-SIM, voir aussi le commentaire de l'art. 50, al. 6). Dans ce type de recherche, qui existe depuis de nombreuses années, il s'agit de localiser des terminaux mobiles via les cellules de téléphonie mobile. Les POC livrent la dernière localisation disponible de l'appareil concerné, quels que soient la technologie et le type d'accès au réseau utilisés.

Le type de recherche EP_58_POS_IMMED à la *let b* est nouveau: il a pour objet la détermination unique et immédiate par le réseau de la position de tous les équipements terminaux associés à l'identifiant surveillé de la personne disparue ou de tiers dans le cadre d'une recherche en cas d'urgence. Sur le plan technique, ce type de recherche correspond au nouveau type de surveillance RT_56_POS_IMMED (voir aussi le commentaire de l'art. 56*a*).

La *let. c* introduit elle aussi un nouveau type de recherche, le type EP_59_POS_PERIOD, qui consiste en la détermination périodique et récurrente par le réseau de la position de tous les équipements terminaux associés à l'identifiant surveillé de la personne disparue ou de tiers. Il correspond sur le plan technique au nouveau type de surveillance RT_57_POS_PERIOD (voir aussi le commentaire de l'art. 56*b*).

La détermination de la position selon les let. b et c est nettement plus précise que la localisation selon la let. a. Son exécution recourt à des fonctions spéciales du réseau qui impliquent un niveau technique supérieur. Les nouvelles fonctions de détermination de la position permettent d'obtenir des données plus précises sur la position du téléphone mobile de la personne recherchée. Des données imprécises

retardent le sauvetage de personnes disparues et entraînent la mobilisation de moyens et d'effectifs importants (véhicules de police, hélicoptère, etc.) avec, au final, des coûts non négligeables. Avec une localisation précise, les équipes peuvent intervenir de manière plus ciblée pour sauver des vies.

La *let. d* correspond à l'actuelle let. b, qui règle la surveillance en temps réel du contenu et des données secondaires pour les besoins d'une recherche en cas d'urgence. Pour ce type de mesure, l'autorité compétente adresse, pour chaque POC et chaque numéro principal, un ordre au Service SCPT, qui transmet les mandats aux POC concernées. Ces dernières sont chargées de mettre en œuvre le type de surveillance appropriée selon les art. 55 et 57, de manière à couvrir tous les services de téléphonie (catégorie «TEL») et d'accès au réseau (catégorie «NA») qu'elles fournissent concernant les numéros associés au numéro principal. Ce regroupement permet de tenir compte de l'urgence de la situation, c'est-à-dire retrouver le plus rapidement des personnes dont l'intégrité corporelle ou la vie est menacée. Donner un mandat par service de téléphonie ou multimédia ou service d'accès au réseau surveillé, comme c'est normalement le cas pour les surveillances, prendrait trop de temps compte tenu des circonstances. Il faut pouvoir là aussi surveiller également les éventuels numéros associés au numéro principal surveillé (par ex. abonnements avec carte SIM supplémentaire, offres multi-appareils ou multi-SIM). Exemple: Une POC reçoit un mandat pour une recherche en cas d'urgence du type EP_36_RT_CC_IRI (let. b) pour le MSISDN x. L'usager possède, auprès de cette POC, un abonnement mobile avec le MSISDN x comprenant la téléphonie et l'accès à internet; l'abonnement comprend une carte SIM supplémentaire avec le MSISDN y pour l'accès à internet. La POC met en œuvre une surveillance en temps réel du contenu et des données secondaires des services de téléphonie et multimédia (art. 57) pour le MSISDN x, et deux surveillances en temps réel du contenu et des données secondaires de l'accès à internet (art. 55) portant sur le MSISDN x et sur le MSISDN y. Lors de recherches en cas d'urgence également, les surveillances en temps réel restent activées jusqu'à ce que le Service SCPT transmette le mandat de désactivation aux POC concernées.

La *let. e* correspond à l'actuelle let. c; elle définit la surveillance en temps réel des seules données secondaires, c'est-à-dire sans le contenu. La procédure est la même que celle décrite sous la let. d, à la différence que la mesure se fonde dans ce cas sur les types de surveillances selon les art. 54 et 56.

La *let. f* règle les recherches en cas d'urgence rétroactives, par exemple pour les situations où l'équipement terminal est éteint ou hors couverture. La mesure est mise en œuvre comme décrit sous la let. d, sauf qu'il s'agit ici de surveillances rétroactives selon les art. 60 et 61 que chacune des POC concernées doit activer concernant tous les services fournis par elle en lien avec le numéro surveillé et les éventuels numéros supplémentaires associés à ce numéro principal. L'autre différence par rapport aux surveillances selon la let. d est qu'un mandat de désactivation n'est pas nécessaire pour les surveillances rétroactives.

L'indemnité versée aux POC dépend du nombre de recherches en cas d'urgence ordonnées par les autorités par POC et par numéro et non du nombre de surveillances effectivement exécutées.

De nouveaux indicateurs correspondant à la technologie 5G (GPSI, SUPI, PEI) ont par ailleurs été introduits dans diverses dispositions (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2 pour le « GPSI » et ch. 10 pour le « SUPI », ainsi que le commentaire de l'art. 36, al. 1, let. d pour le « PEI »).

L'*al. 2* précise que le début et la fin des surveillances rétroactives selon l'al. 1, let. f sont déterminés par les règles prévues à l'art. 4*a* (voir le commentaire s'y rapportant).

Art. 68 Recherche de personnes condamnées

Trois nouveaux types de surveillances sont ajoutés aux *let. a à c*.

La *let. a* introduit le type de surveillance *paging*, c'est-à-dire la détermination de la position lors de la dernière activité selon l'art. 63 (voir le commentaire s'y rapportant), pour la recherche de personnes condamnées.

La *let. b* règle quant à elle l'utilisation unique de la fonction LALS, c'est-à-dire la détermination unique et immédiate de la position par le réseau conformément à l'art. 56*a* (voir le commentaire s'y rapportant).

La *let. c* enfin définit le recours périodique et récurrent à la fonction LALS, c'est-à-dire la détermination périodique et récurrente de la position par le réseau conformément à l'art. 56*b* (voir le commentaire s'y rapportant).

Le contenu des lettres restantes est repris sans changement de la version en vigueur, la seule différence étant que la let. a de l'actuelle version devient la *let. d* dans la nouvelle, et ainsi de suite jusqu'à la let. d (dans la version en vigueur) qui devient la *let. g*.

L'*al. 2* renvoie aux règles de l'art. 4*a* (voir le commentaire s'y rapportant) s'agissant du début et de la fin des surveillances rétroactives selon l'al. 1, let. f.

Art. 74a Dispositions transitoires relatives à la modification du xx.xx.xxxx

Afin de coordonner l'introduction des nouveaux types de surveillances et de renseignements entre les POC et le Service SCPT, il est judicieux de prévoir des dispositions transitoires détaillées pour les différentes modifications. Des délais sont impartis aux POC concernées et au Service SCPT pour qu'ils procèdent aux adaptations techniques requises et effectuent les tests nécessaires, de sorte que les nouveaux types de surveillances et de renseignements puissent être mis en œuvre de manière standardisée le plus rapidement possible, mais au plus tard à l'échéance du délai en question.

L'*al. 1* prévoit, pour les POC mentionnées, un délai de douze mois à compter de l'entrée en vigueur de la révision de l'ordonnance pour les quatre nouveaux types de renseignements suivants:

1. IR_51_EMAIL_LAST (renseignements sur des services de courrier électronique; art. 42*a*)
2. IR_52_COM_LAST (renseignements sur des services de communication dérivés; art. 43*a*)
3. IR_53_ASSOC_PERM (renseignements sur les identifiants attribués pour une longue durée; art. 48*a*),

4. IR_55_TEL_ADJ_NET (détermination des réseaux voisins pour les services de téléphonie et multimédia*, art. 48*c)

L'*al. 2* donne aux POC ayant des obligations complètes un délai transitoire allongé à 24 mois à compter de l'entrée en vigueur de la révision de l'ordonnance pour le cinquième nouveau type de renseignements IR_54_ASSOC_TEMP (renseignements immédiats sur les identifiants attribués pour une courte durée; art. 48*b*), qui requiert des adaptations importantes (voir aussi le commentaire de l'art. 18, al. 3). Un délai relativement court de douze mois après l'entrée en vigueur de la révision de l'ordonnance est en revanche fixé pour les deux nouveaux types de détermination unique et immédiate de la position selon les art. 56*a* (RT_56_POS_IMMED) et 67, al. 1, let. b (EP_58_POS_IMMED). Compte tenu de la plus-value attendue de ces nouveaux types de surveillances, il faut que les autorités de poursuite pénale puissent y recourir au plus vite.

L'*al. 3* prévoit deux délais pour la modification du type de renseignements HD_29_TEL ayant pour objet la désignation du réseau immédiatement voisin de la communication ou tentative d'établissement de la communication (art. 61, let. j): les POC ayant des obligations complètes doivent tout d'abord assurer la conservation des données nécessaires à cette fin dans les douze mois suivant l'entrée en vigueur de la révision de l'ordonnance et être ensuite en mesure, dans les 18 mois, de livrer les nouvelles données rétroactives (art. 61, let. j).

L'*al. 4* contient les dispositions transitoires applicables aux POC ayant des obligations complètes pour les deux nouveaux types de détermination périodique de la position selon les art. 56*b* (RT_57_POS_PERIOD) et 67, al. 1, let. c (EP_59_POS_PERIOD). Mettre en œuvre ces deux nouveaux types de surveillances dans le composant actuel de surveillance en temps réel du système de traitement ne serait judicieux ni sur le plan économique, ni du point de vue du calendrier. Ce composant arrive au terme de son cycle de vie et devra être remplacé dans un avenir proche. Cela reviendrait à faire du travail à double: il faudrait adapter une première fois le composant actuel puis, dans un second temps, le nouveau. La faisabilité d'une mise en œuvre dans le composant actuel n'est en outre pas garantie, car le fabricant ne développe plus cette version du composant. Ces nouveaux types de surveillances ne pourront par conséquent être exécutés de manière standardisée qu'une fois que le nouveau composant pour la surveillance en temps réel aura été entièrement mis en service et adapté. Les POC concernées disposeront alors de 18 mois au plus pour adapter leurs propres systèmes et effectuer les tests requis avec le Service SCPT.

L'*al. 5* est le pendant de l'al. 1, première partie, et de l'al. 2 pour le Service SCPT, qui dispose d'un délai relativement court de douze mois pour que les renseignements visés puissent être fournis de manière standardisée et les surveillances visées exécutées elles aussi de manière standardisée. Les deux nouveaux types de détermination unique et immédiate de la position selon les art. 56*a* (RT_56_POS_IMMED) et 67, al. 1, let. b (EP_58_POS_IMMED) doivent aussi être mis en œuvre dans le nouveau composant pour la surveillance en temps réel du système de traitement.

L'*al. 6* fixe, sur le modèle de l'al. 3, un délai de 18 mois au Service SCPT pour être en mesure de réceptionner les données historiques.

L'*al. 7* correspond à la deuxième partie de l'al. 1, tandis que l'*al. 8* est le pendant de l'al. 4 pour le Service SCPT.

5.2 Ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication (OEI-SCPT)

Art. 3, al. 4, let. a et b, 4bis et 5

L'*al. 4, let. a* est complété par le nouveau type de renseignements IR_53_ASSOC_PERM (art. 48*a* OSCPT). À la *let. b*, ce sont quatre nouveaux types de renseignements qui sont ajoutés : IR_51_EMAIL_LAST (art. 42*a* OSCPT), IR_51_COM_LAST (art. 43*a* OSCPT), IR_54_ASSOC_TEMP (art. 48*b* OSCPT) et IR_55_TEL_ADJ_NET (art. 48*c* OSCPT).

L'*al. 4bis* est lui aussi complété, avec l'ajout du nouveau type de renseignements IR_53_ASSOC_PERM (art. 48*a* OSCPT).

L'*al. 5* précise désormais que les recherches par champ d'antennes doivent être ordonnées en l'espace de 24 heures (dans la version actuelle: « à intervalles rapprochés ») pour que la norme s'applique. Le Service SCPT continue de fixer les montants dus conformément aux art. 13 et 17 (émoluments et indemnités pour des prestations non répertoriées).

Art. 15 **Droit**

Le *titre* est raccourci : l'article s'intitule désormais simplement « droit » (au lieu de « droit à l'indemnité »). L'art. 38, al. 2, LSCPT[33] prévoit que les POC reçoivent du Service SCPT une indemnité équitable[34] pour les frais qui leur sont occasionnés par l'exécution des surveillances et par la fourniture des renseignements visés aux art. 21 et 22.

L'*al. 1* n'est pas modifié quant au fond. Ont droit à une indemnité les POC selon l'art. 2, let. a à e, LSCPT, c'est-à-dire toutes les POC à l'exception des revendeurs professionnels (art. 2, let. f, LSCPT), à condition qu'elles remplissent les obligations que leur imposent la LSCPT et l'OSCPT en matière de fourniture de renseignements et de surveillance, indépendamment de ce que leur disponibilité à renseigner et à surveiller ait été confirmée (art. 33, al. 6, LSCPT, art. 31 OSCPT). Les POC qui ne remplissent pas leurs obligations en matière de fourniture de renseignements et de surveillance selon la LSCPT et l'OSCPT n'ont pas droit à une indemnité. Celles qui remplissent en partie leurs obligations, par exemple en apportant leur soutien au Service SCPT, peuvent être indemnisées conformément à l'art. 19, al. 2.

33 Selon la version en vigueur à partir du 1er janvier 2022.
34 « Indemnité appropriée » ; voir l'arrêt du Tribunal fédéral du 27 juillet 2021 (2C_650/2020).

L'*al. 2* dispose que les POC pourront dorénavant aussi percevoir une indemnité lorsqu'elles apportent leur soutien au Service SCPT pour la fourniture de renseignements ou la mise en œuvre de surveillances alors qu'elles ne sont pas elles-mêmes tenues de livrer des renseignements ou d'exécuter des surveillances. Ce soutien peut consister, par exemple, à prévoir une connexion à internet, à garantir au Service SCPT un accès sans entraves aux serveurs (dans les cas où cet accès induit des coûts) ou à adapter son infrastructure. À la différence de l'al. 1, cet alinéa ne crée pas de droit à l'indemnité pour les POC concernées (disposition potestative). Il est possible de ne pas indemniser certains coûts supportés par les POC, comme le courant électrique consommé en plus. L'al. 2 concerne plus particulièrement des FST ayant des obligations restreintes en matière de surveillance (art. 51 OSCPT) et des FSCD sans obligations étendues en matière de fourniture de renseignements ou de surveillance (voir art. 22 et 52 OSCPT), mais il peut aussi s'agir d'exploitants de réseaux de télécommunication internes ou de personnes qui mettent leur accès à un réseau de télécommunication public à la disposition de tiers.

Le nouvel *al. 3* reprend les dispositions qui figurent jusqu'ici à l'art. 16.

Art. 16 Abrogé

Les dispositions de cet article se trouvent désormais à l'art. 15, al. 3, et l'art. 16 est abrogé.

Art. 17, al. 3 et 3bis

L'actuel al. 4, qui fixe la règle des 80 % pour le montant de l'indemnité, se recoupe avec la fin de l'al. 3. La précision « et ce, à hauteur de 80 % » peut donc être supprimée de l'*al. 3*.

L'*al. 3bis* fixe le montant maximal de l'indemnité sur le principe de l'art. 19, al. 2, troisième phrase.

Art. 18 **Cas de prise en charge des coûts**

Compte tenu des adaptations d'ordre formel effectuées dans l'OSCPT concernant la catégorie des FSCD, la désignation « FSCD ayant des obligations étendues selon les art. 22 ou 52 OSCPT » est aussi employée dans cette ordonnance (cf. par ex. les art. 11, al. 1, let. a et 19, al. 1, OSCPT).

Art. 19, al. 1

Un renvoi à l'art. 13 (émolument pour des prestations non répertoriées) est inscrit à l'*al. 1*. Le Service SCPT peut ainsi se fonder sur cette disposition pour déterminer le montant des coûts qu'il a supportés pour cause de manquement à la collaboration de la part d'une POC. C'est le cas lorsque le Service SCPT doit fournir un surcroît de travail à la place d'une POC et que les coûts qui en résultent dépassent le montant de l'émolument correspondant. Dans le libellé actuel, le renvoi à l'art. 13 avec l'expression «sur la base du temps investi» est trop restrictif, car dans ce cas seul le premier alinéa peut s'appliquer. Avec la modification proposée (suppression de la précision «sur la base du temps investi»), le renvoi inclut également le deuxième alinéa de

l'art. 13. Grâce à cette adaptation, il sera possible de facturer la mise à disposition de matériel destiné à un usage unique directement sur la base de l'OEI-SCPT. Dans ce type de situation en effet, le Service SCPT doit décider à chaque fois au terme d'une mesure de surveillance s'il est possible ou non de laisser à la POC le matériel utilisé une seule fois. Les coûts correspondant au matériel qui est utilisé à plusieurs reprises sont compris dans le tarif horaire. Or avec ce mode de facturation, la mise en œuvre d'un cas spécial chez une POC peut générer des coûts importants. Il est donc recommandé à l'autorité qui entend ordonner une mesure de ce type de prendre contact au préalable avec le Service SCPT pour s'enquérir du montant des coûts.

Annexe

L'annexe récapitule, dans un tableau, les différents types de surveillances et de renseignements, ainsi que les émoluments (prélevés par le Service SCPT) et les indemnités (destinées aux POC) définis dans l'ordonnance. Les autorités habilitées à ordonner des mesures et celles chargées d'exploiter les données peuvent ainsi déterminer à l'avance le coût d'une surveillance. Le cas échéant, elles peuvent faire appel au Service SCPT pour connaître certains paramètres, comme le nombre de POC concernées dans un cas particulier. Les autorités qui ordonnent une mesure doivent payer l'«émolument du Service SCPT» et l'«indemnité aux personnes obligées de collaborer». Pour les renseignements selon les art. 27, 35, 37, 40, 42, 43 et 48*a* (nouveau) OSCPT, le Service SCPT ne facture plus d'émolument global (comprenant l'«émolument du Service SCPT» et l'«indemnité aux personnes obligées de collaborer») aux autorités concernées depuis le 1er juillet 2020. Les POC continuent en revanche de toucher l'indemnité de 3 francs. Sur recommandation du groupe de travail «Financement de la surveillance», les émoluments dus pour les surveillances en temps réel et les surveillances rétroactives ont été revus à la hausse, afin de compenser la perte de recettes du Service SCPT[35].

Cinq nouveaux types de renseignements et quatre nouveaux types de surveillances ont été créés dans le cadre de la révision partielle de l'OSCPT :

1) le type de renseignements IR_51_EMAIL_LAST: renseignements sur des services de courrier électronique (art. 42*a* OSCPT);
2) le type de renseignements IR_52_COM_LAST: renseignements sur d'autres services de télécommunication ou services de communication dérivés (art. 43*a* OSCPT);
3) le type de renseignements IR_53_ASSOC_PERM: renseignements sur les identifiants attribués pour une longue durée (art. 48*a* OSCPT);
4) le type de renseignements IR_54_ASSOC_PERM : renseignements immédiats sur les identifiants attribués pour une courte durée (art. 48*b* OSCPT);
5) le type de renseignements IR_55_TEL_ADJ_NET: détermination des réseaux voisins de services de téléphonie et multimédia (art. 48*c* OSCPT);
6) le type de surveillance (en temps réel) RT_56_POS_IMMED: détermination unique et immédiate de la position par le réseau (art. 56*a* OSCPT);

35 Voir la révision partielle de l'OIE-SCPT du 20 mai 2020, en vigueur depuis le 1er juillet 2020 (RO **2020** 2061) et le rapport explicatif

7) le type de surveillance (en temps réel) RT_57_POS_PERIOD: détermination récurrente et périodique de la position par le réseau (art. 56*b* OSCPT);
8) le type de surveillance (recherche en cas d'urgence) EP_58_POS_IMMED: détermination unique et immédiate de la position par le réseau (art. 67, al. 1, let. b, OSCPT); et
9) le type de surveillance (recherche en cas d'urgence) EP_59_POS_PERIOD: détermination périodique et récurrente de la position par le réseau (art. 67, al. 1, let. c, OSCPT).

Une révision partielle de l'annexe de l'OEI-SCPT est donc aussi nécessaire.

Pour fixer de nouveaux émoluments et de nouvelles indemnités, les nouveaux types de renseignements et de surveillances concernés sont confrontés aux types de renseignements et de surveillances existants. Le montant des émoluments dépend aussi d'autres facteurs, comme les coûts d'entretien, d'amortissement et d'investissement du système de traitement. La fréquence du recours aux nouveaux types de renseignements et de surveillances joue également un rôle.

En l'occurrence, les émoluments et les indemnités prévus pour les nouveaux types de renseignements correspondent aux montants en vigueur. Parmi les nouveaux types de renseignements, seul le type IR_53_ASSOC_PERM (art. 48*a* OSCPT) peut être considéré comme un renseignement « simple ». Le Service SCPT ne peut par conséquent prélever aucun émolument; les POC touchent cependant une indemnité de Fr. 3.- par enregistrement livré. Les autres nouveaux types de renseignements doivent être considérés comme des renseignements « complexes »; par demande de renseignements, un émolument de Fr. 75.- est prélevé pour le Service SCPT et une indemnité de Fr. 125.- est versée aux POC.

Dans le cas des nouveaux types de surveillances, les similitudes avec les types en vigueur sont moins nombreuses. Les deux nouveaux types de surveillances visant la détermination de la position par le réseau (LALS) proposent une fonction entièrement nouvelle. S'ils se fondent sur les montants prévus pour le type de surveillance vaguement similaire HD_31_PAGING (art. 63 OSCPT), l'émolument et l'indemnité pour la détermination unique et immédiate de la position RT_56_POS_IMMED (art. 56*a* OSCPT) sont supérieurs de Fr. 50.- afin de tenir compte de la charge de travail plus importante qui en résulte pour le Service SCPT et les POC. La détermination de la position étant néanmoins nettement plus précise, ce type de surveillance offre une plus-value considérable par rapport au type HD_31_PAGING.

Le deuxième nouveau type de surveillance visant la détermination de la position par le réseau (LALS), le type RT_57_POS_PERIOD (art. 56*b* OSCPT), correspond au type même de la surveillance en temps réel, de son activation à sa désactivation. Concrètement, le réseau détermine, à intervalles fixes, la position actuelle exacte de l'équipement terminal de la personne surveillée et la livre immédiatement au service de traitement. L'émolument global est légèrement supérieur à celui perçu pour les types de surveillances portant sur les données secondaires uniquement et plus de quatre fois supérieur à l'émolument global perçu pour la détermination unique et immédiate de la position RT_54_POS_IMMED (Fr. 2 800.- contre Fr. 600.-), car une adaptation du système de traitement est nécessaire pour réceptionner et traiter les données.

Les recherches en cas d'urgence peuvent jouer un rôle crucial pour sauver des personnes portées disparues. De fait, il n'est possible de recourir à ce type de mesure que lorsque la vie ou l'intégrité corporelle d'une personne sont menacées. C'est pourquoi, comme pour les autres types de surveillances mises en œuvre aux fins de recherches en cas d'urgence, les émoluments et les indemnités sont moins élevés que pour des surveillances comparables. Il n'est pas non plus perçu de supplément pour la détermination de la position (unique ou récurrente). L'émolument pour le type de surveillance EP_58_POS_IMMED (art. 67, let. b, OSCPT), d'un montant de Fr. 50.-, est donc identique à celui des autres types de surveillances employés dans le cadre de recherches en cas d'urgence. Fondée sur son pendant pour le type de surveillance RT_56_POS_IMMED, l'indemnité (Fr. 350.-) est toutefois inférieure de Fr. 50.-.

Le montant de l'émolument pour le type de surveillance EP_59_POS_PERIOD (art. 67, let. c, OSCPT) est identique à celui des autres types de surveillances employés lors de recherches en cas d'urgence. Comme pour la surveillance, l'indemnité prévue pour la détermination récurrente de la position dans une recherche en cas d'urgence, à savoir Fr. 750.-, est plus élevée que pour la détermination unique. Elle est en revanche plus basse que pour son pendant pour les surveillances RT_57_POS_PERIOD et identique à l'indemnité prévue pour les autres surveillances en temps réel aux fins de recherches en cas d'urgence EP_36_RT_CC_IRI (art. 67, let. d, OSCPT) et EP_37_RT_IRI (art. 67, let. e, OSCPT).

Pour les conséquences financières des nouveaux types de surveillances et de renseignements pour la Confédération, les cantons et les POC, voir le ch. 4.

Par ailleurs, sous le type de renseignements IR_18_ID, la désignation «copie de la pièce d'identité» est remplacée par «preuve de l'identité», comme dans le titre de l'art. 45 OSCPT. Sous le type de renseignements IR_21_TECH enfin, le terme «type de renseignements» est ajouté dans la colonne «détail de la mesure» dans un souci de symétrie avec les quatre types de renseignements qui précédent.

5.3 Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT)

Art. 1 Champ d'application

Étant donné que les modalités de la sécurisation de la communication seront dorénavant aussi réglées, pour les autorités, dans une ordonnance du département (cf. art. 3), il y a lieu d'adapter également le champ d'application. L'OME-SCPT, annexes comprises, s'appliquera donc non seulement au Service SCPT et aux POC, mais aussi aux autorités selon l'art. 1, al. 2, let. a à f, OSCPT.

Art. 3 Sécurisation de la communication

Dans sa teneur actuelle, cette disposition porte uniquement sur la communication entre les POC et le Service SCPT. La modification de l'art. 3 OSCPT, qui prévoit que c'est le DFJP qui détermine quels moyens de communication sont réputés sûrs, rend

nécessaire une extension du champ d'application de l'art. 3 OME-SCPT à la communication entre le Service SCPT et les autorités.

L'*al. 1* inclut désormais aussi la communication sécurisée entre le Service SCPT et les autorités selon l'art. 1, al. 2, let. a à f, OSCPT. Sont considérés des moyens de communication sûrs les moyens de transmission électronique disponibles dans le système de traitement du Service SCPT (*let. a*) et les solutions de cryptage de courriels (*let. b*), définis plus en détail dans l'annexe 1 de l'OME-SCPT. Après entente avec le Service SCPT, un autre moyen de transmission équivalent peut aussi être considéré comme sûr (*let. c*).

L'actuelle let. a concernant les communications confidentielles entre les POC et le Service SCPT est transférée dans le nouvel *al. 2*, sans faire l'objet de modifications matérielles.

Art. 10, al. 4

Les délais prévus pour la transmission par le Service SCPT aux POC des demandes de renseignements (art. 14, al. 1) et des mandats de surveillance (art. 16, al. 1, 17, al. 1 et 18, al. 1) sont repris dans le nouvel al. 4 pour les surveillances du courrier postal. Le délai pour la transmission au fournisseur d'un mandat de surveillance en temps réel du courrier est aussi fixé à une heure. Une surveillance du courrier peut uniquement être ordonnée et exécutée pendant les heures normales de travail.

Art. 11, al. 2

Le nouvel *al. 2* fixe, par analogie avec les art. 10, al. 4, 14, al. 1, 16, al. 1, 17, al. 1 et 18, al. 1, le délai dont dispose le Service SCPT pour transmettre un mandat de surveillance rétroactive de la correspondance postale (voir le commentaire de l'art. 10, al. 4).

Art. 12 **Demande de renseignements**

Les deux premières phrases de l'actuel article sont reprises telles quelles dans les *al. 1* et *2*. L'insertion d'un nouvel *al. 3* est une conséquence des adaptations des art. 35, al. 1, let. b et c et 40, al. 1, let. b et c, OSCPT, qui précisent que la période de validité devra dorénavant aussi être indiquée pour les types de renseignements IR_4_NA et IR_10_Tel. On trouve en effet souvent dans les banques de données des fournisseurs non seulement l'adresse du client valable au moment de l'enregistrement, mais aussi ses adresses successives (suite à des déménagements) et une série d'indications supplémentaires, comme le nom ou l'adresse d'une autre personne, qui tient lieu d'adresse de notification. Le fournisseur devra donc livrer, pour la durée sur laquelle porte la requête, toutes les adresses et indications dont il a connaissance, ainsi que leurs périodes de validité respectives.

Art. 14, al. 2, 3 et 4

L'*al. 2* définit les délais de traitement que doivent respecter les «grandes» POC et celles de «taille moyenne», à savoir les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance selon l'art. 51 OSCPT («grandes» POC),

les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22, POC de «taille moyenne») et les FSCD ayant des obligations étendues en matière de surveillance (art. 52 OSCPT, «grandes» POC).

La *let. a* dispose que les demandes de renseignements selon l'art. 48*b* OSCPT doivent être traitées immédiatement. Le temps de réponse à ce nouveau type de renseignements doit être très court (quelques secondes à peine), car les identifiants temporaires changent fréquemment. Ce renseignement doit donc être demandé et livré via une nouvelle interface de consultation du type LI_HIQR. S'agissant d'une consultation en temps réel, il n'est pas possible d'indiquer un moment précis. C'est le moment de la requête qui est déterminant. Il n'est pas possible non plus de faire une requête rétroactive. Il y a lieu de signaler que les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22 OSCPT, « taille moyenne ») ne sont pas tenus de livrer les renseignements selon l'art 48*b* OSCPT (voir art. 18, al. 3 OSCPT), en d'autres termes ils ne sont pas soumis à la let. a.

À la *let. b*, le délai d'une heure pour le traitement des demandes portant sur les renseignements mentionnés est maintenu. Les temps de réaction sont volontairement courts puisque ces renseignements doivent être livrés de manière automatisée (voir art. 18, al. 2, OSCPT). Sont concernés les types de renseignements suivants : IR_4_NA (art. 35), IR_5_NA_FLEX (art. 27 en relation avec l'art. 35), IR_6_NA (art. 36), IR_7_IP (art. 37), IR_10_TEL (art. 40), IR_11_TEL_FLEX (art. 27 en relation avec l'art. 40), IR_12_TEL (art. 41), IR_13_EMAIL (art. 42), IR_14_EMAIL_FLEX (art. 27 en relation avec l'art. 42) Le délai d'une heure vaut aussi pour les nouveaux renseignements suivants: IR_51_EMAIL_LAST renseignements sur des services de courrier électronique; art. 42*a* OSCPT), IR_52_COM_LAST (renseignements sur d'autres services de télécommunication ou services de communication dérivés; art. 43*a*) et IR_53_ASSOC_PERM (renseignements sur les identifiants attribués pour une longue durée ; art. 48*a* OSCPT).

À la *let. c, ch. 1*, le délai de traitement d'un jour ouvré est conservé pour les demandes qui parviennent aux fournisseurs durant les heures normales de travail. Sont concernés les types de renseignements suivants: IR_8_IP (NAT) (art. 38), IR_9_NAT (art. 39), IR_15_COM (art. 43), IR_16_COM_FLEX (art. 27 en relation avec l'art. 43), IR_17_PAY (art. 44), IR_18_ID (art. 45), IR_19_BILL (art. 46), IR_20_CONTRACT (art. 47) et IR_21_TECH (art. 48), auxquels vient s'ajouter le nouveau type de renseignements IR_55_TEL_ADJ_NET (détermination du réseau voisin de services de téléphonie et multimédia, art. 48*c* OSCPT).

Dans un délai d'un jour ouvré signifie que la réponse doit parvenir au Service SCPT et à l'autorité à l'origine de la demande avant 17 heures le jour ouvré suivant (voir exemple 1 ci-après).

Les autorités habilitées à obtenir des renseignements estiment que ce délai d'un jour ouvré est trop long lorsqu'ils transmettent une demande – urgente – durant le week-end ou un jour férié. Aussi un délai plus court de six heures est-il désormais prévu au *ch. 2* pour les «grands» FST et FSCD en cas de demandes portant sur ces types de renseignements en dehors des heures normales de travail. Ce délai de six heures correspond à celui des surveillances rétroactives déclarées urgentes. La pratique montre

que seul un très faible nombre de demandes de renseignements et d'ordres de surveillances sont transmis pendant le service de piquet. Cette disposition ne devrait donc pas entraîner de surcharge de travail pour les POC. Les autorités de poursuite doivent pouvoir obtenir le week-end et les jours fériés également les renseignements dont elles ont urgemment besoin pour avancer dans leurs investigations. Il convient de rappeler que les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22 OSCPT, FSCD de «taille moyenne») ne doivent pas mettre en place un service de piquet (cf. art. 11, al. 1, OSCPT). Ils ne sont donc pas soumis à la let. c, ch. 2.

Si une demande de renseignements qui ne peut pas être traitée de manière automatisée doit être transmise à une POC en dehors des heures normales de travail, les autorités habilitées à obtenir des renseignements (cf. art. 15 LSCPT) doivent en avertir au préalable le Service SCPT (cf. art. 11, al. 2, OSCPT) afin qu'il puisse à son tour prendre contact avec la POC concernée.

Le délai de traitement de six heures signifie que la POC dispose de six heures à compter du moment où elle reçoit la demande pour charger les renseignements demandés dans l'IRC ou, en cas de dysfonctionnement de l'IRC, pour les transmettre de manière sécurisée (cf. art. 3) au Service SCPT. Les exemples ci-après illustrent différents cas de figure.

Exemple 1: Une demande de renseignements est saisie dans l'IRC le lundi à 16 h 10 et réceptionnée quelques secondes plus tard par la POC. Dans ce cas, le délai de traitement est d'un jour ouvré. Le fournisseur a jusqu'à la fin du jour ouvré suivant, c'est-à-dire jusqu'au mardi à 16 h 59, pour livrer les renseignements.

Exemple 2: Une demande de renseignements est saisie dans l'IRC le lundi à 17 h 05 et réceptionnée quelques secondes plus tard par la POC. Le moment de la saisie de la demande se situant en dehors des heures normales de travail, l'autorité habilitée à obtenir des renseignements doit en avertir le Service SCPT, qui doit en informer sans délai la POC concernée. Cette dernière dispose d'un délai de six heures à compter de la réception de la demande pour y répondre, soit jusqu'à 23 h 05 le jour même. L'autorité doit payer un émolument supplémentaire (émolument supplémentaire pour des prestations en dehors des heures normales de travail), tandis que la POC a droit, pour les mêmes raisons, à une indemnité supplémentaire (cf. art. 6 OEI-SCPT).

Exemple 3: Lorsqu'une demande de renseignements est transmise le samedi à 18 h 50 (en dehors des heures normales de travail), le fournisseur a jusqu'au dimanche à 00 h 50 pour la traiter. La procédure est la même que dans l'exemple 2.

L'*al. 3* fixe les délais de traitement impartis aux «petites» POC, c'est-à-dire les FST ayant des obligations restreintes en matière de surveillance (art. 51).

Comme à l'al. 2, let. a et b, une distinction est faite selon la complexité des renseignements à fournir. Pour les renseignements mentionnés à la *let. a*, le délai de deux jours ouvrés selon le droit en vigueur est ramené à un jour ouvré. Le délai (deux jours ouvrés) prévu pour les renseignements sous la *let. b* reste quant à lui inchangé.

L'*al. 4* règle les délais de traitement pour les FSCD n'ayant pas d'obligations étendues selon les art. 22 ou 52 OSCPT et pour les exploitants de réseaux de communication

internes, qui doivent uniquement livrer les données dont ils disposent (cf. art. 22, al. 3, LSCPT). Ces deux catégories de POC ne sont pas tenues, pour livrer des renseignements, de s'en tenir aux types standardisés prévus dans l'OSCPT (art. 18*a* OSCPT).

Pour le détail des délais de traitements, voir le tableau «Vue d'ensemble des délais de traitement» en annexe.

Art. 18, al. 2 et 3

Suite à l'introduction de nouvelles lettres aux art. 67, al. 1, et 68, al. 1, OSCPT, il y a lieu d'adapter les renvois aux. al. 2 et 3.

Annexe 1

Cinq nouveaux types de renseignements et quatre nouveaux types de surveillances sont créés avec la révision partielle de l'OSCPT :

1) le type de renseignements IR_51_EMAIL_LAST: renseignements sur des services de courrier électronique (art. 42*a* OSCPT);
2) le type de renseignements IR_52_COM_LAST: renseignements sur d'autres services de télécommunication ou services de communication dérivés (art. 43*a* OSCPT);
3) le type de renseignements IR_53_ASSOC_PERMl: renseignements sur les identifiants attribués pour une longue durée (art. 48*a* OSCPT);
4) le type de renseignements IR_54_ASSOC_PERM: renseignements immédiats sur les identifiants attribués pour une courte durée (art. 48*b* OSCPT);
5) le type de renseignements IR_55_TEL_ADJ_NET: détermination des réseaux voisins de services de téléphonie et multimédia (art. 48*c* OSCPT);
6) le type de surveillance (en temps réel) RT_56_POS_IMMED: détermination unique et immédiate de la position par le réseau (art. 56*a* OSCPT);
7) le type de surveillance (en temps réel) RT_57_POS_PERIOD: détermination récurrente et périodique de la position par le réseau (art. 56*b* OSCPT);
8) le type de surveillance (recherche en cas d'urgence) EP_58_POS_IMMED: détermination unique et immédiate par le réseau de la position (art. 67, al. 1, let. b, OSCPT); et
9) le type de surveillance (recherche en cas d'urgence) EP_59_POS_PERIOD: détermination périodique et récurrente par le réseau de la position (art. 67, al. 1, let. c, OSCPT).

Une révision partielle de l'annexe 1 de l'OME-SCPT est nécessaire afin de fixer les prescriptions applicables aux interfaces pour la mise en œuvre de la surveillance des télécommunications. Il s'agit aussi d'y intégrer des paramètres et des désignations relatives à la technologie 5G.

5.4 Ordonnance sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication (OST-SCPT)

Art. 3, al. 2, let. a à c

À l'*al. 2*, le renvoi à la section 1 du chapitre 3 de l'OSCPT est précisé aux *let. a* à *c* afin d'indiquer clairement que les données issues de mesures en application des articles figurant dans cette section de l'ordonnance – par exemple les art. 25 (surveillances et renseignements spéciaux) et 27 (types de renseignements avec recherche flexible de nom) – peuvent aussi être traitées dans le système de traitement pour la surveillance des télécommunications. Grâce au nouveau composant pour la surveillance en temps réel, un volume toujours plus important de données issues de surveillances dites spéciales pourront également être livrées aux autorités de poursuite pénale via le système de traitement. Pour le reste, le contenu de la disposition reste inchangé. Aucune modification n'est apportée à l'al. 2, let. d.

Art. 8, al. 3 à 6

Conformément à l'*al. 3*, le Service SCPT peut autoriser des collaborateurs (ceux assumant le rôle «OrgAdmin») de certaines autorités, principalement la police, à octroyer des accès à d'autres personnes. Actuellement, ces personnes ne peuvent octroyer des accès qu'à l'intérieur de leur organisation ou à des personnes directement concernées par la procédure et à leurs conseils juridiques. À l'avenir, il sera possible de donner accès également aux membres des autorités chargées d'autoriser les mesures, en particulier du tribunal des mesures de contrainte. Les autorisations prévues dans l'annexe sous le ch. 2.7 «Autorité qui donne l'autorisation» restent inchangées. Selon le droit en vigueur, seul le Service SCPT est habilité à octroyer ces accès. Les collaborateurs assumant le rôle d'OrgAdmin pourront dorénavant aussi le faire. Les droits ainsi octroyés donnent uniquement accès au système MCM (*Warrant Management Component*), c'est-à-dire le système utilisé pour la gestion des mandats. Ils ne permettent pas d'accéder aux données proprement dites de la surveillance de la correspondance par poste et télécommunication.

Les *al. 4 et 5* précisent que l'accès aux données est réservé au Service SCPT. Les collaborateurs du service ou les auxiliaires éventuels n'ont en principe pas accès aux données des différentes surveillances. Dans la plupart des cas, un logiciel se contente de balayer les données enregistrées dans le système. Il n'est pas prévu qu'une personne puisse prendre connaissance du contenu des données (principe «privacy by design», c'est-à-dire le respect de la confidentialité dès la conception). Les collaborateurs du Service SCPT et les autres personnes auxquelles celui-ci fait appel pour le soutenir dans l'exécution de son mandat sont en général tout de même soumis à un contrôle de sécurité relatif aux personnes. Il peut être nécessaire de faire appel à des personnes externes par exemple lorsqu'un problème complexe affecte un composant matériel ou logiciel et que seul un spécialiste du fabricant du matériel ou du fournisseur du logiciel est à même de le résoudre, ou encore lorsque le recours à des auxiliaires est indispensable pour faire face à la charge de travail. Les art. 18, al. 1, LSCPT et 29 OSCPT

chargent le Service SCPT de prendre des mesures pour assurer la qualité des données livrées par les fournisseurs.

L'*al. 4* concrétise le principe inscrit à l'art. 18, al. 2, LSCPT selon lequel le Service SCPT peut, avec l'accord préalable de l'autorité en charge de la procédure, prendre connaissance du contenu des données, par exemple lorsque l'autorité qui a ordonné une surveillance constate elle-même une anomalie, comme une conversation téléphonique où seule la voix d'un des deux participants est audible.

L'assurance de la qualité n'est pas le seul motif valable pour autoriser l'accès aux données et à leur contenu: il peut aussi être nécessaire d'y accéder pour conseiller l'autorité qui ordonne la mesure ou toute autre autorité habilitée (art. 16, let. j, LSCPT) ou pour assurer le bon fonctionnement du système de traitement. Dans ces cas de figure, le Service SCPT doit toujours obtenir au préalable l'autorisation écrite de l'autorité en charge de la procédure. L'exigence de la forme écrite selon l'al. 4 est nécessaire à des fins de preuve. L'art. 11, al. 1, let. b, OTNI[36] prévoit de la même manière que l'autorité responsable doit donner son accord par écrit. En revanche, les exigences fixées à l'art. 14 CO[37] concernant la forme écrite ne s'appliquent pas. L'accord ne doit donc pas obligatoirement être accompagné d'une signature manuscrite ou d'une signature électronique qualifiée. Un simple courriel est suffisant pour remplir le critère de la forme écrite.

L'art. 6 LSCPT charge le Service SCPT d'exploiter un système informatique pour le traitement des données de la surveillance des télécommunications. Afin de garantir une exploitation sûre de ce système, l'al. 5 prévoit des exceptions aux exigences de l'al. 4: en tant que responsable de la sécurité du système de traitement, le Service SCPT doit prendre des mesures (art. 12 LSCPT et art. 11 OST-OSCPT) qui ne requièrent pas toujours l'accord préalable de l'autorité en charge de la procédure (cf. al. 5). Il peut s'agir aussi bien de mesures préventives, comme des tests de fonctionnement ou des observations statistiques du comportement du système, que d'interventions destinées à réparer un dysfonctionnement constaté. C'est pourquoi le Service SCPT effectue, à des fins de contrôle de la qualité, un monitorage qui permet de vérifier que le système fonctionne correctement et que les données qui s'affichent sont plausibles (les données sont-elles lisibles, le contenu est-il utile et peut-il être exploité?). Les collaborateurs du Service SCPT et les auxiliaires éventuels (par ex. des spécialistes du fournisseur du logiciel employé) doivent accéder à cet effet à différentes données de surveillance (données secondaires, données de journalisation, contenu proprement dit, etc.). Il peut alors arriver qu'ils prennent ce faisant connaissance du contenu de la surveillance, même si ce n'est ni leur intention, ni leur objectif premier. La personne est cependant concentrée sur le problème qu'elle doit régler et ne perçoit le plus souvent que des bribes du contenu. Les accès destinés à contrôler périodiquement la qualité des données et la stabilité du système et à corriger au plus vite d'éventuels problèmes se font généralement de manière automatisée. Il s'agit notam-

36 Ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (ordonnance sur la transformation numérique et l'informatique, **OTNI**; RS **172.010.58**)

37 Loi fédérale du 30 mars 1911 complétant le code civil suisse (livre cinquième : code des obligations, **CO** ; RS **220**)

ment de déterminer l'étendue du dysfonctionnement (un seul dossier est-il concerné ?), ainsi que sa portée (la livraison des données est-elle retardée, incomplète voire impossible ?), sa durée et ses caractéristiques (types de surveillances concernés, fournisseurs touchés ?).

L'*al. 5* énumère donc les situations dans lesquelles, en dérogation à l'al. 4, le Service SCPT n'a pas besoin de l'accord de l'autorité en charge de la procédure.

Pour assurer le bon fonctionnement du système, en cas de graves dysfonctionnements ou de risque de graves dysfonctionnements (*let. a, ch. 1),* un accès rapide est nécessaire pour identifier les données concernées et résoudre le problème (cf. aussi l'art. 11). Un risque de dysfonctionnement est aussi considéré comme une urgence qui requiert une intervention immédiate. On peut imaginer le cas d'une surveillance dont il apparaît durant la nuit qu'elle occupe très rapidement un espace de stockage considérable, or l'autorité à l'origine de la mesure est joignable uniquement pendant les heures de bureau. Les collaborateurs du Service SCPT doivent pouvoir accéder aux données à ce stade déjà, afin de circonscrire le problème et préserver la stabilité du système.

Il en va de même des cas dans lesquels il serait impossible, sauf au prix d'efforts disproportionnés, de retrouver une surveillance à l'origine d'un problème (*let. a, ch. 2*) ou de contacter l'autorité concernée (par ex. les jours fériés). Un changement minime dans la transmission des produits ou des formats peut entraîner des problèmes de représentation dans le système de traitement (erreurs ou distorsions) susceptibles de causer à leur tour des difficultés lors de l'exploitation des données par les autorités compétentes. Des pertes de qualité voire des problèmes affectant le système dans son ensemble ne peuvent pas non plus être exclus lors de l'enregistrement et de la conversion des données, pourtant de bonne qualité, livrées par les POC. Des analyses approfondies sont parfois nécessaires pour remonter à la source du dysfonctionnement et il est impossible de savoir, avant d'y procéder, laquelle des surveillances est à l'origine du problème. Il n'est donc pas possible, dans ce type de situation, d'obtenir un accord préalable.

Il faut bien souvent confronter un très grand nombre de données pour détecter des anomalies, identifier la surveillance ou le format à l'origine d'un problème ou, de manière générale, assurer le bon fonctionnement et la stabilité du système de traitement (cf. monitorage évoqué ci-dessus). Si les messages d'erreur concernent un grand nombre de surveillances, il faut vérifier chacune d'elles. Identifier et contacter toutes les autorités concernées serait quasiment impossible et impliquerait une charge de travail disproportionnée. C'est pourquoi le consentement n'est pas non plus requis lorsqu'un grand nombre de surveillances sont concernées (*let. b*).

L'*al. 6* charge le Service SCPT de prévoir des mesures d'ordre contractuel, technique ou organisationnel pour empêcher une diffusion des données. Il s'agit d'empêcher que toutes les personnes – pas seulement des tiers (par ex. auxiliaires du Service SCPT), mais aussi les collaborateurs du Service SCPT – qui doivent accéder aux données des surveillances pour exécuter leurs tâches ne les divulguent à d'autres.

Art. 10, al. 4

Les délais de conservation des données dans le système de traitement pour la surveillance des télécommunications sont définis à l'art. 11 LSCPT. L'*art. 10, al. 4* règle la durée de conservation des fichiers de journalisation. Dans la version allemande, le terme « Speicherdauer » (littéralement durée d'enregistrement) est remplacé par celui plus précis de « Aufbewahrungsdauer » (durée de conservation).

Une disposition fait toutefois défaut dans l'ordonnance en vigueur concernant la durée de conservation des fichiers de journalisation de la destruction des données. Le but principal est de pouvoir déterminer quelles données conservées auparavant sur une longue période avec des fonctions de traitement restreintes ont été détruites et à quel moment. L'art. 10 OLPD[38] n'est pas applicable.

Art. 11 **Mesures pour la sécurité du système**

Le terme quelque peu imprécis et restrictif d'« exploitation ordinaire » est remplacé par celui de « bon fonctionnement », également employé à l'art. 8, al. 4.

Annexe, let. af

L'«affichage du statut des parties du système de traitement auxquelles la personne a accès», c'est-à-dire le *Dashboard PTSS*, est une application qui permet de visualiser la performance des différents composants de surveillance. C'est là que sont publiés en effet les tickets et les communications (par ex. annonces de dérangements et leur statut, statut des composants système, stabilité des réseaux), ainsi que les échéances à venir (par ex. fenêtres de maintenance pour les composants système ou d'autres systèmes, comme I-Net de Teldas). Le Dashboard PTSS traite aussi notamment des données permettant de visualiser, sous la forme de graphiques, la performance actuelle du composant de surveillance en temps réel (ISS). Cette précision du tableau synoptique permet de régler les accès des autorités habilitées et du Service SCPT au Dashboard PTSS, l'étendue concrète des droits et des données affichées dépendant des droits d'accès effectifs de chaque personne aux composants du système de traitement.

Annexe

Tableau «Vue d'ensemble des délais de traitement»

38 Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (**OLPD** ; RS **235.11**)

Tableau «Vue d'ensemble des délais de traitement»

Mandat	Art. OSCPT	Types de mesures	Service SCPT	Fournisseur de services postaux
Surveillance en temps réel services postaux pendant les heures de bureau	16, let. a 16, let. b	PO_1_RT_INTERCEPTION PO_2_RT_DELIVERY	≤ 1 heure	≤ 1 jour ouvré
Surveillance rétroactive services postaux pendant les heures de bureau	16, let. c	PO_3_HD	≤ 1 heure	≤ 3 jours ouvrés
Désactivation uniquement pendant les heures de bureau	16, let. a	PO_1_RT_INTERCEPTION	≤ 1 heure	≤ 1 jour ouvré

Mandat	Art. OSCPT	Types de mesures	Service SCPT	FST ayant des obligations complètes* FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22 OSCPT) FSCD ayant des obligations étendues en matière de surveillance (art. 52 OSCPT)	FST ayant des obligations restreintes en matière de surveillance (art. 51 OSCPT)
Renseignements	35 27, 35 36 37 40 27, 40 41 42 27, 42 42*a* 43*a* 48*a*	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 IR_51_EMAIL_LAST IR_52_COM_LAST IR_53_ASSOC_PERM	≤ 1 heure	≤ 1 heure	≤ 1 jour ouvré
	48*b*	IR_54_ASSOC_TEMP	immédiatement	Immédiatement (sauf FSCD ayant des obligations étendues en matière de fourniture de renseignements, art. 22 OSCPT)	--
	38 39 43 27, 43 44 45 46 47 48 48*c*	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 IR_55_TEL_ADJ_NET	≤ 1 heure	Réception durant les heures normales de travail: ≤ 1 jour ouvré Réception en dehors des heures normales de travail ou un jour férié: ≤ 6 heures (sauf FSCD ayant des obligations étendues en matière de fourniture de renseignements, art. 22 OSCPT)	≤ 2 jours ouvrés

Mandat	**Art. OSCPT**	**Types de mesures**	**Service SCPT**	**FST ayant des obligations complètes*** **FSCD ayant des obligations étendues en matière de surveillance (art. 52 OSCPT)**
Surveillance en temps réel pendant les heures de bureau	54 55 56 56*a* 56*b* 57 58 59	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 heure	≤ 1 heure
Surveillance en temps réel par date pendant les heures de bureau	54 55 56 56*a* 56*b* 57 58 59	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 heure	À mettre en place pour le moment indiqué dans le mandat (> 1 heure)
Surveillance en temps réel pendant le service de piquet	54 55 56 56*a* 56*b* 57 58 59	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 heure	≤ 2 heures
Surveillance rétroactive pendant les heures de bureau	60 61 62 63 64 65 66	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV AS_33_PREP_REF AS_34	≤ 1 heure	≤ 3 jours ouvrés
Surveillance rétroactive	60 61	HD_28_NA HD_29_TEL	≤ 1 heure	≤ 6 heures

situations déclarées urgentes (pendant les heures de bureau ou le service de piquet)	62 63 64 65 66	HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV* AS_33_PREP_REF AS_34		
Recherche en cas d'urgence pendant les heures de bureau ou le service de piquet	67, al. 1, let. a 67, al. 1, let. b 67, al. 1, let. c 67, al. 1, let. d 67, al. 1, let. e	EP_35_PAGING EP_58_POS_IMMED EP_59_POS_PERIOD EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 heure	≤ 1 heure
	67, al. 1, let. f	EP_38_HD	≤ 1 heure	≤ 4 heures
Recherche de personnes condamnées pendant les heures de bureau ou le service de piquet	68, al. 1, let. a 68, al. 1, let. e 68, al. 1, let. d 68, al. 1, let. e 68, al. 1, let. e 68, al. 1, let. e 68, al. 1, let. d 68, al. 1, let. b 68, al. 1, let. c	HD_31_PAGING 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 RT_56_POS_IMMED RT_57_POS_PERIOD	≤ 1 heure	≤ 1 heure
Recherche de personnes condamnées pendant les heures de bureau ou le service de piquet	68, al. 1, let. f 68, al. 1, let. f 68, al. 1, let. f 68, al. 1, let. g 68, al. 1, let. g 68, al. 1, let. g	HD_28_NA HD_29_TEL HD_30_EMAIL AS_32_PREP_COV** AS_33_PREP_REF AS_34	≤ 1 heure	≤ 4 heures
Désactivation uniquement pendant les heures de bureau	54 55 56 56*b* 57 58 59 67, al. 1, let. c	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_57_POS_PERIOD RT_25_TEL_IRI_CC RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_59_POS_PERIOD	≤ 1 heure	≤ 1 jour ouvré

	67, al. 1, let. d 67, al. 1, let. e	EP_36_RT_CC_IRI EP_37_RT_IRI		

* FST, sauf ceux ayant des obligations restreintes en matière de surveillance (art. 51 OSCPT)

** Le type de surveillance AS_32_PREP_COV (art. 64 OSCPT) n'est pas possible pendant le service de piquet (art. 11, al. 1, let. d, OSCPT).